Automatic Presentations of Groups and Semigroups

Graham Oliver

Department of Computer Science

University of Leicester

Thesis submitted for the degree of Doctor of Philosophy

August 2006

Abstract

Effectively deciding the satisfiability of logical sentences over structures is an area well-studied in the case of finite structures. There has been growing work towards considering this question for infinite structures. In particular the theory of automatic structures, considered here, investigates structures representable by finite automata. The closure properties of finite automata lead naturally to algorithms for deciding satisfiability for some logics.

The use of finite automata to investigate infinite structures has been inspired by the interplay between the theory of finite automata and the theory of semigroups. This inspiration has come in particular from the theory of automatic groups and semigroups, which considers (semi)groups with regular sets of normal forms over their generators such that generator-composition is also regular.

The work presented here is a contribution to the foundational problem for automatic structures: given a class of structures, classify those members that have an automatic presentation. The classes considered here are various interesting subclasses of the class of finitely generated semigroups, as well as the class of Cayley Graphs of groups. Although similar, the theories of automatic (semi)groups and automatic presentations differ in their construction. A classification for finitely generated groups allows a direct comparison of the theory of automatic presentations with the theory of automatic groups.

Acknowledgements

First, the professional: genuine thanks must go, of course, to my supervisor Rick Thomas - a never-ending supply of sharp insights, readily available support, and good humour. This thesis would be nothing without him.

For interesting and enjoyable discussions, I would like to acknowledge many both at home and abroad. I will single out only Sasha Rubin, whose work and enthusiasm were both always inspiring.

I am most grateful to the EPSRC, for making the funds available that saw me through the course.

And finally, thanks must go to my examiners - Nik Ruškuc and Fer-Jan de Vries - for enduring the work presented to them, and managing to drag it somewhere towards a comprehensible document.

Next, the personal: above all, for love, support, encouragement and distraction as required, my sincerest thanks to Steph.

I would like to thank my family - Mum, Dad, Tom and Stephen - for making me who I am, and showing love and encouragement throughout.

And finally, to all my friends - at Leicester, Warwick, and further afield - for showing an interest, and more generally just for being there.

Contents

Chapter 1

Introduction

It is structures in a formal sense, and logics over them, that constitute the area of *model theory*. *Finite model theory*, where the domain of the structures is taken to be finite, has been of particular interest to computer science - see for example [25]. One major area is that of *descriptive complexity*, where problems solvable in certain complexity classes are shown to be equivalently definable in certain logics.

Recently, there has been an interest in moving to *infinite* structures, for instance the state space of non-terminating systems, or many interesting mathematical objects. The difficulty is that for many structures with infinite domains most interesting logics become undecidable. As such, effort has been directed towards the problem of finding classes of (in general infinite) structures that have finite presentations that allow for deciding at least some reasonable strength of logical definability.

There is now a body of work on this problem for graphs, particularly with respect to monadic second order logic, with many interesting results - see for example [50]. The same sort of questions are beginning to be asked with regard to another central class of structures: semigroups. Semigroups tend to have a more complicated form than graphs, so first-order logic is a more appropriate starting point for attaining decidability. For instance, in [21] it is shown that $FOLM$, a restricted version of first-order logic (FO), is decidable for monoids presented by recognisable, convergent, suffix semi-Thue systems. They show how to construct, for every $FOLM$ sentence, a $FO(TC^1)$ sentence over the Cayley graph of the monoid. If the monoid is presented by a recognisable, convergent, suffix semi-Thue system, then its Cayley graph is prefix-recognisable, and so $FO(TC^1)$ is decidable by [14]. Other work on algorithmic and complexity questions for semigroups, particularly monoids, includes [10, 18, 52].

Considering questions of computability with respect to infinite structures is not new: taking the Turing machine as our computational paradigm, a *computable structure* is one for which there exists Turing machines which 'check' the relations in the structure. However, the theory of computable structures does not help with decidability of logics: in particular, being computable only guarantees decidability for quantifier-free sentences over the structure. Khoussainov and Nerode have introduced [42] a very interesting restriction that has more potential from this angle, a restriction to *automatic structures.* These are structures whose domain and relations can be checked by finite automata, a natural restriction of Turing machines. A structure isomorphic to an automatic structure is said to have an *automatic presentation.* As well as these presentations clearly being finite, they also give a generic algorithm for deciding the full first-order theory of the structures (even supplemented with certain counting quantifiers - see [5, 68]). More model-theoretic aspects have been drawn out - see for example [5, 7]. One particularly interesting result is a characterisation of automatic structures as those structures that are first-order interpretable in the infinite binary tree supplemented with an equal depth relation. This should be compared with [2, 6], where structures that are monadic-second-order interpretable in the infinite binary tree are considered. Although the theory of automatic structures continues to be developed, the two theses [5, 68] contain the main bulk of known results.

The notion of automatic structures has multiple precedents - originating in the work of Buchi [8], early results were presented by Hodgson [37, 38], and the idea can also be seen in work by Pelecq [62] and Sénizergues [69]. One motivation for using finite automata in particular comes from group and semigroup theory. A group is said to be automatic if, when the elements of the group are coded as strings of generators, there is a regular subset of the set of all strings of generators such that there are finite automata to check composition of words in this subset with generators. This concept was introduced in [27], motivated by work in hyperbolic manifolds as well as a general interest in computing on groups, and has been generalised to semigroups in [12]. The considerable success of this area suggests that a similar approach for more general structures could prove fruitful. It should be noted that, for technical reasons, the definitions do not coincide for groups.

The foundational question asking which structures have, and have not, got automatic presentations is just beginning to be investigated. This thesis addresses this question for (in general finitely generated) groups, semigroups and their Cayley graphs. As well as being fundamentally interesting classes in themselves, this also allows for a direct comparison of the theory of automatic presentations with the theories of automatic groups and automatic semigroups. For finitely generated groups, we have shown that they have an automatic presentation exactly when they are *virtually abelian*, i.e. contain an abelian (commutative) subgroup of finite index, Theorem 3.4.5. This result has been published as [61]. We have also shown that a finitely generated cancellative monoid has an automatic presentation only if it is a subsemigroup of a finitely generated virtually abelian group, Theorem 4.2.6.

Chapter 2

Preliminaries

2.1 Logic

We shall begin by introducing the notions we need from logic and model theory; the exposition will loosely follow [36], where many more details, interesting and useful results, and historical information, may be found.

A *signature* is a set of function and relation symbols, each with an *arity* (some $n \in \mathbb{N}$), and constant symbols (throughout, we shall implicitly take signatures to be finite). Given a signature τ, a τ*-structure* $\mathcal{S}$ consists of a set S, and: for each function symbol of arity n, an n-ary function on S; for each relational symbol of arity n, a subset of S^n; and for each constant symbol, an element $s \in S$.

Example 2.1.1. For a graph, it is usual to consider a signature with just one arity 2 relation symbol, say $\tau = \{E\}$. Then, a graph is a τ-structure $\mathcal{G} = (G, E^G)$, where $E^G \subseteq G^2$.

A *relational structure* is a structure whose signature consists solely of relation symbols. Any structure may be viewed as a relational structure:

informally, replace every function symbol of arity n in the signature by a relation symbol of arity $n+1$ and every constant symbol by a relation symbol of arity 1. To aid later exposition we shall, when being formal, consider all structures as relational; however, the replacement will often only be implicit, and any later references to 'functions' or 'constants' should be treated accordingly. This replacement is not free from complications (consider, say, the effect on quantifier depth), but none will really impinge on this thesis.

A large variety of mathematics can be framed around structures of one sort or another. Mathematicians are usually happy to talk about any properties of the structure they are considering; however, for computer scientists, it is more usual to insist on a restricted formal language, in order that questions may be answered algorithmically. Let τ be a signature. Let V be an infinite set of variable symbols. The *terms* of τ are the variables in V. The *atomic formulas* of τ are: $s = t$, where s and t are terms of τ; $R(t_1 \ldots, t_n)$, where R is an n-ary relation symbol in τ and $t_1, \ldots, t_n$ are terms of τ.

Atomic formulas are used as the building blocks of sentences describing a structure. They are combined using the following symbols:

$\neg$ 'not' $\wedge$ 'and' $\vee$ 'or' $\rightarrow$ 'implication' $\forall$ 'for all' $\exists$ 'there exists'.

Given these, the *(first-order) formulas* of τ are: all atomic formulas; $\neg\phi$, where ϕ is a formula of τ; $\phi \wedge \psi$, where ϕ and ψ are formulas of τ; $\phi \vee \psi$, where ϕ and ψ are formulas of τ; $\forall x \phi$, where x is a variable and ϕ is a formula of τ; $\exists x \phi$, where x is a variable and ϕ is a formula of τ.

The formulas used in building up a formula ϕ are called *subformulas* of ϕ. Let x be a variable symbol in ϕ. If each occurrence of x in ϕ occurs in a (not necessarily new) subformula of the form $\forall x \psi$ or $\exists x \psi$, then x is called *bound*; otherwise, x is called *free*. A *sentence* of τ is a formula with every variable bound. If a formula ϕ contains variables $x_1, \ldots, x_n$ that are not bound, then we will sometimes write $\phi(x_1, \ldots, x_n)$ to emphasise this.

We shall leave as intuitive what is meant by an n-tuple of elements $(a_1, \ldots, a_n)$ from a structure $\mathcal{S}$ *satisfying* $\phi(x_1, \ldots, x_n)$ (see [36] for details). If they do, we shall denote this as $S \models \phi(a_1, \ldots, a_n)$. Also, $\phi(X^n)$ shall denote $\{(a_1, \ldots, a_n) \in X^n : S \models \phi(a_1, \ldots, a_n)\}$.

If $\mathcal{S}$ is a τ-structure, then $\mathrm{Th}(\mathcal{S})$, called the *first-order* (or *elementary*) *theory* of $\mathcal{S}$, is the set of sentences ϕ of τ such that $S \models \phi$.

2.1.1 Interpretations

It is often useful to be able to find one structure inside another. The model theoretical way of doing this is via an interpretation.

Definition 2.1.2. *Let τ and ρ be signatures, $\mathcal{S}$ a τ-structure, and $\mathcal{T}$ a ρ-structure. Let $n \in \mathbb{N}$. An* (n-dimensional) interpretation *of $\mathcal{T}$ in $\mathcal{S}$ consists of the following:*

- *a formula $\delta(x_1, \ldots, x_n)$ of τ, called the domain formula;*
- *a surjective map $f : \delta(S^n) \to T$, called the co-ordinate map;*
- *for each atomic formula $\phi(y_1, \ldots, y_m)$ of ρ, a formula $\phi^S(\bar{x}_1, \ldots, \bar{x}_m)$ of τ with $\bar{x}_i$ an n-tuple of variables.*

where for each atomic formula ϕ of ρ and $\bar{a}_i \in \delta(S^n)$,

$$\mathcal{T} \models \phi(f(\bar{a}_1), \ldots, f(\bar{a}_m)) \Leftrightarrow \mathcal{S} \models \phi^S(\bar{a}_1, \ldots, \bar{a}_m).$$

If there is an interpretation of $\mathcal{T}$ in $\mathcal{S}$, we say $\mathcal{T}$ is *interpretable* in $\mathcal{S}$. For more details on interpretations, see Chapter 5 of [36]. We will see later on how this definition will be of use to us.

2.2 Automata over Structures

Now we have set the context, we can build up to the definition of an automatic presentation.

2.2.1 Regular Languages

Let Σ be a finite set. We shall refer to this set as an *alphabet*, and call its members *symbols*. Informally we are interested in finite strings of symbols, called *words*. We shall denote the string of zero symbols, the empty word, by λ. Then, $\Sigma^\star$ denotes the set of all finite words over Σ. A *language* is a subset $L \subseteq \Sigma^\star$.

We hope to sometimes be able to recognise membership of a specified language. A *finite automaton* is built as follows. We start with a finite set Q, whose members are called *states*, and an alphabet Σ. We then take a relation $R \subseteq Q \times \Sigma \times Q$, called the *transition* relation, describing how to move between states. A state $s \in Q$ is specified as the *start* state, and a set of states $F \subseteq Q$ as the *finish* states.

Now take $a \in \Sigma^\star$, i.e. $a = a_1 a_2 \ldots a_n$, with $a_i \in \Sigma$. If there is a sequence of states $q_1, q_2, \ldots, q_{n+1}$ satisfying:

- $q_1 = s$ *"Start at the beginning...*
- $(q_i, a_i, q_{i+1}) \in R, 1 \leq i \leq n$ *...keep going...*
- $q_{n+1} \in F$ *...until you reach the end, then stop." [13]*

then a is said to be *accepted* by the automaton. The language of words accepted by an automaton A is denoted $L(A)$.

If for every state p and symbol $a \in \Sigma$ there *is* a state q such that $(p, a, q) \in R$, the automaton is called *complete*; if for every state p and symbol a there is *at most one* state q such that $(p, a, q) \in R$, the automaton is called *deterministic*. In particular, a deterministic complete finite automaton is an automaton with R a function. We shall need the following, see for example [40]:

Proposition 2.2.1. *Let L be a language such that $L = L(A)$ for some finite automaton A; then there is a deterministic complete finite automaton A' such that $L = L(A')$.*

If a language $L \subseteq \Sigma^\star$ is the language of some finite automaton A, i.e. $L = L(A)$, then L is called *regular*.

The class of regular languages satisfies many useful closure properties - this robustness is one reason for its ubiquity. The following are standard:

Proposition 2.2.2. *Let A and A' be finite automata; then,*

- *there is a finite automaton B such that $L(B) = L(A) \cup L(A')$;*
- *there is a finite automaton B such that $L(B) = L(A) \cap L(A')$;*
- *there is a finite automaton B such that $L(B) = L(A) \setminus L(A')$.*

Soon, we shall want to speak of automata reading multiple words simultaneously. This does not in fact require a new machine model - we just need to set up the correct definitions.

Let $L \subseteq \Sigma^\star$ be a language. Consider n words from this language:

$$w_1 = w_{1,1}w_{1,2} \dots w_{1,l_1}$$

$$w_2 = w_{2,1}w_{2,2} \dots w_{2,l_2}$$

$$\dots$$

$$w_n = w_{n,1}w_{n,2} \dots w_{n,l_n}$$

where $w_{i,j} \in \Sigma$. Let $l = \max\{l_i\}$, and $\# \notin \Sigma$. The *convolution* of $w_1, \ldots, w_n$ is the word

$$(w_{1,1}, w_{2,1}, \ldots, w_{n,1})(w_{1,2}, w_{2,2}, \ldots, w_{n,2}) \ldots (w_{1,l}, w_{2,l}, \ldots, w_{n,l})$$

over the alphabet $(\Sigma \cup \#)^n$, where $w_{i,j} = \#$ when $j > l_i$. We shall denote this word $\mathrm{conv}(w_1, \ldots, w_n)$.

The notion of convolution enables us to talk of 'regular languages' of n-tuples. To be precise, we will call a set $S \subseteq (\Sigma^\star)^n$ *regular* if the language

$$\{\mathrm{conv}(w_1, \ldots, w_n) : (w_1, \ldots, w_n) \in S\}$$

is regular over the alphabet $(\Sigma \cup \#)^n$.

Proposition 2.2.3. *Let $L_1, \ldots, L_n$ be languages.*

- *$L_1 \times \ldots \times L_n$ is regular if and only if $L_1, \ldots, L_n$ are regular.*
- *If $L_1 \times \ldots \times L_i \times \ldots \times L_n$ is regular, and $L_i' \subseteq L_i$ is regular, then $L_1 \times \ldots \times L_i' \times \ldots \times L_n$ is regular.*

Proof. See [26]. □

2.2.2 Automatic Presentations

We can now give the definition of an automatic presentation.

Definition 2.2.4. *Let $\mathcal{S} = (S, R_1, \ldots, R_n)$ be a relational structure.*

Let L be a regular language over an alphabet Σ, with a surjective map $\phi : L \to S$.

(L, ϕ) is an automatic presentation *for $\mathcal{S}$ if:*

- *$L_= = \{(w_1, w_2) \in L^2 : \phi(w_1) = \phi(w_2)\}$ is regular, and*

- *for each R_i, arity r_i,*

$$L_{R_i} = \{(w_1, w_2, \ldots, w_{r_i}) \in L^{r_i} : R(\phi(w_1), \ldots, \phi(w_{r_i}))\}$$

is regular.

If ϕ is also injective then the presentation is called *injective.* If Σ contains precisely two elements, then the presentation is called *binary.* These two restrictions are, in fact, not restrictive at all:

Proposition 2.2.5 (Blumensath, Gradël [7]; Khoussainov, Nerode [42]). *Let A be a structure with an automatic presentation; then:*

- *A has a binary automatic presentation.*
- *A has an injective automatic presentation.*

Moreover, they may be effectively constructed.

Remark 2.2.6. The proof in [42] that if we have an automatic presentation then we have an injective automatic presentation, uses the same alphabet and constructs a subset of the initial language. We may, therefore, put the two parts of Proposition 2.2.5 together and say that every structure with an automatic presentation has an injective binary automatic presentation.

It seems appropriate to include an example to illuminate the definition; the following is simple, but instructive.

Example 2.2.7. Consider the structure $(\mathbb{N}, \geq)$, i.e. the natural numbers with the 'greater than or equals' relation.

Let $L = \{1\}^\star$, and $\phi(1^n) = n$. This is an automatic presentation for $(\mathbb{N}, \geq)$, as:

- $L_= = \{(w_1, w_2) \in L^2 : \phi(w_1) = \phi(w_2)\} = \{(1, 1)\}^\star$, and

- $L_{R_i} = \{(w_1, w_2) \in L^2 : \phi(w_1) \geq \phi(w_2))\} = \{(1,1)\}^\star\{(1,\#)\}^\star$

are regular.

The following lemma bounds the size of structures that can have automatic presentations.

Lemma 2.2.8. *Let S be a structure:*

- *If S is finite, then S has an automatic presentation.*
- *If S has an automatic presentation, then S is countable.*

Proof. All finite languages are regular; all regular languages are countable.

□

These next examples are taken from [42]; see also [5, 68]. They give an idea of the range of structures known to have automatic presentations.

Proposition 2.2.9 (Khoussainov, Nerode). *The following have automatic presentations:*

- *Structures with only unary predicates;*
- $(\mathbb{Q}, <)$*;*
- *All ordinals ω^n, where $n < \omega$;*
- *Transition graphs of Turing machines;*
- $(\mathbb{Z}, +)$.

It is not difficult to construct examples of structures with automatic presentations. There is less known with regard to classifications of exactly when a member of a class of structures has such a presentation: we shall add to this in Chapter 3. In the meantime, the next theorems are most of the known classifications.

Theorem 2.2.10 (Khoussainov, Nies, Rubin, Stephan [43]). *An infinite Boolean algebra has an automatic presentation if and only if it is a finite product of copies of the Boolean algebra of finite and cofinite subsets of* $\mathbb{N}$.

Theorem 2.2.11 (Delhommé [19], see also [20]). *An ordinal* α *has an automatic presentation if and only if* $\alpha < \omega^{\omega}$.

2.3 Automatic Presentations and First-Order Logic

2.3.1 Decidability

Let $\mathcal{S}$ be a structure. When can we decide whether a first-order sentence is satisfied by $\mathcal{S}$? When, equivalently, can we decide (membership of) $\mathrm{Th}(\mathcal{S})$? There is no general answer to this question, but we will see in this section that having an automatic presentation is a sufficient condition.

The following theorem can be found in [42].

Theorem 2.3.1. *Let* $\mathcal{S}$ *be a structure with an automatic presentation; then, for every first-order formula* $\theta(x_1, \ldots, x_n)$ *over the structure there is an automaton which accepts* $(w_1, \ldots, w_n)$ *if and only if* $\mathcal{S} \models \theta(\phi(w_1), \ldots, \phi(w_n))$. *Moreover, this automaton may be effectively constructed.*

Proof. We can assume, by Proposition 2.2.5, that the automatic presentation for $\mathcal{S}$ is injective. The proof goes by induction on the complexity of $\theta(x_1, \ldots, x_n)$:

- If $\theta(x_1, \ldots, x_n)$ is an atomic formula:

  An atomic formula is either of the form $s = t$, with s and t variables, or $R(y_1, \ldots, y_n)$, with $y_1, \ldots, y_n$ variables. Take the automaton for, respectively, equality, or the relation R in S; replace with an equivalent deterministic and complete automaton, which exists by Proposition 2.2.1.

Assume $\theta(x_1, \ldots, x_n) := R(y_1, \ldots, y_m)$, where $y_i = x_j$ for some (not necessarily distinct) $j \leq n$. Note that, as we are considering only relational structures, we need not account for any of the y_i being a constant.

For each member $(p, (a_1, \ldots, a_m), q)$ of the transition relation of the automaton,

$$\text{if for any } j, k \text{ with } j < k \text{ we have } y_j = y_k \text{ but } a_j \neq a_k$$

then remove this tuple from the relation. As we are assuming the presentation to be injective, the differing symbols denote differing elements.

Now, for all j, k with $j < k$,

$$\text{if } y_j = y_k \text{ and } a_j = a_k$$

then replace this tuple with $(p, (a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_m), q)$. As all tuples will all have either been removed, or reduced in length to n, we have a well-defined automaton over an alphabet of n-tuples.

Finally, permute the a_i so that if $y_i = x_j$, then a_i is in position j. By construction, this will merely reorder the a_i. Similarly for $\theta(x_1, \ldots, x_n) := y_1 = y_2$.

- If $\theta(x_1, \ldots, x_n) := \psi(x_{i_1}, \ldots, x_{i_u}) \vee \overline{\psi}(x_{j_1}, \ldots, x_{j_v})$:

Take the automata for ψ and $\overline{\psi}$; replace with equivalent deterministic and complete automata, which exist by Proposition 2.2.1.

First, consider ψ.

For each $(p, (a_{i_1}, \ldots, a_{i_u}), q)$ in the transition relation, permute the a_{i_k} so that the i_k are in order.

Now, if there is an x_r such that $r \neq i_k$ for all k, replace each $(p, (a_{i_1}, \ldots, a_{i_u}), q)$ with

$$\{(p, (a_{i_1}, \ldots, a_{i_k}, a, a_{i_{k+1}}, \ldots), q) : a \in \Sigma \cup \{\#\}\}$$

where $i_k < r, i_{k+1} < r$. Now consider the resulting automaton. Repeat, for each remaining x_r such that $r \neq i_k$ for all k.

Repeat for $\overline{\psi}$, then form the automaton accepting the union of the two languages now accepted, as allowed by Proposition 2.2.2.

- If $\theta(x_1, \ldots, x_n) := \neg\psi(x_1, \ldots, x_n)$:

  Take the automaton for ψ; replace with an equivalent deterministic and complete automaton, which exists by Proposition 2.2.1.

  Now, if F is the set of finish states, replace F with $Q \setminus F$, where Q is the set of states.

- If $\theta(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) := \exists x_i \psi(x_1, \ldots, x_n)$:

  Take the automaton for ψ; replace with an equivalent deterministic and complete automaton, which exists by Proposition 2.2.1.

  Replace all members $(p, (a_1, \ldots, a_n), q)$ of the transition relation with $(p, (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), q)$.

  Now, if there is a sequence of transitions from some state s to an accept state, such that all transitions are of the form $(p, (\#, \ldots, \#), q)$, then add s to the set of final states.

  Remove from the transition relation any elements $(p, (\#, \ldots, \#), q)$.

□

Corollary 2.3.2. *Let $\mathcal{S} = (S, R_1, \ldots, R_n)$ be a structure that has an automatic presentation, and let X be a relation over $\mathcal{S}$ definable in first-order logic; then, $\overline{\mathcal{S}} = (S, R_1, \ldots, R_n, X)$ has an automatic presentation.*

The following result may also be found in [42].

Theorem 2.3.3. *Let $\mathcal{S}$ be a structure with an automatic presentation; then, Th($\mathcal{S}$) is decidable.*

Proof. Let θ be a sentence over $\mathcal{S}$. Without loss of generality, either $\theta := \exists x \psi(x)$ or $\theta := \forall x \psi(x)$.

Assume $\theta := \exists x \psi(x)$. Using Theorem 2.3.1, find an automaton for $\psi(x)$. Check if this automaton is non-empty - if so, θ is in Th($\mathcal{S}$), else not.

Assume $\theta := \forall x \psi(x)$. Using Theorem 2.3.1, find an automaton A for $\psi(x)$. Let A^S be the automaton accepting the language of the presentation of $\mathcal{S}$. Form the automaton accepting $L(A^S) \setminus L(A)$, which exists by Proposition 2.2.2. Check if this automaton is empty - if so, θ is in Th($\mathcal{S}$), else not. □

This theorem has actually been extended to include some counting quantifiers. Let $\exists^{\infty} x \phi(x)$ be satisfied if there exists infinitely many elements satisfying $\phi(x)$. Let $\exists^{(m,n)} x \phi(x)$ be satisfied if there exists m modulo n many elements satisfying $\phi(x)$. Let $\mathrm{Th}^C(\mathcal{S})$ represent Th($\mathcal{S}$) supplemented with sentences containing these quantifiers.

Proposition 2.3.4 (Blumensath [5]; Rubin [68]). *Let $\mathcal{S}$ be a structure with an automatic presentation; then, $Th^C(\mathcal{S})$ is decidable.*

2.3.2 Interpretations and Automatic Presentations

Proposition 2.3.5 (Blumensath). *Let $\mathcal{S}$ and $\mathcal{T}$ be structures. Assume $\mathcal{S}$ has an automatic presentation, and assume there is an interpretation of $\mathcal{T}$ in $\mathcal{S}$; then, $\mathcal{T}$ has an automatic presentation.*

Sketch Proof. Using Theorem 2.3.1, we can construct automata corresponding to the first-order formulas defining the interpretation. These new automata guarantee an automatic presentation for $\mathcal{T}$. □

The following is noted in [5] (Corollary 3.14).

Corollary 2.3.6. *The class of structures with automatic presentations is closed under:*

- *direct products;*
- *quotients by first-order definable congruences; and*
- *first-order definable substructures.*

Moreover, in each case an automatic presentation is effectively constructable.

Proposition 2.3.5 gives the basis for a logical characterisation of structures with automatic presentations, see [5, 68]:

Theorem 2.3.7 (Blumensath). *A structure has an automatic presentation if and only if it is interpretable in:*

- $(\{0,1\}^\star, (\sigma_x)_{x\in\Sigma}, \preceq, l)$*; or equivalently,*
- $(\mathbb{N}, +, |_2)$

where

$$\sigma_x(w) = wx, u \preceq v := \exists w(uw = v), l(u,v) := |u| = |v|$$

$$x|_2 y := (\exists n)x = 2^n \wedge (\exists m)y = mx.$$

Remark 2.3.8. The finite word automata in the definition of automatic presentations can, of course, be replaced by other types of automata. This idea has been considered in [5], where tree, infinite word, and infinite tree automata are considered. The motivation for considering these automata is that for each of these types Theorem 2.3.3 generalises, and there is an equivalent to Theorem 2.3.7. For more on infinite word automata presentations, see [48].

2.4 Groups and Semigroups

Let $\tau = \{\circ\}$ be a signature consisting solely of a symbol for a binary operation. Let $\mathcal{S}$ be a τ-structure. If the function for $\circ$ in $\mathcal{S}$ is *associative*, i.e. if for all $x, y, z \in S$

$$(x \circ y) \circ z = x \circ (y \circ z)$$

then $\mathcal{S}$ is a *semigroup*.

Example 2.4.1. The following are standard examples of semigroups.

- $\mathcal{S} = (\mathbb{N}, \circ^{\mathcal{S}})$, where $\circ^{\mathcal{S}}$ is the addition operation $+$.
- $\mathcal{S} = (X^\star, \circ^{\mathcal{S}})$, where $\circ^{\mathcal{S}}$ is concatenation.

To simplify the following, we shall relax some of the notation: S will be used to denote either S or $\mathcal{S}$, $\circ$ and $\circ^{S}$ may be replaced by the usual symbol for the context or removed entirely (particularly in the case of concatenation), and we shall refer to $\circ$ as both the symbol and the function it represents.

Also, in future chapters, we may also drop $\circ$, just concatenating instead. It should be clear that associativity allows us to unambiguously avoid the use of brackets, and we shall use this throughout.

Lemma 2.4.2. *Assume S contains an element i such that for all $x \in S$*

$$x \circ i = i \circ x = x.$$

Then, this element will be unique.

Proof. Assume S also contains an element $j \neq i$ such that for all $x \in S$

$$x \circ j = j \circ x = x.$$

Then,

$$j = j \circ i = i.$$

□

Such an element is called the *identity* element for the semigroup. The identity for a semigroup will be denoted i_S, or i if there is no chance of confusion. A semigroup containing an identity element is called a *monoid.*

Lemma 2.4.3. *Assume that for an element $x \in S$, there is an element $y \in S$ such that*

$$x \circ y = y \circ x = i.$$

Then, this element will be unique for x.

Proof. Assume that for an element $x \in S$, there is also an element $\bar{y} \in S, \bar{y} \neq y$ such that

$$x \circ \bar{y} = \bar{y} \circ x = i.$$

Then,

$$\bar{y} = \bar{y} \circ i = \bar{y} \circ x \circ y = i \circ y = y.$$

□

This element is called the *inverse* of x. The inverse of x will be denoted x^{-1}. A monoid containing an inverse for *every* element is called a *group*.

When referring to monoids, we will often implicitly use the signature $\{\circ, i\}$ with the constant symbol i corresponding to the identity element.

When referring to groups, we will often implicitly use the signature $\{\circ, i, ^{-1}\}$ with the unary function symbol $^{-1}$ corresponding to the function taking an element to its inverse.

Example 2.4.4. The following are standard examples of groups.

- $S = (\mathbb{Z}, +)$;
- $S = (Aut(X), \circ)$, where X is some structure, $Aut(X)$ is the set of automorphisms of X, and $\circ$ is function composition.

Let S be a semigroup (we include the possibility that S may be a monoid, or even a group). Let T be a subset of S. If T is closed under the function $\circ$, i.e.

$$x, y \in T \Rightarrow x \circ y \in T$$

then T is called a *subsemigroup* of S - in particular, associativity will be preserved. If T contains an identity element, T is called a *submonoid* of S; if T contains an inverse for every element in T, T is called a *subgroup* of S. We denote any of these containments as $T \leq S$.

A *homomorphism* is, intuitively, a map between structures that preserves shared relations. In this context we shall have:

Definition 2.4.5. • *A map ϕ from a semigroup $(S, \circ)$ to a semigroup $(T, \bullet)$ is a* semigroup homomorphism *if $\phi(s \circ t) = \phi(s) \bullet \phi(t)$ for all $s, t \in S$.*

- *A map ϕ from a monoid $(S, \circ, i)$ to a monoid $(T, \bullet, j)$ is a* monoid homomorphism *if it is a semigroup homomorphism and $\phi(i) = j$*

- *A map ϕ from a group $(S, \circ, i, ^{-1})$ to a group $(T, \bullet, j, ^{v})$ is a* group homomorphism *if it is a monoid homomorphism and, for all $s \in S$, $\phi(s^{-1}) = \phi(s)^{v}$. (This last requirement is actually redundant, but included for clarity.)*

We will often call these just homomorphisms *if the context is clear.*

A bijective homomorphism is called an *isomorphism*; if there is an isomorphism between two semigroups S and T, they are said to be *isomorphic*, denoted $S \cong T$. If two structures are isomorphic they are usually, at least algebraically, treated as being the same structure.

Definition 2.4.6. *Let $(S, \circ)$ and $(T, \bullet)$ be semigroups. The* direct product *of S and T is the semigroup $(S \times T, \diamond)$, where:*

$$(s, t) \diamond (s', t') = (s \circ s', t \bullet t').$$

Note that the direct product of two monoids is a monoid, and the direct product of two groups is a group.

Definition 2.4.7. *Let S be a semigroup. Let $X \subseteq S$ be a finite set. Assume that, for all $s \in S$, there exists*

$$x_1, x_2, \ldots, x_n \in X$$

such that

$$s = x_1 x_2 \ldots x_n.$$

Then, X is called a finite generating set *for S.*

If $|X| = 1$, S is called cyclic *(or often, except for groups,* monogenic*).*

Definition 2.4.8. *Let G be a group. Let $X \subseteq G$ be a finite set.*

- *If $X \cup X^{-1}$ is a finite generating set for G, then we also call X a finite generating set for G.*
- *If X is a finite generating set for G, and $X^{-1} \subseteq X$, X is* closed under inverses.

Proposition 2.4.9. *Let S be a semigroup. Let $X \subseteq S$ be a finite set. Let $T = \{x_1 \circ x_2 \circ \ldots \circ x_n : n \in \mathbb{N}, x_i \in X\}$; then, T is a subsemigroup of S.*

Proof. Let $x_1 \circ x_2 \circ \ldots \circ x_i$ and $x'_1 \circ x'_2 \circ \ldots \circ x'_j$ be elements of T.

$$(x_1 \circ x_2 \circ \ldots \circ x_i) \circ (x'_1 \circ x'_2 \circ \ldots \circ x'_j) = x_1 \circ x_2 \circ \ldots \circ x_i \circ x'_1 \circ x'_2 \circ \ldots \circ x'_j \in T.$$

□

Let $X = \{x_1, \ldots, x_n\}$. We will denote T by $\langle x_1, \ldots, x_n \rangle_S$ (S for semigroup).

Proposition 2.4.10. *Let G be a group. Let $X \subseteq G$ be a finite set. Let $H = \{x_1 \circ x_2 \circ \ldots \circ x_n : n \in \mathbb{N}, x_i \in X \cup X^{-1}\}$; then, H is a subgroup of G.*

Proof. H is a subsemigroup by the previous proposition. $x_1 \circ x_1^{-1} = 1$ is in H, so H is a submonoid.

Let $x_1 \circ x_2 \circ \ldots \circ x_n \in H$. $(x_1 \circ x_2 \circ \ldots \circ x_n)^{-1} = x_n^{-1} \circ \ldots \circ x_2^{-1} \circ x_1^{-1}$, and as $(x_i^{-1})^{-1} = x_i$, $x_n^{-1} \circ \ldots \circ x_2^{-1} \circ x_1^{-1} \in H$. □

Let $X = \{x_1, \ldots, x_n\}$. We will denote H by $\langle x_1, \ldots, x_n \rangle_G$ (G for group). In general, if it is clear whether we are talking about a semigroup or a group, we shall just use $\langle x_1, \ldots, x_n \rangle$.

2.4.1 Presentations

Definition 2.4.11. *Let $\sim$ be a relation on a semigroup S. If $\sim$ is an equivalence relation, and $\sim$ satisfies for all $a, b \in S$:*

$$a \sim b \Rightarrow \forall s \in S, s \circ a \sim s \circ b \text{ and } a \circ s \sim b \circ s$$

then $\sim$ is called a congruence *on S.*

Let X be a set, and let $\bar{X} = X^+$ (or, respectively, $X^\star$), the set of all words over X (excluding or, respectively, not including λ). Let $R \subseteq \bar{X} \times \bar{X}$ be a subset of pairs of words over X. Define a relation on $\bar{X}$ as follows:

$$u \sim v \Leftrightarrow \exists w, w' \in \bar{X}, \exists (s,t) \in R, u = wsw' \text{ and } v = wtw'$$

Now, let $\sim_R$ be the congruence generated by R, that is, the intersection of all congruences on $\bar{X}$ containing $\sim$.

Let $[X]$ be the set of equivalence classes of $\bar{X}$ under $\sim_R$. Define a semigroup on this set:

$$[u]_{\sim_R} \circ [v]_{\sim_R} = [uv]_{\sim_R}$$

We will denote this semigroup by

$$\langle X : s = t, (s,t) \in R \rangle,$$

assuming $\bar{X} = X^+$ unless there is an s or t equal to λ.

Theorem 2.4.12. *For every semigroup S, there exists X, and $R \subseteq X^\star \times X^\star$, such that:*

$$S \cong \langle X : s = t, (s,t) \in R \rangle.$$

This is called a presentation *of S.*

For more information on this construction see Section 1.6 of [41].

Example 2.4.13. The bicyclic monoid arises in many contexts within semigroup theory. It has the following presentation:

$$\langle a,\ b:\ ab = \lambda \rangle.$$

That is, elements of this semigroup consist of a string of b symbols, followed by a string of a symbols. Composition is given by

$$b^i a^j \circ b^k a^l = \begin{cases} b^i a^{l+(j-k)} & \text{if } j \geq k \\ b^{i+(k-j)} a^l & \text{if } j < k \end{cases}.$$

2.4.2 Groups

A group G is *abelian* (or *commutative*), if for all $g, g' \in G$

$$g \circ g' = g' \circ g.$$

The *order of an element* $g \in G$ is the smallest n such that $g^n = 1$. The *order of a group* G is the number of elements in G, denoted $|G|$.

We will need the following result later on:

Proposition 2.4.14. *Let G and H be finite abelian groups, and assume G and H have the same number of elements of each order; then $G \cong H$.*

To give an idea of the proof, we need the following definitions and results.

Definition 2.4.15. *Let G be a group, and let p be a prime number.*

A p-subgroup *of G is a subgroup of G all of whose elements have order a power of p.*

A Sylow p-subgroup *of G is a p-subgroup of G which is not strictly contained in any other p-subgroup of G.*

Proposition 2.4.16 (Sylow). *Let G be a group, and let p be a prime number dividing $|G|$. There exists a Sylow p-subgroup of G, and all such subgroups are isomorphic. Further more, G is a direct product of its Sylow subgroups.*

Proof. See [66]. □

The proof of Proposition 2.4.14 is as follows.

Proof. By the assumption, G and H have the same number of elements; as such, we proceed by induction on this number.

The statement is clearly true for groups of order 2 and 3, so suppose that G and H are groups of order greater than 3, and that the statement holds for all groups of lower order. Let p be a prime number dividing $|G|$, and let G_p and H_p be the Sylow p-subgroups of G and H respectively.

Since the Sylow p-subgroups contain all elements of order a power of p, the induction hypothesis applies to G_p and H_p. If we can show that $G_p \cong H_p$ for all p dividing $|G|$, then it will follow that $G \cong H$, since G and H are direct products of their Sylow subgroups.

Let $x \in G_p$, with maximal order $q = p^m$; then $\langle x \rangle$, the group generated by x, is a direct factor of G_p, so there is a subgroup G' with $G_p = \langle x \rangle \times G'$. Similarly, we have $H_p =< y > \times H'$, where y has the same order as x.

Now, consider the subgroups $\langle x^p \rangle \times G'$ and $\langle y^p \rangle \times H'$ of, respectively, G_p and H_p. Each of these subgroups is constructed by removing elements of the form (x^k, g'), where x^k has order q and g' is any element in G'. Because x has maximal order in a p-subgroup, in each case the order of g' is a divisor of q, and so (x^k, g') has order q since the order of an element in a direct product is the least common multiple of the orders of the components. Thus to construct each of these subgroups, we have removed $(p^m - p^{m-1}) \times |G'|$ elements, each having order q. It follows from the hypothesis that we are left with the same number of elements of each order, and so the induction hypothesis implies that $\langle x^p \rangle \times G'$ and $\langle y^p \rangle \times H'$ are isomorphic. As such, G' and H' are isomorphic, and so $G_p \cong H_p$ as required.

For details of this proof, see [66]. $\square$

Let G be a group. Let H be a subgroup of G. Define:

$$Hg = \{h \circ g : h \in H\};$$

$$gH = \{g \circ h : h \in H\}.$$

Sets of this form are called (respectively *right*, *left*) *cosets* of H in G. Any two (respectively right, left) cosets are either equal or disjoint. As such, the set of all (respectively right, left) cosets of a subgroup partitions the group.

If for every $g \in G$ we have $Hg = gH$, then H is a *normal* subgroup of G. Normal subgroups play a fundamental role in group theory, only part of which we draw out here. Note that for normal subgroups there is no distinction between right and left cosets, so we shall just refer to cosets. Consider two cosets of a subgroup H in G, say Hg and $H\bar{g}$. We can define a product:

$$Hg \bullet H\bar{g} = H(g \circ \bar{g})$$

This product is well-defined when H is normal. It actually makes the set of cosets into a group - the identity is H, the inverse of Hg is Hg^{-1}. This group is denoted G/H, and called a *quotient* group. The number of cosets is called the *index* of H in G, and is denoted $[G : H]$. In particular, if there are only a finite number of cosets of H in G - that is, if $[G : H] < \infty$ - then H is said to have *finite index* in G. Let $R \subseteq G$ be a subset of G. If the cosets $\{Hr : r \in R\}$ are distinct, and $|R|$ is the index of H, then R is a set of *coset representatives* for H in G.

Let χ be a group property (such as being abelian). Then, a group G is said to be *virtually* (or *almost*) χ if G contains a subgroup of finite index with the property χ.

Let $\mathbb{Z}_i = \mathbb{Z}/i\mathbb{Z}$, where $i\mathbb{Z} = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z}, x = iy\}$.

Theorem 2.4.17 (Fundamental Theorem of Finitely Generated Abelian Groups [66]). *Let G be a finitely generated abelian group; then,*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_n},$$

where the k_i are (not necessarily distinct) powers of prime numbers.

Note that r is called the *torsion-free rank* of G.

Although groups, as semigroups, may have presentations as in Section 2.4.1, there is a more standard form. We need some general results first.

Definition 2.4.18. *If a (semi)group has a presentation of the form*

$$\langle x_1, \ldots, x_n, y_1, \ldots, y_n : x_i y_i = \lambda, y_i x_i = \lambda, i \in \{1, \ldots, n\}\rangle,$$

then it is called the free group on $\{x_1, \ldots, x_n\}$.

Remark 2.4.19. It should be clear in the above definition that the elements y_i act as the inverses of the x_i, and that, roughly, two words over the x_i and y_i are only equivalent if required to ensure the semigroup is a group.

Definition 2.4.20. *If H is a subgroup of a group G, then the* normal closure *of H is the intersection of all the normal subgroups containing H. This will also be a subgroup of G, denoted H^N.*

Now, let $X = \{x_1, \ldots, x_n\}$, and let F_X be the free group on X. Let R be a subset of F_X. We will denote the group $F_X/\langle R\rangle^N$ by $\langle X : R\rangle$.

Theorem 2.4.21. *For every group G, there exists X, and $R \subseteq F_X$, such that:*

$$G \cong \langle X : R \rangle.$$

This is called a presentation *of S.*

Remark 2.4.22. The members of R correspond to words from $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}^\star$. We will often denote a member of R as an equality $u = v$, which can be interpreted as the word uv^{-1} where v^{-1} is the word produced by reversing v and replacing x_i by y_i and y_j by x_j.

For more details on group presentations see Chapter 2 of [63].

2.4.3 Semigroups and Monoids

Although groups have been intensively studied in mathematics, there is also a growing body of work on semigroups and monoids. Here, we shall mention some definitions and results that will be of use to us. For a comprehensive introduction, see [41].

We begin by expanding on the section on presentations. Let S be a semigroup, and $\sim$ a congruence on S (Definition 2.4.11). Let $[s]_\sim$ denote the equivalence class of $s \in S$ under $\sim$. As before, these classes may be combined as $[s]_\sim \circ [t]_\sim = [s \circ t]_\sim$. Denote this semigroup $S/\sim$.

Proposition 2.4.23. *Define $\phi : S \to S_\sim$ as $\phi(s) = [s]_\sim$.*

This map is a homomorphism.

Proof.

$$\phi(s) \circ \phi(s') = [s]_\sim \circ [s']_\sim = [s \circ s']_\sim = \phi(s \circ s').$$

□

The following definitions are a little scattered in topic, but will be useful later on.

A semigroup S is *commutative* if for all $s, s' \in S$

$$s \circ s' = s' \circ s.$$

Definition 2.4.24. *Let S be a semigroup, $T \leq S$ a subsemigroup.*

We call T

- *a* left ideal *if for all $s \in S, t \in T$, $s \circ t \in T$,*
- *a* right ideal *if for all $s \in S, t \in T$, $t \circ s \in T$, and*
- *an* ideal *if T is both a left and right ideal.*

If x is an element of S, then the smallest left (respectively right) ideal containing x in S is $Sx \cup \{x\}$ (respectively $xS \cup \{x\}$). This is called the principal left (respectively right) ideal generated by *x.*

We can now present the beginnings of the theory of Green's equivalences: again, about as much as will be useful later on.

Definition 2.4.25. *Let S be a semigroup, $x, y \in S$.*

- *$x\mathcal{L}y$ if and only if x and y generate the same principal left ideal.*
- *$x\mathcal{R}y$ if and only if x and y generate the same principal right ideal.*
- *$x\mathcal{H}y$ if and only if $x\mathcal{L}y$ and $x\mathcal{R}y$.*

Considering equivalence classes, the $\mathcal{L}$-class (respectively $\mathcal{R}$-class, $\mathcal{H}$-class) containing an element x will be denoted L_x (respectively R_x, H_x).

Remark 2.4.26. It should be noted that these equivalences are just the universal equivalence when considered on groups. For more details on these equivalences, see [41].

Chapter 3

Groups

This chapter contains the main result of this thesis: a classification of those finitely generated groups with automatic presentations (Theorem 3.4.5). A version of part of this chapter forms the main part of [61].

3.1 The Signature for Groups

Before presenting the results on groups with automatic presentations, it is worthwhile commenting on the appropriate signature for groups. Groups are usually defined as having a single binary operation, which satisfies certain properties. From a mathematical logic point of view, however, it would be more usual to explicitly include a symbol for both the identity element and the inverse operation. Is either 'correct'? The answer depends on how you are considering the structures. As noted in [36], the main difference is that of substructures: the substructures of groups as structures $(G, \circ)$ need only be subsemigroups, whereas, with $(G, \circ, i, {}^{-1})$, they must be subgroups. For our purposes, we needn't be too worried by this distinction. It is clear that, for the structure $(G, \circ)$, the properties of having an identity and having inverses are both first-order definable; so, if a group as structure $(G, \circ)$ has an automatic presentation, then (as in Proposition 2.3.2) this same presentation may be expanded to one for the structure $(G, \circ, i, {}^{-1})$. With this in mind, we need only concentrate on $(G, \circ)$ in what follows.

3.2 Known Results and Virtually Abelian Groups

The following results, from [42], sum up much of what was previously known concerning finitely generated groups with automatic presentations:

Proposition 3.2.1 (Khoussainov and Nerode [42]). *$\mathbb{Z}$ has an automatic presentation.*

Proof. Although we could construct automata, it is simpler to give an interpretation of $(\mathbb{Z}, +)$ in $(\mathbb{N}, +, |_2)$. The result then follows from Theorem 2.3.7.

The interpretation is 2-dimensional.

- The domain formula is just $\phi(x_1, x_2) := x_1 = x_1$, i.e. a tautology, so we are using all pairs of elements of $\mathbb{N}$.
- The co-ordinate map is $f(x_1, x_2) = x_1 - x_2$.
- Equality is $\theta_=(x_1, x_2; y_1, y_2) := x_1 + y_2 = y_1 + x_2$, as

$$\begin{array}{rrcl} & f(x_1, x_2) & = & f(y_1, y_2) \\ \Leftrightarrow & x_1 - x_2 & = & y_1 - y_2 \\ \Leftrightarrow & x_1 + y_2 & = & y_1 + x_2. \end{array}$$

- The product $+$ is $\theta_+(x_1, x_2; y_1, y_2; z_1, z_2) := (x_1+y_1)+z_2 = (x_2+y_2)+z_1$, as

$$\begin{aligned} & f(x_1, x_2) + f(y_1, y_2) &=& f(z_1, z_2) \\ \Leftrightarrow\ & (x_1 - x_2) + (y_1 - y_2) &=& z_1 - z_2 \\ \Leftrightarrow\ & (x_1 + y_1) - (x_2 + y_2) &=& z_1 - z_2 \\ \Leftrightarrow\ & (x_1 + y_1) + z_2 &=& (x_2 + y_2) + z_1. \end{aligned}$$

$\square$

Remark 3.2.2. Note that in the previous proof the relation $|_2$ is not used, so this is equally an interpretation of $(\mathbb{Z}, +)$ in $(\mathbb{N}, +)$.

Proposition 3.2.3 (Khoussainov and Nerode[42]). *Finitely generated abelian groups have automatic presentations.*

Proof. All finitely generated abelian groups are direct products of a finite number of copies of $(\mathbb{Z}, +)$ and a finite number of finite abelian groups (see [66]). All finite structures have automatic presentations (Lemma 2.2.8), as does $(\mathbb{Z}, +)$, and having an automatic presentation is closed under direct products (Corollary 2.3.6): as such, the result follows immediately. $\square$

We will now extend this result a little.

Theorem 3.2.4. *Finitely generated virtually abelian groups have automatic presentations.*

Proof. Let G be a finitely generated group with an abelian subgroup A of finite index; then, G is interpretable in A (see [3], for example). The result follows from Propositions 2.3.5 and 3.2.3. $\square$

Remark 3.2.5. Suppose that G is a finitely generated virtually abelian group, so that G has an abelian subgroup A of finite index. Then A is finitely generated and hence is a direct product $C_1 \times C_2 \times \ldots \times C_k$ of cyclic groups. If we consider the subgroup B of A generated by the infinite groups C_i (i.e. ignore the C_i which are finite cyclic groups), then B has finite index in A, and hence has finite index in G.

Now B is a free abelian group isomorphic to $\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ for some n; so, every finitely generated virtually abelian group has a free abelian subgroup of finite index. Moreover, if H is a subgroup of finite index in a group G, then there is a normal subgroup N of G contained in H with N also of finite index in G. As a subgroup of a free abelian group is free abelian, we have that every finitely generated virtually abelian group has a normal free abelian subgroup of finite index. $\square$

Remark 3.2.6. It is possible to prove Theorem 3.2.4 directly by constructing appropriate automata. An outline of the proof is given here - for full details, see the Appendix.

Let G be a finitely generated virtually abelian group. As in Remark 3.2.5, let $A = \langle x_1, x_2, \ldots, x_n \rangle$ be a normal subgroup of G of finite index isomorphic to $\mathbb{Z}^n$ and then let $T = \{t_1, t_2, \ldots, t_k\}$ be a set of coset representatives for A in G.

Any element g of G can be expressed in the form $t_j a$ with $a \in A$, and then a can be written in the form $x_1^{\epsilon_1 m_1} x_2^{\epsilon_2 m_2} \ldots x_n^{\epsilon_n m_n}$ with $\epsilon_i \in \{1, -1\}$ and $m_i \in \mathbb{N}$ (if $m_i = 0$ we take $\epsilon_i = 1$). We then represent g as

$$t_j\,(\epsilon_1, \epsilon_2, \ldots, \epsilon_n)\,\mathrm{conv}(\overline{m_1}, \overline{m_2}, \ldots, \overline{m_n})$$

where $\overline{m_i}$ is the representation of m_i in binary notation. The language representing G is clearly regular. We now need to ensure that equality and composition are regular. Equality is clear, so we turn to composition. Since A is normal in G, each $x_i t_j$ is of the form $t_j x_1^{u_{1,i,j}} x_2^{u_{2,i,j}} \dots x_n^{u_{n,i,j}}$ for some $u_{h,i,j} \in \mathbb{Z}$; so the product in G is given by

$$\begin{aligned} t_i x_1^{a_1} \dots x_n^{a_n} . t_j x_1^{b_1} \dots x_n^{b_n} &= t_i t_j x_1^{a'_1} \dots x_n^{a'_n} x_1^{b_1} \dots x_n^{b_n} \\ &= t_i t_j x_1^{a'_1 + b_1} \dots x_n^{a'_n + b_n}. \end{aligned}$$

where

$$a'_i = \sum_{k=1}^{n} a_k u_{i,k,j}.$$

Now let t_k and $c_1, c_2, \dots, c_n$ be such that $t_i t_j = t_k x_1^{c_1} \dots x_n^{c_n}$; then

$$\begin{aligned} t_i t_j x_1^{a'_1 + b_1} \dots x_n^{a'_n + b_n} &= (t_k x_1^{c_1} \dots x_n^{c_n}) x_1^{a'_1 + b_1} \dots x_n^{a'_n + b_n} \\ &= t_k x_1^{a'_1 + b_1 + c_1} \dots x_n^{a'_n + b_n + c_n}. \end{aligned}$$

Given all this, we can now show that it is possible to construct an automaton corresponding to the product. We first create different transitions in our automaton for each possible pair of t_i's, and then, from these different transitions, for each possible combination of values of the ϵ_i. Then, based on the binary addition of n-tuples and taking into account the $u_{1,i,j}$ and c_i, we construct the rest of the automaton. The states, roughly, represent the current value of the carry in the addition. As the total amount carried at each stage is bounded by $n - 1$ we have a finite automaton. □

3.3 Growth

Currently, there are not many techniques for showing that a structure does *not* have an automatic presentation. One such method follows from decidability: if the first-order theory $\mathrm{Th}(\mathcal{S})$ of a structure $\mathcal{S}$ is undecidable then it cannot have an automatic presentation (by Theorem 2.3.3). For further conditions, see e.g. [43, 46, 67].

The other main method involves growth. Let S be a structure that has an automatic presentation, and fix one such presentation that is injective (guaranteed by Proposition 2.2.5). Then, for $x \in S$, let $l(x)$ denote the length of the word representing x in this presentation. We have the following result from [5]:

Theorem 3.3.1. *Let $f : S^n \to S$ be a first-order definable function on $\mathcal{S}$; then there exists a constant $N \in \mathbb{N}$ such that, for all $\overline{x} \in S^n$,*

$$l(f(\overline{x})) \leqslant max\{l(x_0), \dots, l(x_{n-1})\} + N.$$

In particular, this result has the following consequence for groups:

Corollary 3.3.2. *Let G be a group with an injective automatic presentation; then there is a constant N such that, for all $g_0, g_1 \in G$,*

$$l(g_0 g_1) \leqslant max\{l(g_0),\ l(g_1)\} + N.$$

There is a corresponding notion of growth in group theory. Let G be a group with a finite generating set X, and assume that X is closed under inverses. Now let $\delta(g)$ be the minimum $n \in \mathbb{N}$ such that

$$g = a_1 a_2 \dots a_n,\ a_i \in X.$$

The *growth function* of G is then defined to be

$$\gamma(n) = |\{g \in G : \delta(g) \leqslant n\}|.$$

The asymptotic nature of this function (in the sense of its being bounded above by a polynomial function, or below by an exponential function, or neither of these), is independent of which particular finite generating set we choose - see [32]. As such, the nature of the growth function is a property solely of the group (as opposed to the group together with a generating set). In the three cases we have mentioned, the group is said to have (respectively) *polynomial growth*, *exponential growth* or *intermediate growth*; see [32] for a survey on growth in groups. We now prove the following result:

Theorem 3.3.3. *If a finitely generated group G has an automatic presentation then G has polynomial growth.*

Before we do this, we first prove a useful proposition:

Proposition 3.3.4. *With notation as above, let $R = max\{l(a) : a \in X\}$; then there is a constant N such that, for all $m \geqslant 1$, we have*

$$\max\{l(a_1 \dots a_m) : a_i \in X\} \leqslant R + \lceil \log_2 m \rceil N.$$

Proof. Let N be the constant of Corollary 3.3.2. We proceed by induction on m.

We first consider the case $m = 1$. Here we clearly have

$$\max\{l(a_1) : a_1 \in X\} = R = R + \lceil \log_2 1 \rceil N.$$

Now assume the result holds for $1 \leqslant m \leqslant k$. We split our proof into two cases.

Case one: k is odd, say $k = 2r - 1$. Then, using Corollary 3.3.2, we have

$$\begin{aligned}
\max\{l(a_1 \dots a_{k+1}) : a_i \in X\} &= \max\{l(a_1 \dots a_{2r}) : a_i \in X\} \\
&\leqslant \max\{l(a_1 \dots a_r),\ l(a_{r+1} \dots a_{2r}) : a_i \in X\} + N \\
&\leqslant \max\{R + \lceil \log_2 r \rceil N,\ R + \lceil \log_2 r \rceil N\} + N \\
&= R + \lceil \log_2 r \rceil N + N \\
&= R + (\lceil \log_2 r + 1 \rceil) N \\
&= R + \lceil \log_2 r + \log_2 2 \rceil N \\
&= R + \lceil \log_2 2r \rceil N \\
&= R + \lceil \log_2 (k+1) \rceil N
\end{aligned}$$

as required.

Case two: k is even, say $k = 2r$. This time we have

$$\begin{aligned}
\max\{l(a_1 \dots a_{k+1}) : a_i \in X\} &= \max\{l(a_1 \dots a_{2r+1}) : a_i \in X\} \\
&\leqslant \max\{l(a_1 \dots a_r),\ l(a_{r+1} \dots a_{2r+1}) : a_i \in X\} + N \\
&\leqslant \max\{R + \lceil \log_2 r \rceil N,\ R + \lceil \log_2 (r+1) \rceil N\} + N \\
&= R + \lceil \log_2 (r+1) \rceil N + N.
\end{aligned}$$

Now, we can not proceed quite as easily as before: we split our consideration of this case into two subcases.

Subcase one: r is not of the form 2^x with $x \geqslant 1$.

The function $\lceil \log_2 y \rceil$ on $\{y \in \mathbb{N} : y > 0\}$ takes the same value on y and $y + 1$ except when y is of the form 2^x; so, if $r \neq 2^x$, then

$$\lceil \log_2 (r+1) \rceil = \lceil \log_2 r \rceil.$$

This gives

$$\begin{aligned}
R + \lceil \log_2(r+1) \rceil N + N &= R + \lceil \log_2 r \rceil N + N \\
&= R + \lceil \log_2 r + 1 \rceil N \\
&= R + \lceil \log_2 r + \log_2 2 \rceil N \\
&= R + \lceil \log_2 2r \rceil N \\
&= R + \lceil \log_2(2r+1) \rceil N \\
&= R + \lceil \log_2(k+1) \rceil N.
\end{aligned}$$

Subcase two: $r = 2^x$ $(x \geqslant 1)$.

Note first that

$$\begin{aligned}
\lceil \log_2(k+1) \rceil &= \lceil \log_2(2r+1) \rceil \\
&= \lceil \log_2(2.2^x+1) \rceil \\
&= \lceil \log_2(2^{x+1}+1) \rceil \\
&= x+2.
\end{aligned}$$

Now

$$\begin{aligned}
R + \lceil \log_2(r+1) \rceil N + N &= R + \lceil \log_2(r+1) + 1 \rceil N \\
&= R + \lceil \log_2(r+1) + \log_2 2 \rceil N \\
&= R + \lceil \log_2 2(r+1) \rceil N \\
&= R + \lceil \log_2 2(2^x+1) \rceil N \\
&= R + \lceil \log_2(2^{x+1}+2) \rceil N \\
&= R + (x+2)N \\
&= R + \lceil \log_2(k+1) \rceil N
\end{aligned}$$

as required. $\square$

Given Proposition 3.3.4, we can now prove Theorem 3.3.3:

Proof. By Remark 2.2.6 we may assume that the presentation for G is injective and binary. Then, as

$$\max\{l(a_1 \dots a_m) : a_i \in X\} \leqslant R + \lceil \log_2 m \rceil N$$

by Proposition 3.3.4, the number of possible words for elements of the form $a_1 \dots a_m$ is

$$\begin{aligned} 2^{R+\lceil \log_2 m \rceil N} &= 2^R (2^{\lceil \log_2 m \rceil})^N \\ &\leqslant 2^R (2^{\log_2 m + 1})^N \\ &= 2^R 2^N (2^{\log_2 m})^N \\ &= k m^N \end{aligned}$$

where $k = 2^R 2^N$ is a constant. So we have at most km^N possible elements g in G with $\delta(g) = m$; as a result, we have

$$\begin{aligned} \gamma(n) &= |\{g \in G : \delta(g) \leqslant n\}| \\ &\leqslant k.1^N + k.2^N + \dots + k.n^N \\ &\leqslant k.n^{N+1}. \end{aligned}$$

So G has polynomial growth as required. □

Corollary 3.3.5. *If a finitely generated semigroup S has an automatic presentation then S has polynomial growth.*

Proof. As there is no use of inverses in the proof, the definitions and proof clearly generalise to semigroups. □

3.4 Classification

We now quote two substantial known theorems that enable us to give a complete classification of those finitely generated groups that have an automatic presentation (to some extent solving a problem of [45]). We first need some more definitions from group theory; see [66] for more details.

If G is a group and if H and K are subsets of G, then we let $[H, K]$ denote the subgroup generated by the set of all elements of G of the form $h^{-1}k^{-1}hk$ with $h \in H$ and $k \in K$. If H and K are normal subgroups in G, then $[H, K]$ is a normal subgroup of G. We now define the following chains of normal subgroups of G:

$$\begin{array}{lll} G^{(0)} = G; & G^{(1)} = [G,G]; & G^{(2)} = [G^{(1)}, G^{(1)}]; \\ G^{(3)} = [G^{(2)}, G^{(2)}]; & \ldots\ldots & \end{array}$$

$$\begin{array}{lll} \gamma_0(G) = G; & \gamma_1(G) = [\gamma_0(G), G]; & \gamma_2(G) = [\gamma_1(G), G]; \\ \gamma_3(G) = [\gamma_2(G), G]; & \ldots\ldots & \end{array}$$

Note that $G \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \ldots$ and that $G \geqslant \gamma_1(G) \geqslant \gamma_2(G) \geqslant \ldots$. A group G is said to be *solvable* if $G^{(r)} = \{i\}$ for some $r \in \mathbb{N}$ and *nilpotent* if $\gamma_r(G) = \{i\}$ for some $r \in \mathbb{N}$; in the first case we call the smallest such r the *derived length* of G and, in the second case, the smallest such r is called the *nilpotency class* of G. Any nilpotent group is necessarily solvable - note that $G^{(k)}$ is contained in $\gamma_k(G)$, and so if $\gamma_r(G) = \{i\}$, so does $G^{(r)}$ - but the converse is false.

Given this, we can now state Gromov's classification [34] of groups with polynomial growth:

Theorem 3.4.1 (Gromov). *If a finitely generated group has polynomial growth then it is virtually nilpotent.*

At the beginning of Section 3.3 it was noted that there are currently two main methods for showing that a structure does not have an automatic presentation: decidability and growth. Having considered, for groups, growth, we now turn to decidability.

Perhaps the most well-used result concerning the first-order theory of groups is the following:

Proposition 3.4.2 (Mal'cev [54]). *Let G be the free nilpotent group of class two on two generators; then, the ring of integers $(\mathbb{Z}, +, \times)$ is interpretable in G.*

Corollary 3.4.3. *Let G be the free nilpotent group on two generators; then, G does not have an automatic presentation.*

Proof. The first-order theory of the ring of integers is undecidable, see for example [71]. □

Eršov, in [28], built on this proposition to show that a nilpotent group has decidable first-order theory if and only if it is virtually abelian. This was generalized by Romanovskiĭ, in [65], to virtually polycyclic groups and then by Noskov, who showed in [60] that a virtually solvable group has decidable first-order theory if and only if it is virtually abelian. The fact we need here is the following intermediate result, a corollary of Romanovskiĭ's result:

Theorem 3.4.4. *Let G be a finitely generated virtually nilpotent group with decidable first-order theory; then, G is virtually abelian.*

We can now combine these two powerful results, Theorem 3.4.1 and Theorem 3.4.4, with our result on growth (Theorem 3.3.3) to give:

Theorem 3.4.5 (Classification [61]). *Let G be a finitely generated group; then, G has an automatic presentation if and only if G is virtually abelian.*

Proof. Assume that G has an automatic presentation. By Theorem 3.3.3, G has polynomial growth, and so, by Theorem 3.4.1, G is virtually nilpotent. By Theorem 2.3.3, G has decidable first-order theory, and so, by Theorem 3.4.4, G is virtually abelian.

The converse is Theorem 3.2.4. □

3.5 The Isomorphism Problem

One of the fundamental algorithmic problems concerning standard semigroup presentations (Section 2.4.1) is the *isomorphism problem*: given two presentations, do they define isomorphic semigroups? It is clear that this problem also makes sense for the theory of automatic presentations: given two automatic presentations, do they represent isomorphic structures?

The problem is, in general, undecidable in both cases. For automatic presentations, there is in fact a stronger result. First, note that Σ_1^1 denotes sentences of arithmetic where the only second-order quantifiers are existential quantifiers over sets; it is a member of the analytical hierarchy. In particular, the superscript 1 denotes the arity of the relations quantified over, the subscript 1 denotes the number of blocks of quantifiers of the same type, and the Σ denotes that the first quantifier block is of existential quantifiers. Σ_1^1 may also be used to denote the class of algorithmic problems corresponding to deciding the satisfaction of members of Σ_1^1. For more information on this notation, see [64]. Second, given an algorithmic problem X, and a class of algorithmic problems χ, we say that X is χ-complete if every problem in χ can be reduced to an instance of X. We can now state the result.

Theorem 3.5.1 (Khoussainov, Nies, Rubin, Stephan [43]). *The complexity of the isomorphism problem for automatic presentations is Σ_1^1-complete.*

Restricting the class of structures under consideration can produce more manageable levels of complexity. In particular, the classification results mentioned earlier - for Boolean algebras and for ordinals - give decidability for these classes.

Remark 3.5.2. The isomorphism problem for a class χ of structures asks: given two automatic presentations of members *of class* χ, do they represent isomorphic members of χ?

Proposition 3.5.3. *The isomorphism problem for:*

- *Boolean algebras [43]; and*
- *ordinals [46],*

is decidable.

As we have now given a classification for finitely generated groups (Theorem 3.4.5), it is natural to ask whether this classification can also give us the corresponding isomorphism result. We have some preliminary results on this, beginning with results on finitely generated abelian groups.

Proposition 3.5.4. *Let A be an automatic presentation for a finitely generated abelian group G, and let*

$$G = \mathbb{Z}^r \times \mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_s} \times \ldots \times \mathbb{Z}_{k_n}$$

from Theorem 2.4.17. In particular, assume that $k_1, k_2, \ldots, k_s$ are all powers of 2, and that the k_t with $t > s$ are odd.

1. *The number of elements of order n in G is computable from A; and*
2. *The torsion-free rank of G is computable from A.*

Proof. (1) There are clearly only a finite number of elements of order n, and the set of such elements is first-order definable. We can assume that each element has a unique representative in the presentation (Proposition 2.2.5). As such, it is straightforward to construct the automaton for the definition (Theorem 2.3.1) and count the number of words accepted.

(2) Recall that the number of appearances of $\mathbb{Z}$, that is r, is the torsion-free rank of G.

The set G^2, i.e. $\{g \circ g : g \in G\}$, is a normal subgroup of G (as G is abelian) and is clearly first-order definable. As such, we can construct an automatic presentation for the set of equivalence classes G/G^2 (Corollary 2.3.6).

Now

$$G/G^2 = \mathbb{Z}_2^{r+s};$$

so

$$|G/G^2| = 2^{r+s}.$$

The elements of order 2 in G are in $\mathbb{Z}_{k_1} \times \ldots \times \mathbb{Z}_{k_s}$ - there are $2^s - 1$ of them. The first part of this proof allows us to calculate the number of elements of order 2, i.e. $2^s - 1$, leaving us with the torsion-free rank. □

We call a statement *semi-decidable* if there is a procedure that, when the statement is true, establishes this and terminates. Note that the procedure may not terminate otherwise.

Corollary 3.5.5. *Let A and A' be automatic presentations for finitely generated abelian groups G and G'. It is semi-decidable if G and G' are* not *isomorphic.*

Proof. By the previous proposition, the torsion-free ranks of the groups can be calculated: if they are different, the groups are not isomorphic.

So, assume that the torsion-free ranks of G and G' are the same.

Begin the following process:

For each $n \in \mathbb{N}$, calculate the number of elements of order n in G, and in G'. If the two groups are not isomorphic, then for some n the two numbers will be different by Proposition 2.4.14. $\square$

Remark 3.5.6. It is clear that the above process will not terminate if the groups *are* isomorphic. This is in sharp contrast to the situation when considering standard group presentations. There, deciding that two presentations represent groups that *are* isomorphic is semi-decidable - there is a process that will terminate if the groups are isomorphic, but no process that will terminate if they are not. The process that terminates if the groups are isomorphic involves enumerating the possible *Tietze transformations* of the presentation. The basic Tietze transformations involve either: adding a new generator symbol, defined from the existing ones; adding a new relation, defined from the existing ones; removing a generator symbol proved redundant by the relations; and, removing a relation proved redundant by the other relations. Note that none of these types of transformation changes the group represented by the presentation. It is possible to move between any two presentations of a group using some series of Tietze transformations. If we have a pair of group presentations, and we enumerate the possible transformations of one of them, then we will eventually reach the other - if the groups are isomorphic.

This leads to the question: is it possible to get from an automatic presentation of an abelian group to a standard presentation of the same group? If so, then we could strengthen Corollary 3.5.5 to say that given automatic presentations for two finitely generated abelian groups, it is decidable if they are isomorphic.

Alternatively, it may be possible to put a bound on the orders of elements in a group as a function of the size of the automata in an automatic presentation. This would enable us to convert the semi-decision procedure in Corollary 3.5.5 into a decision procedure.

Conjecture 3.5.7. *Let A and A' be automatic presentations for finitely generated abelian groups G and G'. It is decidable if G and G' are isomorphic.*

We now consider finitely generated *virtually* abelian groups. An obvious approach is to attempt to reduce the problem to one concerning abelian subgroups, and thereby fall back onto Conjecture 3.5.7. To do this, it is necessary to in some way extract an automatic presentation of a finite index abelian subgroup from a virtually abelian group.

We need some additional notation: for a subset X of a group G, the *centraliser* of X - denoted $C_G(X)$ - is the set of elements in G that commute with all elements in X; the *centre* of X - denoted $Z(X)$ - is the set of elements in X that commute with all other elements in X.

Lemma 3.5.8. *Let G be a finitely generated virtually abelian group.*

For some $n \in \mathbb{N}$, $Z(C_G(G^n))$ is an abelian subgroup in G of finite index.

Proof. Let A be a finitely generated abelian subgroup in G of finite index t.

For some n, the set G^n of nth powers of G is in A. This is because A has finite index in G. It follows, then, that the subgroup generated by G^n is also in A:

$$\langle G^n \rangle \leq A.$$

Now, $G/\langle G^n \rangle$ has exponent (dividing) n. As such, so does the abelian group $A/\langle G^n \rangle$. But a finitely generated abelian group of finite exponent is finite. So, $\langle G^n \rangle$ has finite index in A.

We now have:

$$[A : \langle G^n \rangle] < \infty;$$

and:

$$[G : A] < \infty;$$

so we can conclude:

$$[G : \langle G^n \rangle] < \infty.$$

Now, as $\langle G^n \rangle$ is in A, it is abelian. So $\langle G^n \rangle$ is in $C_G(G^n)$. In particular, it is in $Z(C_G(G^n))$, the centre of the centraliser of G^n.

So we now have:

$$[G : Z(C_G(G^n))] < \infty$$

The subgroup $Z(C_G(G^n))$ is abelian by definition. $\square$

Proposition 3.5.9. *Given an automatic presentation for a finitely generated virtually abelian group G, it is possible to effectively produce an automatic presentation that presents a finite index finitely generated abelian subgroup of G.*

Proof. Begin enumerating sets in G of the form G^n.

The subgroups $Z(C_G(G^n))$ are all normal in G - in fact, characteristic: that is, they are preserved under automorphisms of G.

They are also first-order definable in G:

$$G^n := \{g^n : g \in G\};$$

$$C_G(G^n) := \{x \in G : \forall y \in G^n, x \circ y = y \circ x\};$$

$$Z(C_G(G^n)) := \{x \in C_G(G^n) : \forall y \in C_G(G^n), x \circ y = y \circ x\}.$$

So, by Corollary 2.3.6, the groups $Z(C_G(G^n))$ have automatic presentations which can be effectively computed.

By Lemma 3.5.8, one of these factor groups will be finite, say for $n = k$. So we can take an automatic presentation of the first-order definable subgroup $Z(C_G(G^k))$. $\square$

Remark 3.5.10. Assume that, given an automatic presentation for a finitely generated abelian group, it is possible to effectively construct a standard group presentation for the group; then, given an automatic presentation for a finitely generated *virtually* abelian group, it is possible to effectively construct a standard group presentation for that group.

Let $\mathcal{S} = (S, \circ_S)$ be an automatic presentation for a finitely generated virtually abelian group G.

By Proposition 3.5.9, it is possible to find an automatic presentation $\mathcal{T} = (T, \circ_T)$ for a (normal) finite index abelian subgroup of G - say A. This automatic presentation is contained within the automatic presentation for G (i.e. $T \subseteq S$, and $\circ_T$ is the restriction of $\circ_S$ to $T \times T \times T$).

Let $\langle z_1, \ldots, z_n : R \rangle$ be a standard group presentation for A constructed from the automatic presentation $\mathcal{T}$.

It is possible to find words in the automatic presentation of G for coset representatives for A as follows.

First, choose a word from the regular language T. The element it presents will be the first coset representative, representing the coset A, say p_1. As regular languages are closed under complement (Proposition 2.2.2), the language $S \setminus T$ is regular. Take any word from this language. This will correspond to the second representative, say p_2. Now, the product of A with p_1 is first-order definable, and as such we may extract the words presenting the coset $A \circ p_1$ - say, T_{p_1}. To find the next representative, form the regular language $S \setminus (T \cup T_{p_1})$ - regular languages are closed under union, again by Proposition 2.2.2 - and so we can take any word from this language. Repeat the process, finding coset representatives $p_1, p_2, \ldots$. As A has finite index in G, this process will eventually produce a language $S \setminus (T \cup T_{p_1} \cup \ldots \cup T_{p_n})$ which is empty - that this regular language is empty is also decidable. Now we have a representative for all the cosets of A in G - $p_1, p_2, \ldots, p_q$.

A standard group presentation for G is then as follows:

$$\langle z_1, \ldots, z_n, p_1, \ldots, p_q \ : R \cup \{p_i{}^{-1} z_j p_i = \alpha_{i,j}\}_{1 \le i \le q, 1 \le j \le n}$$
$$\cup \{p_i p_j = \beta_{i,j} p_{k(i,j)}\}_{1 \le i,j,k \le q} \rangle$$

where the $\alpha_{i,j}$ and $\beta_{i,j}$ are words in the z_l and $z_l{}^{-1}$.

The words $\alpha_{i,j}$ and $\beta_{i,j}$ can be deduced using the automatic presentation for G. For instance, let α be the word representing $p_1{}^{-1} z_1 p_1$ in the automatic presentation. Then, enumerate the words representing the products of the z_l and $z_l{}^{-1}$ in the automatic presentation until α is found. As there are only a finite number of new relations, this process terminates.

The preceding discussions lead us to make the following conjecture:

Conjecture 3.5.11. *Let A and A' be automatic presentations for finitely generated virtually abelian groups G and G'. It is decidable whether G and G' are isomorphic.*

3.6 Unary Presentations for Groups

If a structure S has an automatic presentation with $|\Sigma| = 1$, then S is said to have a *unary* automatic presentation. Structures with such a presentation have been considered in [5] and [44].

The following is from [5]:

Theorem 3.6.1. *Let G be a group; then, G has a unary automatic presentation if and only if G is finite.*

3.7 Graph Products

Taking a slight interlude, we briefly consider graph products. The notion of a graph product of groups generalises the notions of direct and free products. Conditions determining exactly when a graph product of groups is hyperbolic, virtually free, or automatic are known - see [56], [53] and [29] respectively. Here, we consider the same question for the class of virtually abelian groups. Note that for this section we will assume implicitly that all groups are finitely generated.

To create a graph product, informally we take a graph and assign a group to each vertex. We then form a new group by taking each pair of groups in turn: if their vertices are joined by an edge, then take their direct product; if they are not, then take their free product. Note that if the graph is complete, we just have the direct product of all the groups, and if the graph has no edges, we just have the free product of all the groups. Formally, we have:

Definition 3.7.1. *Let $X = (V, E)$ be a finite undirected graph. For each $v \in V$, let G_v be a (non-trivial) group with presentation $\langle A_v : R_v \rangle$.*

The graph product *of the $(G_v)_{v \in V}$ with respect to X is defined as:*

$$\mathbb{GP}(X, (G_v)_{v \in V}) = \langle \bigcup_{v \in V} A_v : \bigcup_{v \in V} R_v, C \rangle$$

where $C = \{x^{-1}y^{-1}xy : x \in A_r, y \in A_s, \{r, s\} \in E\}$.

We now need to fix some notation. Let $X = (V, E)$ be a graph, $U \subseteq V$. We shall write $X|_U$ for $(U, E \cap (U \times U))$. Let $G = \mathbb{GP}(X, (G_v)_{v \in V})$. We shall write $G \restriction_U$ for $\mathbb{GP}(X|_U, (G_v)_{v \in U})$.

Proposition 3.7.2. *Let $G = \mathbb{GP}(X, (G_v)_{v \in V})$ be a graph product with $X = (V, E)$; then, G is virtually abelian if and only if:*

- *for every $v \in V$, G_v is virtually abelian; and*
- *if G_u and G_v are groups with $u \neq v$, and $\{u, v\} \notin E$, then $G_u \cong G_v \cong \mathbb{Z}_2$ and for all $w \in V \setminus \{u, v\}$ we have that $\{u, w\}$, $\{v, w\} \in E$.*

Proof. Suppose the conditions are satisfied. If there are no groups G_u and G_v with $u \neq v$, and $\{u, v\} \notin E$, we have a complete graph. Assume not, and let $U = \{u, v\}$. As $\{u, v\} \notin E$, $G \restriction_U \cong \mathbb{Z}_2 \star \mathbb{Z}_2 \cong D_\infty$. Now, as for all $w \in V \backslash \{u, v\}$, $\{u, w\}$, $\{v, w\} \in E$, it is clear that $G \cong G \restriction_{V \backslash U} \times D_\infty$. So, in the original graph, we can identify the vertices u and v as, say, a, and let G_a be D_∞. By repeating for all such G_u and G_v, the result is a complete graph.

We now have a complete graph. As virtually abelian groups are closed under direct products, the statement follows immediately.

Now for the converse: a finitely generated subgroup of a virtually abelian group is virtually abelian, so the first condition is clear. So assume we have G_u, G_v, $u \neq v$ with $\{u, v\} \notin E$.

Case i: Assume $G_u \not\cong \mathbb{Z}_2$. So, there exists $x_1, x_2 \in G_u$ with $x_1 \neq x_2$, both non-trivial. Let $y \in G_v$.

Consider the elements $x_1^{-1} y^{-1} x_1 y$ and $x_2^{-1} y^{-1} x_2 y$, and their respective inverses $y^{-1} x_1^{-1} y x_1$ and $y^{-1} x_2^{-1} y x_2$.

As $\{u, v\} \notin E$, there are no relations between x_i and y, so each element generates an infinite group.

Also, as $x_1 \neq x_2$, $x_1 x_2^{-1}$ and $x_2 x_1^{-1}$ are non-trivial, so there is no collapse in any product of these elements.

Therefore, $\langle x_1^{-1} y^{-1} x_1 y, x_2^{-1} y^{-1} x_2 y \rangle$ is a free group on two generators, so G is not virtually abelian.

Case ii: Assume there exists G_w, $w \neq u, v$, such that $\{v, w\} \notin E$. Let $x \in G_u$, $y \in G_v$, $z \in G_w$.

Consider the elements $x^{-1}y^{-1}xy$ and $z^{-1}y^{-1}zy$, and their respective inverses $y^{-1}x^{-1}yx$ and $y^{-1}z^{-1}yz$.

As $\{u, v\}, \{v, w\} \notin E$, there are no relations between x and y or z and y, so each element generates an infinite group.

Also, as $x \neq z$, xz^{-1} and zx^{-1} are non-trivial, so there is no collapse in any product of these elements.

Therefore, $\langle x^{-1}y^{-1}xy, z^{-1}y^{-1}zy \rangle$ is a free group on two generators, so G is not virtually abelian. $\square$

Corollary 3.7.3. *A graph product $G = \mathbb{GP}(X, (G_v)_{v \in V})$ has an automatic presentation if and only if:*

- *for every $v \in V$, G_v is virtually abelian, and*
- *if G_u and G_v are groups with $u \neq v$, and $\{u, v\} \notin E$, then $G_u \cong G_v \cong \mathbb{Z}_2$ and for all $w \in V \setminus \{u, v\}$ we have that $\{u, w\}$, $\{v, w\} \in E$.*

Proof. This follows immediately from Theorem 3.4.5. $\square$

Chapter 4

Cancellative Semigroups

Chapter 3 classified those finitely generated groups with automatic presentations. We attempt to generalise that result here. Groups may be viewed as semigroups with a particularly stringent condition: the existence of inverses. We shall consider a slightly weaker case here: semigroups that satisfy cancellation laws.

4.1 Definition and Basic Results

Definition 4.1.1. *Let S be a semigroup. S is said to be* cancellative *if for all $a, b, c \in S$:*

$$ab = ac \Rightarrow b = c$$

$$ba = ca \Rightarrow b = c$$

This definition is satisfied by groups, so groups are an example of cancellative semigroups. There are cancellative semigroups that are not groups: $(\mathbb{N}, +)$, for example. More importantly, subsemigroups of groups are cancellative, with the conditions being inherited from the group itself (note that the conditions needed for a semigroup to be cancellative are universal statements). Not all cancellative semigroups are subsemigroups of groups: see [55].

Similar to the idea of a field of quotients in ring theory, it is sometimes possible to add inverses to a cancellative semigroup to embed it into a group.

Definition 4.1.2. *Let S be a subsemigroup of a group G. If every element in G is equal to $a^{-1}b$ for some $a, b \in S$ then G is a* group of left quotients *for S. If every element in G is equal to ab^{-1} for some $a, b \in S$ then G is a* group of right quotients *for S.*

Lemma 4.1.3. *Let S be a semigroup with a group of left (or right) quotients G; if S is finitely generated, then so is G.*

Proof. Let G be a group of left quotients for S. The proof for a group of right quotients proceeds similarly. Let $\{x_1, \ldots, x_n\}$ be a generating set for S. Let $X \subseteq G$ contain $x_1, \ldots, x_n$ and $x_1^{-1}, \ldots, x_n^{-1}$. Let $g \in G$. By the hypothesis, $g = a^{-1}b$ with $a, b \in S$. Now, $a = x_{i_1}x_{i_2} \ldots x_{i_n}$ and $b = x_{j_1}x_{j_2} \ldots x_{j_n}$, say, so:

$$\begin{aligned} g &= (x_{i_1}x_{i_2} \ldots x_{i_n})^{-1}x_{j_1}x_{j_2} \ldots x_{j_n} \\ &= (x_{i_n})^{-1} \ldots (x_{i_1})^{-1}x_{j_1}x_{j_2} \ldots x_{j_n}. \end{aligned}$$

As such, X is a (finite) generating set for G. □

We need the following proposition:

Proposition 4.1.4. *Let S be a semigroup with a virtually nilpotent group of left quotients G; then, G is also a group of right quotients for S.*

The proof, implicit in [9], requires the following definitions and results.

Definition 4.1.5. *A* semigroup law *consists of two words u, v over an alphabet X, and is denoted $u = v$. A semigroup S satisfies such a law if $\theta(u) = \theta(v)$ for every homomorphism $\theta : X^+ \to S$. The law is called* non-tautological *if u and v are not the same word.*

Lemma 4.1.6. *Let G be a virtually nilpotent group; then, G satisfies a non-tautological semigroup law.*

Proof. The proof of this lemma is contained within the proof of Theorem 5.3.5 of [9]; briefly, nilpotent groups satisfy a non-tautological semigroup law, and if a group has a subgroup of finite index satisfying a non-tautological semigroup law then the group will also satisfy a non-tautological semigroup law. □

Definition 4.1.7. *A semigroup is called* right-reversible *if for all $s, s' \in S$ there exists $t, t' \in S$ such that $ts = t's'$. A semigroup is called* left-reversible *if for all $s, s' \in S$ there exists $t, t' \in S$ such that $st = s't'$.*

The following is taken from [9], where it is adapted from a proof in [59].

Proposition 4.1.8. *If S is a cancellative semigroup that satisfies a non-tautological semigroup law, then S is both left- and right-reversible.*

Now, a theorem of Dubreil:

Theorem 4.1.9 (Dubreil [24]). *Let S be a cancellative semigroup. S is right-reversible if and only if S has a group of left quotients. S is left-reversible if and only if S has a group of right quotients.*

Proposition 4.1.10. *Let S be a cancellative semigroup with a group of left quotients G_L and a group of right quotients G_R; then, $G_L \cong G_R$.*

Proof. The result follows from results in [9] drawn from a proof in [16]: note that such a semigroup is both left- and right-reversible by the previous theorem, and then Proposition 5.2.4 from [9] establishes that both G_L and G_R are isomorphic to the group generated by S (within, say, G_L). □

We may now prove Proposition 4.1.4:

Proof. Lemma 4.1.6 establishes that G satisfies a semigroup law. As S is a subsemigroup of G it clearly satisfies the same law, so by Proposition 4.1.8 S is both left- and right-reversible. Theorem 4.1.9 shows that S has a group of right quotients G_R, and Proposition 4.1.10 shows that $G_R \cong G$. □

4.2 Necessary Conditions

We will present a necessary condition for a cancellative semigroup to have an automatic presentation. We need the following proposition, a generalisation of Gromov's theorem (Theorem 3.4.1) by Grigorchuk.

Theorem 4.2.1 (Grigorchuk [33]). *Let S be a finitely generated cancellative semigroup; then, S has polynomial growth if and only if it has a virtually nilpotent group of left quotients G.*

Corollary 4.2.2. *Let S be a finitely generated cancellative semigroup. If S has an automatic presentation, then S has a virtually nilpotent group of left quotients G.*

Proof. By Theorem 3.3.3, if S has an automatic presentation then S has polynomial growth. □

This corollary can be usefully combined with Proposition 4.1.4:

Proposition 4.2.3. *Let S be a finitely generated cancellative semigroup. If S has an automatic presentation, then S is a subsemigroup of a virtually nilpotent group G that is both a group of left and right quotients of S.*

Proof. By the preceeding corollary, S has a virtually nilpotent group of left quotients G: Proposition 4.1.4 implies that this group is also a group of right quotients for S. □

We will now establish that G must also have an automatic presentation. Note that, as G is both a group of left and right quotients for S, for every $g \in G$ there exists $s, t \in S$ such that $g = st^{-1}$ and there exists $p, q \in S$ such that $g = p^{-1}q$.

Proposition 4.2.4. *Let S be a finitely generated cancellative semigroup. If S has an automatic presentation, then there is an interpretation of its group of left(and right) quotients G in S.*

Proof. The interpretation is 2-dimensional.

- The domain formula is just $\phi(x_1, x_2) := x_1 = x_1$, i.e. a tautology, so we are using all pairs of elements of S.
- The co-ordinate map is $f(x_1, x_2) = x_1^{-1}x_2$; this is surjective, as required, from the definition of a group of left quotients.
- Equality is $\theta_=(x_1, x_2; y_1, y_2) := \exists a, b(x_1 a = x_2 b \wedge y_1 a = y_2 b)$, as

$$\begin{array}{rrcl} & f(x_1, x_2) & = & f(y_1, y_2) \\ \Leftrightarrow \exists a, b & (f(x_1, x_2) = ab^{-1} & \wedge & f(y_1, y_2) = ab^{-1}) \\ \Leftrightarrow \exists a, b & (x_1^{-1}x_2 = ab^{-1} & \wedge & y_1^{-1}y_2 = ab^{-1}) \\ \Leftrightarrow \exists a, b & (x_1 a = x_2 b & \wedge & y_1 a = y_2 b). \end{array}$$

- Composition is

$$\theta_\circ(x_1, x_2; y_1, y_2; z_1, z_2) := \exists a, b, c, d(cx_1 a = dy_2 b \wedge cx_2 = dy_1 \wedge z_2 b = z_1 a)$$

as

$$
\begin{array}{rrcl}
& f(x_1,x_2)\circ f(y_1,y_2) & = & f(z_1,z_2) \\
\Leftrightarrow \exists a,b & (f(x_1,x_2)\circ f(y_1,y_2) = ab^{-1} & \wedge & f(z_1,z_2) = ab^{-1}) \\
\Leftrightarrow \exists a,b & (x_1^{-1}x_2y_1^{-1}y_2 = ab^{-1} & \wedge & z_1^{-1}z_2 = ab^{-1}) \\
\Leftrightarrow \exists a,b,c,d & (c^{-1}d = x_2y_1^{-1} & \wedge & x_1^{-1}c^{-1}dy_2 = ab^{-1} \quad \wedge \quad z_1^{-1}z_2 = ab^{-1}) \\
\Leftrightarrow \exists a,b,c,d & (cx_2 = dy_1 & \wedge & dy_2b = cx_1a \quad \wedge \quad z_2b = z_1a).
\end{array}
$$

□

Corollary 4.2.5. *Let S be a finitely generated cancellative semigroup. If S has an automatic presentation, then its group of left(and right) quotients G has an automatic presentation.*

Theorem 4.2.6. *Let S be a finitely generated cancellative semigroup; if S has an automatic presentation, then S has a finitely generated virtually abelian group of left quotients G.*

Proof. Let S be a finitely generated cancellative semigroup with an automatic presentation. By Corollary 4.2.5, its group of left quotients G has an automatic presentation, and by Lemma 4.1.3 G is finitely generated. So, by Theorem 3.4.5 G is virtually abelian. □

Corollary 4.2.7. *Let S be a finitely generated cancellative semigroup; if S has an automatic presentation, then S is a subsemigroup of a finitely generated virtually abelian group.*

4.3 Subsemigroups of Virtually Abelian Groups

We would, of course, like to establish the converse to Theorem 4.2.6. In this section, we prove a proposition which is a step in that direction.

First, a lemma. If S is not a monoid, i.e. does not contain an identity element, then we shall denote by S^1 the result of adding an extra element acting as an identity. If S is a monoid, we take $S^1 = S$.

Lemma 4.3.1. *S^1 has an automatic presentation if and only if S has an automatic presentation.*

Proof. If S contains an identity element, then $S = S^1$ and the result is trivial. So, assume S contains no identity element.

Only if: Let (L, θ) be an automatic presentation for S^1 over the alphabet Σ.

Let $W = \theta^{-1}(1)$. Note that this is first-order definable over S^1:

$$\psi(x) := \forall y, xy = yx = y.$$

So, by Theorem 2.3.1 W is regular. Let $\overline{L} = L \setminus W$

Define $\overline{\theta} : \overline{L} \to S$ as:

$$\overline{\theta}(w) = \theta(w)$$

As S contains no identity element, $\overline{\theta}$ is surjective, and by Proposition 2.2.2 $\overline{L}$ is regular.

To establish that $(\overline{L}, \overline{\theta})$ is an automatic presentation for S, we need to show that $\overline{L}_=$ and $\overline{L}_\circ$ are regular.

Clearly,

$$\overline{L}_= = L_= \setminus \{\text{conv}(r, s) : r, s \in W\}$$

$$\overline{L}_\circ = L_\circ \setminus \{\text{conv}(r, s, t) : r \in W \text{ or } s \in W \text{ or } t \in W\}.$$

These are both regular by Proposition 2.2.2 and Proposition 2.2.3.

If: Now, let (L, θ) be an automatic presentation for S over the alphabet Σ.

Let $\iota \notin \Sigma$, and let $\overline{\Sigma} = \Sigma \cup \{\iota\}$. Let $\overline{L} = L \cup \{\iota\}$.

Define $\overline{\theta} : \overline{L} \to S^1$ as:

$$\overline{\theta}(w) = \begin{cases} \theta(w) & \text{if } w \in L \\ 1 & \text{if } w = \iota \end{cases}$$

As θ is surjective, $\overline{\theta}$ is surjective, and by Proposition 2.2.2 $\overline{L}$ is regular.

To establish that $(\overline{L}, \overline{\theta})$ is an automatic presentation for S, we need to show that $\overline{L}_=$ and $\overline{L}_\circ$ are regular.

Clearly,

$$\overline{L}_= = L_= \cup \{\text{conv}(\iota, \iota)\}$$

$$\overline{L}_\circ = L_\circ \cup \{\text{conv}(r, s, t) : s, t \in L, r = \iota \text{ or } r, t \in L, s = \iota\}.$$

These are both regular by Proposition 2.2.2 and Proposition 2.2.3. □

Proposition 4.3.2. *Let S be a finitely generated cancellative semigroup.*

Let G be a finitely generated virtually abelian group, with A a normal abelian subgroup of finite index, and (L, ϕ) an automatic presentation of G.

If S is a subsemigroup of G, and $L|_{S\cap A}$ is regular, then S has an automatic presentation.

Proof. By the previous lemma, we may assume that S contains an identity element 1.

Let $C = S \cap A$. Let X be a generating set for S, and let $Y = X \setminus C \cup \{1\}$ i.e. the generators of S not in C (and the identity).

As X generates S, $X \subseteq Y \cup C$, and $1 \in C$ we have for all $s \in S$, there exists $r \in \mathbb{N}$, such that:

$$s \in (YC)^r.$$

Let k be the index of A in G.

Let $s \in S$, and $s \in (YC)^t$ where $t > k + 1$. So, $s = y_1c_1 \dots y_tc_t$, where $y_i \in Y, c_i \in C$. Let $g_i = y_ic_i$.

Consider the sequence $g_1, g_1g_2, g_1g_2g_3, \ldots, g_1g_2\cdots g_{k+1}$. As this sequence of elements (of G) is longer than the index of A in G, there exist i, j (without loss of generality $i < j$) and a coset of A, say Ag, such that

$$g_1 \cdots g_i \in Ag$$
$$g_1 \cdots g_i g_{i+1} \cdots g_j \in Ag$$

i.e.

$$g_1 \cdots g_i = ag$$
$$g_1 \cdots g_i g_{i+1} \cdots g_j = \bar{a}g$$

so

$$g_{i+1} \cdots g_j = (ag)^{-1}\bar{a}g \in A \cap S = C.$$

Now let $g_{i+1} \cdots g_j = c_g$

$$
\begin{aligned}
& s = y_1c_1 \ldots y_ic_iy_{i+1}c_{i+1} \cdots y_jc_jy_{j+1}c_{j+1} \cdots y_tc_t \\
\Rightarrow \quad & s = y_1c_1 \cdots y_ic_ig_{i+1} \cdots g_jy_{j+1}c_{j+1} \cdots y_tc_t \\
\Rightarrow \quad & s = y_1c_1 \cdots y_ic_ic_gy_{j+1}c_{j+1} \cdots y_tc_t \\
\Rightarrow \quad & s \in (YC)^{t-(j-i)}.
\end{aligned}
$$

We have shown that, if $s \in (YC)^t$ with $t > k+1$, then $s \in (YC)^{t-(j-i)}$ with $i < j < t$. By cascading down, we get that $s \in (YC)^t$, $t > k+1$, implies $s \in (YC)^{k+1}$.

Now, as $1 \in C \cap Y$, for all $s \in S$,

$$s \in (YC)^{k+1}.$$

So, to find a regular language representing S, we only need to find a regular language representing $(YC)^{k+1}$.

The composition of $2(k+1)$ elements in G is first-order definable, and therefore there is a corresponding regular language R. As we have a regular language $\bar{C} = L|_{S\cap A}$ representing C, and $\bar{Y}$ representing Y (Y is finite), the language

$$R' = \{\mathrm{conv}(u_1, v_1, u_2, v_2 \ldots, u_{k+1}, v_{k+1}, w) \in R : u_i \in \bar{C}, v_j \in \bar{Y}\}$$

is regular by Proposition 2.2.3. Again using this proposition, the language

$$L_S = \{w \in L : \exists w_1 \ldots w_{2(k+1)}, \mathrm{conv}(w_1, \ldots, w_{2(k+1)}, w) \in R'\}$$

is regular, and contains a representative for all elements in $(YC)^{k+1}$, i.e. S.

It should now be clear that $(L_S, \phi|_{L_S})$ is an automatic presentation for S, with the regularity of composition and equality shown by restricting the corresponding languages for G, using the second part of Proposition 2.2.3. □

The problem now is to try and show that the regularity condition always holds. As a step towards this, we will show that C, a subsemigroup of S, being finitely generated is enough to guarantee the regularity condition. We need a definition and a lemma from [33], which generalise the notion of finite index to semigroups.

Definition 4.3.3. *Let S_0 be a subsemigroup of a semigroup S.*

S_0 has finite index *in S if there exists a finite set $K \subseteq S$ such that for all $s \in S$, there exists $k \in K$ such that:*

$$sk \in S_0.$$

This definition only has application for some classes of semigroup (by this definition, any semigroup with zero is virtually trivial), but is useful at least within the class of cancellative semigroups.

Lemma 4.3.4 (Grigorchuk [33]). *Let S be a finitely generated semigroup that has a group G of (left) quotients and $H \lhd G$ a normal subgroup of finite index. Then there exists a subsemigroup $S_0 = S \cap H$ of S of finite index such that H is its group of (left) quotients.*

Proposition 4.3.5. *Let S be a finitely generated cancellative semigroup.*

Let G be a finitely generated virtually abelian group, with A an abelian subgroup of finite index, and (L, ϕ) an automatic presentation of G.

Assume S is a subsemigroup of G. If $C = S \cap A$ is finitely generated then $L|_{S \cap A}$ is regular.

Proof. We may assume A is a free abelian normal subgroup of finite index, by Remark 3.2.5.

As S is a subsemigroup of a group with polynomial growth, it has a group of (left) quotients by [33] (Corollary 1). This group will be a subgroup of G, so will also be a finitely generated virtually abelian group. Without loss of generality, we will assume this group is G itself.

Let $C = S \cap A$. By Lemma 4.3.4 C is a semigroup, and has finite index in S, with A its group of (left) quotients. Clearly, C is commutative.

By Remark 3.2.6, G has a presentation where $g \in G$ is represented by $\text{conv}(k, x_1, \ldots, x_n)$, with $k \in K$ for some finite language K of equal size to the index of A in G, and $x_i \in \{+, -\}\{0,1\}^*1 \cup \{+0\}$, where n is the size of a minimal generating set for A. We will assume that (L, ϕ) is this presentation.

Let $\{c_1, \ldots, c_m\}$ be a generating set for C. Let $\{a_1, \ldots, a_n\}$ be a generating set for A, such that a_i corresponds to the $i+1$ component of the convolution representing elements of G.

Each c_i is in A, so $c_i = a_1^{\epsilon_{i_1}} a_2^{\epsilon_{i_2}} \ldots a_n^{\epsilon_{i_n}}$ for some $\epsilon_{i_j} \in \mathbb{Z}$.

Now, let $c \in C$. As C is commutative, we have $c = c_1^{\alpha_1} \ldots c_m^{\alpha_m}$ for some

$\alpha_i \in \mathbb{N}$. Representing c as an element of A, we have $c = a_1^{\beta_1} \ldots a_n^{\beta_n}$ where

$$\beta_i = \epsilon_{1_i}\alpha_1 + \epsilon_{2_i}\alpha_2 + \ldots + \epsilon_{m_i}\alpha_m.$$

Consider words in the presentation of the form $\mathrm{conv}(\lambda, x_1, \ldots, x_n)$, where $\lambda \in K$ represents the coset A. The image of this language under ϕ is A. We need to show that there is a regular subset of these words whose image under ϕ is C.

Take the structure $(\mathbb{Z}, +, \geq)$, and in particular let (B, ψ_B) be an automatic presentation of the structure where each element of $\mathbb{Z}$ is represented in binary with a preceding $+$ or $-$ symbol, i.e. $B = \{+,-\}\{0,1\}^{\star}1 \cup \{+0\}$. This is essentially the automatic presentation of the structure, as a group, from remark 3.2.6, noting that $\geq$ is regular in this presentation (It is an open question as to whether $\geq$ is regular in *any* automatic presentation of $(\mathbb{Z}, +)$ - see [47]).

We can now use this structure to define the possible combinations of values of β_i for the members of C as follows:

$$\begin{aligned}
\theta(u_1, \ldots, u_n) := \exists v_1, \ldots, v_m, \qquad & (v_1 \geq 0 \wedge \ldots \wedge v_m \geq 0) \\
\wedge \quad & ((u_1 = \epsilon_{1_1}v_1 + \epsilon_{2_1}v_2 + \ldots + \epsilon_{m_1}v_m) \\
\wedge \quad & (u_2 = \epsilon_{1_2}v_1 + \epsilon_{2_2}v_2 + \ldots + \epsilon_{m_2}v_m) \\
& \ldots \\
\wedge \quad & (u_n = \epsilon_{1_n}v_1 + \epsilon_{2_n}v_2 + \ldots + \epsilon_{m_n}v_m)).
\end{aligned}$$

Note that the set of words representing 0 is regular, and that $\epsilon_{i_j}v_i$ is shorthand for $v_i + v_i + \ldots + v_i$ where v_i is combined with itself ϵ_{i_j} times. Also, note that the u_i correspond to the β_i, and the v_j correspond to the α_j, from above.

Recalling the words x_i from the automatic presentation for G, it should be noted at this point that these x_i are contained in B by definition. As such, we may define the following language:

$$\overline{C} = \{\text{conv}(\lambda, x_1, x_2, \ldots, x_n) \in L : (\mathbb{Z}, +, \geq) \vDash \theta(\phi_B(x_1), \ldots, \phi_B(x_n))\}.$$

Now, $\overline{C}$ is regular by Theorem 2.3.1, and each element of C is represented by an element of $\overline{C}$. Note also that $w \in \overline{C}$ implies $\phi(w) \in C$.

Now we can show, as required, that $L|_{S\cap A}$ is regular. In fact,

$$L|_{S\cap A} = L|_C = \{w \in L : \exists z \in \overline{C}, \text{conv}(w, z) \in L_=\},$$

which is regular via Proposition 2.2.3. □

Unfortunately, it is not necessarily the case that C is finitely generated - even if both S and G are. The following example is adapted from [9].

Example 4.3.6. Let

$$G = \langle x, y, a, r : r^{-1}xr = y, r^{-1}yr = x, r^2 = a \rangle.$$

Let $H = \langle x, y, a \rangle_G \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \lhd G$. As $r^2 = a$, it is clear that $|G : H| = 2$.

Now consider the semigroup $S = \langle x, r \rangle_S$. Note in particular that

$$rx^ir = r^2r^{-1}x^ir = ay^i \in S$$

for all $i \in N$.

Every element of G is expressible as $s^{-1}t$, where $s, t \in S$, so G is a group of (left) quotients of S.

Now let $C = S \cap H$.

$x^iy^ja^k \in C \Rightarrow i, j, k \geq 0$, and $j > 0 \Rightarrow k > 0$.

As such, all the ay^i are indecomposable in C: so, C not finitely generated.

Despite this example, we still hold out hope for the result:

Conjecture 4.3.7. *Let S be a finitely generated cancellative semigroup; then, S has an automatic presentation if and only if S is a subsemigroup of a virtually abelian group.*

4.4 Unary Presentations for Cancellative Semigroups

Theorem 4.4.1. *Let S be a cancellative semigroup; then, S has a unary automatic presentation if and only if S is finite.*

Proof. The proof of Theorem 3.6.1, as given in [5], assumes only that the product function is cancellative. □

This result is a generalisation of Theorem 3.6.1. We will now demonstrate that the assumption of cancellativity cannot be weakened to either left- or right-cancellativity.

Definition 4.4.2. *A semigroup S is* left-cancellative *if for all $a, b, c \in S$,*

$$ab = ac \Rightarrow b = c.$$

A semigroup S is right-cancellative *if for all $a, b, c \in S$,*

$$ba = ca \Rightarrow b = c.$$

A semigroup S is left-zero *if for all $a, b \in S$,*

$$ab = b.$$

A semigroup S is right-zero *if for all $a, b \in S$,*

$$ab = a.$$

Proposition 4.4.3. *All left- and right- zero semigroups have a unary automatic presentation.*

Proof. Enumerate the elements of the semigroup, and let the word 1^n represent the nth element. The product automaton merely checks that the representative for the product is the same length as the representative for the second (respectively first) element. □

Corollary 4.4.4. *There exist infinite left- and right-cancellative semigroups with unary presentations.*

Proof. Left-zero semigroups are left-cancellative:

$$\text{For all } a, b, c \in S, \;\; ab = b \text{ and } ac = c \therefore ab = ac \Rightarrow b = c.$$

Similarly for right-cancellative.

It should be clear that there exist infinite left- and right-zero semigroups: e.g. define on $\mathbb{N}$ the product $x \circ y = x$. $\square$

Chapter 5

Other Semigroups

Chapter 4 dealt with a particular class of interesting semigroups, with an attempt to generalise the result of Chapter 3 on groups. Here we collect together the results obtained for other classes of semigroups.

5.1 Commutative Semigroups

All finitely generated commutative (abelian) groups have an automatic presentation (Proposition 3.2.3). Similarly, we have:

Theorem 5.1.1. *Let S be a finitely generated commutative semigroup; then, S has an automatic presentation.*

Proof. Clearly this is true for finitely generated free commutative semigroups, as they are isomorphic to $(\mathbb{N}, +)^n$ for some n.

Every commutative semigroup is a quotient of a free commutative semigroup and, by [70], the corresponding congruence is first-order definable.

The result then follows from Corollary 2.3.6. □

5.2 Completely Simple Semigroups

Before presenting the results of this section, we need some preliminary definitions.

Definition 5.2.1. *Let S be a semigroup.*

- *Let T be a subsemigroup of S. T is an* ideal *if, for all $s \in S$ and $t \in T$, we have that $st \in T$ and $ts \in T$.*

- *An element $x \in S$ such that for all $s \in S$, $sx = xs = x$ is called a* zero*; if present, it must clearly be unique, and we shall denote it 0. For notation:*
$$S^0 = \begin{cases} S & \text{if } 0 \in S \\ S \cup \{0\} & \text{if } 0 \notin S \end{cases}.$$

- *If S contains a zero, and for all $s, t \in S$ we have $st = 0$, then S is called* null.

- *An element $s \in S$ is an* idempotent *if $ss = s$.*

Analogously to ring theory, a semigroup is called *simple* if it has no proper ideals. Since $\{0\}$ is always an ideal in a semigroup with 0, a semigroup is called 0-*simple* if it contains a zero and no other proper ideals; we also insist that $S^2 \neq \{0\}$, to exclude the null semigroup with two elements.

There is a natural partial order on the idempotents in a semigroup:

$$e \leq f := ef = fe = e$$

Clearly, if there is a zero in the semigroup it is the minimum of this order. We call an idempotent *primitive* if it is minimal amongst the non-zero idempotents.

The importance of the notion of a primitive idempotent for simple (and 0-simple) semigroups comes from the existence of the classification theorems of Rees for such semigroups containing a primitive idempotent. A simple semigroup is called *completely simple* if it contains a primitive idempotent; a 0-simple semigroup is called *completely* 0*-simple* if it contains a primitive idempotent.

Definition 5.2.2. *Let G be a group, I and Λ non-empty sets. Let $P = (p_{\lambda,i})$ be a $\Lambda \times I$ matrix over the group G. Now, define a semigroup $S = (I \times G \times \Lambda)$, with:*

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda,j}h, \mu)$$

We will denote S by $\mathcal{M}[G;\ I,\ \Lambda;\ P]$.

Let G be a group, I and Λ non-empty sets. Let $P = (p_{\lambda,i})$ be a $\Lambda \times I$ matrix over the semigroup G^0. Assume every row and column of P contains a non-zero element. Now, define a semigroup $S = (I \times G \times \Lambda) \cup \{0\}$, with:

$$(i, g, \lambda)(j, h, \mu) = \begin{cases} (i, gp_{\lambda,j}h, \mu) & \text{if } p_{\lambda,j} \neq 0 \\ 0 & \text{if } p_{\lambda,j} = 0 \end{cases}$$

We will denote S by $\mathcal{M}^0[G;\ I,\ \Lambda;\ P]$.

In both cases, S is called a Rees matrix semigroup.

Theorem 5.2.3 (Rees)**.** *Let S be a semigroup.*

- *S is completely simple if and only if $S \cong \mathcal{M}[G;\ I,\ \Lambda;\ P]$ for some G, I, Λ and P.*

- *S is completely* 0*-simple if and only if $S \cong \mathcal{M}^0[G;\ I,\ \Lambda;\ P]$ for some G, I, Λ and P.*

As has been a common theme, we can obtain a clear classification if we restrict our attention to finitely generated semigroups. As such, the following proposition, from [1], is useful for us:

Proposition 5.2.4. *A completely simple (completely* 0*-simple) semigroup* $S \cong \mathcal{M}[G;\ I,\ \Lambda;\ P]$ *(*$\cong \mathcal{M}^0[G;\ I,\ \Lambda;\ P]$*) is finitely generated if and only if:*

- G *is finitely generated, and*
- I *and* Λ *are finite.*

We can now present the classifications.

Theorem 5.2.5. *A finitely generated completely simple semigroup* S*, with* $S \cong \mathcal{M}[G;\ I,\ \Lambda;\ P]$*, has an automatic presentation if and only if* G *is virtually abelian.*

Proof. Assume G is virtually abelian; then, as it is finitely generated, it has an automatic presentation. We need to show that $S = \mathcal{M}[G;\ I,\ \Lambda;\ P]$ has an automatic presentation.

For all $g \in G$, let $\bar{g}$ denote the word representing g in a fixed automatic presentation.

Let $P = (p_{\lambda i})_{i \in I, \lambda \in \Lambda}$.

By the construction of $\mathcal{M}[G;\ I,\ \Lambda;\ P]$ (for which see [41]) it is possible to choose $\Lambda_G = \{q_\lambda : \lambda \in \Lambda\} \subseteq G$ and $I_G = \{r_i : i \in I\} \subseteq G$ such that $p_{\lambda i} = q_\lambda r_i$.

As S is finitely generated I and Λ are finite sets, and so I_G and Λ_G are finite sets of the same orders.

Replace I with I_G and Λ with Λ_G: as these are merely indexing sets, the resulting semigroup is isomorphic to S. Composition in $\mathcal{M}[G;\ I_G,\ \Lambda_G;\ P]$

is now equivalently given by

$$(r_i,\ g,\ q_\lambda)(r_j,\ h,\ q_\mu) = (r_i,\ g.q_\lambda r_j.h,\ q_\mu). \qquad (*)$$

We will represent $(r_i,\ g,\ q_\lambda)$ by $\text{conv}(\bar{r_i},\ \bar{g},\ \bar{q_\lambda})$.

We have, by assumption, an automaton M for checking the composition of elements in G.

It is clear that composition of four elements (i.e. $g_1g_2g_3g_4 = g$) is first-order definable, and as such an automaton M_4 can be constructed for checking it.

Considering composition for the semigroup $(*)$, it is clear that the only work being done is, in fact, the composition of four elements of the group.

As such, an automaton may be constructed to check composition in the semigroup by merely amending M_4 to account for the outside values that are kept constant. This is feasible as I and Λ are finite sets, ensuring the representations remain regular.

Now assume $S = \mathcal{M}[G;\ I,\ \Lambda;\ P]$ has an automatic presentation (M, ϕ).

We need to show that the underlying group G has an automatic presentation. As all the $\mathcal{H}$-classes are isomorphic to G (see [41]), we only need to show that any one of these has an automatic presentation.

Choose $x \in S$. Let $\widetilde{x}$ be the word in the automatic presentation corresponding to x. Let M be the composition-checking automaton for S, and denote the language of M by $L(M)$ as usual. The $\mathcal{H}$-class containing x is denoted H_x - we will show that this group has an automatic presentation.

Now, denoting the L-class containing x by L_x, and the R-class containing x by R_x, we know from [41] that $H_x = L_x \cap R_x$.

Let

$$M_\circ = \{\text{conv}(w_1, w_2, w_3) : (w_1, w_2, w_3) \in M \times M \times M, \phi(w_1) \circ \phi(w_2) = \phi(w_3)\},$$

i.e. the language representing composition, which is regular as (M, ϕ) is an automatic presentation.

Again from [41] $L_x = Sx = \{s \circ x : s \in S\} \subseteq S$, so we first need to show that the set of representatives for Sx form a regular language. Let

$$M_L = \{\text{conv}(w_1, \widetilde{x}, w_3) \in M_\circ\}.$$

By the second part of Proposition 2.2.3, this language is regular. Now let

$$M_L' = \{w : \text{conv}(w_1, w_2, w) \in M_L\}.$$

By the first part of Proposition 2.2.3, this language is regular, and clearly represents Sx.

Similarly, $R_x = xS = \{x \circ s : s \in S\} \subseteq S$, so we first need to show that the set of codes for xS form a regular language. Let

$$M_R = \{\text{conv}(\widetilde{x}, w_2, w_3) \in M_\circ\}.$$

By the second part of Proposition 2.2.3, this language is regular. Now let

$$M_R' = \{w : \text{conv}(w_1, w_2, w) \in M_R\}.$$

By the first part of Proposition 2.2.3, this language is regular, and clearly represents xS.

As the regular language M_L' represents L_x, and the regular language M_R' represents R_x, the language $M_L' \cap M_R'$ represents H_x. By Proposition 2.2.2, this language is regular. □

Theorem 5.2.6. *A finitely generated completely* 0*-simple semigroup* S*, with* $S = \mathcal{M}^0[G;\ I,\ \Lambda;\ P]$*, has an automatic presentation if and only if* G *is virtually abelian.*

Proof. Assume G is virtually abelian; then, as it is finitely generated, it has an automatic presentation. We need to show that $S = \mathcal{M}^0[G;\ I,\ \Lambda;\ P]$ has an automatic presentation.

As G is a group, it has no zero element. Add a new element 0 to G such that $0.g = g.0 = 0$, and give it a new code $\bar{0}$. Although $G \cup \{0\}$ is no longer a group, it clearly still has automatic presentation.

For all $g \in G$, let $\bar{g}$ denote the word representing g in a fixed automatic presentation.

Let $P = (p_{\lambda i})_{i \in I, \lambda \in \Lambda}$.

By the construction of $\mathcal{M}^0[G;\ I,\ \Lambda;\ P]$ (for which see [41]) it is possible to choose $\Lambda_G = \{q_\lambda : \lambda \in \Lambda\} \subseteq G$ and $I_G = \{r_i : i \in I\} \subseteq G$ such that, where $p_{\lambda i}$ is not 0, $p_{\lambda i} = q_\lambda r_i$.

As S is finitely generated I and Λ are finite sets, and so I_G and Λ_G are finite sets of the same orders.

Replace I with I_G and Λ with Λ_G: as these are merely indexing sets, the resulting semigroup is isomorphic to S.

Composition in $\mathcal{M}^0[G;\ I_G,\ \Lambda_G;\ P]$ is now equivalently given by

$$\begin{aligned}
(r_i,\ g,\ q_\lambda)(r_j,\ h,\ q_\mu) &= \quad (r_i,\ g.q_\lambda r_j.h,\ q_\mu) \quad : p_{\lambda j} \neq 0,\\
(r_i,\ g,\ q_\lambda)(r_j,\ h,\ q_\mu) &= \qquad\qquad 0 \qquad\qquad : p_{\lambda j} = 0,
\end{aligned}$$

$$(r_i,\ g,\ q_\lambda).0 = 0.(r_i,\ g,\ q_\lambda) = 0,$$

and

$$0.0 = 0.$$

We will represent $(r_i,\ g,\ q_\lambda)$ by $\mathrm{conv}(\bar{r_i},\ \bar{g},\ \bar{q_\lambda})$, and $0 \in S$ as $\bar{0}$.

We have, by assumption, an automaton M for checking the composition of elements in G.

It is clear that composition of four elements (i.e. $g_1g_2g_3g_4 = g$) is first-order definable, and as such an automaton M_4 can be constructed for checking it.

Considering composition for the semigroup, it is clear that there are two main factors involved: determining if $p_{\lambda j}$ is 0; and if not, the composition of four elements of the group.

As such, an automaton may be constructed to check composition in the semigroup by merely amending M_4 to account for the outside values that are kept constant, and to include a check as to whether $p_{\lambda j}$ is 0. This is feasible for two reasons: first, as I and Λ are finite sets (in G), there is a maximum length on the code of any of their elements - as such, a finite number of states can ensure they are accounted for; and secondly, the matrix P has only finitely many entries, ensuring that checking if the relevant entry (corresponding to a pair of elements from I and Λ) is 0 involves only a (fixed) finite number of checks. It is clear that accounting for composition with 0 brings no difficulties.

Now assume $S = \mathcal{M}^0[G;\ I,\ \Lambda;\ P]$ has an automatic presentation (M, ϕ).

We need to show that the underlying group G has an automatic presentation. As all the $\mathcal{H}$-classes which are not null are isomorphic to G (see [41]), we only need to show that any one of these has an automatic presentation.

Choose $x \in S$ such that $x^2 \neq 0$. Let $\widetilde{x}$ be the word in the automatic presentation for x. Let $\widetilde{0}$ be the code for 0. Let M be the composition-checking automaton for S, and denote the language of M by $L(M)$ as usual. The $\mathcal{H}$-class containing x is denoted H_x - we will show that this group has an automatic presentation.

Now, denoting the $\mathcal{L}$-class containing x by L_x, and the $\mathcal{R}$-class containing x by R_x, we know from [41] that $H_x = L_x \cap R_x$.

Let

$$M_\circ = \{\text{conv}(w_1, w_2, w_3) : (w_1, w_2, w_3) \in M \times M \times M, \phi(w_1) \circ \phi(w_2) = \phi(w_3)\},$$

i.e. the language representing composition, which is regular as (M, ϕ) is an automatic presentation.

Again from [41] $L_x = Sx \backslash \{0\} = \{s \circ x : s \in S \backslash \{0\}\} \subseteq S$, so we first need to show that the set of representatives for $Sx \setminus \{0\}$ form a regular language. Let

$$M_L = \{\text{conv}(w_1, \widetilde{x}, w_3) \in M_\circ\}.$$

By the second part of Proposition 2.2.3, this language is regular. Now let

$$M'_L = \{w : \text{conv}(w_1, w_2, w) \in M_L\}.$$

By the first part of Proposition 2.2.3, this language is regular, and clearly represents $Sx \setminus \{0\}$.

Similarly, $R_x = xS \setminus \{0\} = \{x \circ s : s \in S \setminus \{0\}\} \subseteq S$, so we first need to show that the set of codes for xS form a regular language. Let

$$M_R = \{\text{conv}(\widetilde{x}, w_2, w_3) \in M_\circ\}.$$

By the second part of Proposition 2.2.3, this language is regular. Now let

$$M'_R = \{w : \text{conv}(w_1, w_2, w) \in M_R\}.$$

By the first part of Proposition 2.2.3, this language is regular, and clearly represents $xS \setminus \{0\}$.

As the regular language M'_L represents L_x, and the regular language M'_R represents R_x, the language $M'_L \cap M'_R$ represents H_x. By Proposition 2.2.2, this language is regular. $\square$

Remark 5.2.7. Theorem 5.2.5 matches the case of automatic completely simple semigroups: if S is a finitely generated completely-simple semigroup $M[H; I, J; P]$, then S is automatic if and only if the group H is automatic. See [11].

If we allow the G in the definition of Rees matrix semigroups to be a semigroup, it is clear that the 'if' direction of the previous Theorems generalises (with 'is virtually abelian' replaced by 'has an automatic presentation'). The analogous problem for automatic semigroups is investigated in [22].

5.3 Inverse Semigroups

Another interesting class of semigroups, with wide relevance (see [49]), is the class of inverse semigroups. A semigroup is called *inverse* if for every element s there is a *unique* element s' such that $s = ss's$ and $s' = s'ss'$. We shall denote this element s^{-1} - note that all groups are inverse semigroups, so this notation is not likely to cause too much confusion. As the function that sends s to s^{-1} is first-order definable, we shall implicitly include $^{-1}$ in the signature.

Following [57], we will begin by looking at inverse semigroups with respect to Grigorchuk's notion of finite index from the previous chapter. In particular, if a subsemigroup of finite index satisfies a property χ then the semigroup is said to be *virtually* χ. The limitations of this generalisation of finite index from groups will soon become apparent.

Proposition 5.3.1. *There exists:*

- *A finitely generated inverse semigroup with an automatic presentation that is not virtually commutative.*

- *A finitely generated virtually commutative inverse semigroup without an automatic presentation.*

Proof. Firstly, take the bicyclic monoid $B = \langle a, b : ab = \lambda \rangle$. It has an automatic presentation as we will see in Subsection 5.3.1, but according to [57] it is not even virtually (Mal'cev) nilpotent, never mind virtually commutative. Secondly, any semigroup with a zero will of course be virtually trivial, and therefore virtually commutative - as such, take any group without an automatic presentation and add a zero. □

Inverse semigroups naturally have a partial order, with $s \leq t$ when $s = te$ for some idempotent e. This order is clearly first-order definable, and so will inherit an automatic presentation as a structure in itself - see [46] for results concerning partial orders with automatic presentations. Note that this partial order is equality exactly when the semigroup is a group, see [49].

5.3.1 The Bicyclic Monoid

Recall the bicyclic monoid from Section 2.4.1: it is an inverse semigroup, and has the following presentation:

$$\langle a,\ b :\ ab = \lambda \rangle.$$

Elements of this semigroup consist of a string of b symbols, followed by a string of a symbols. Composition is given by

$$b^i a^j \circ b^k a^l = \begin{cases} b^i a^{l+(j-k)} & \text{if } j \geq k \\ b^{i+(k-j)} a^l & \text{if } j < k \end{cases}.$$

Proposition 5.3.2. *The bicyclic monoid has an automatic presentation.*

Proof. For $x \in \mathbb{N}$, let $\mathrm{rb}(x)$ denote x in binary notation. Begin by representing $b^i a^j$ with $\mathrm{conv}(rb(i),\ rb(j))$.

For the composition automaton, take notation as above. It is clear that we must check that the difference between j and k has been added to the appropriate outer value i or l. This can be accomplished as follows. Fix a start state (which is also a final state). Consider the automaton reading the six binary values. While the binary symbols of the inner pair j and k are equal, note that the difference between j and k in binary will be 0. As such, begin by looping on the start state, ensuring the two values for the product (the last two binary values) are identical to the outer pair of values i and l respectively. As soon as the binary values of the inner pair j and k differ, we can tell which is greater as follows. Note that if the current binary symbols of j and k differ, their binary difference at this point must be 1. As such, it is at this point that we must begin to check that this difference is being added to one of the two binary values of the product. If the b value of the first element, i, is different from the b value of the product, then the difference must be being added to i, and so k must be greater than j. Note that it is irrelevant as to which of the currently read binary symbols is greater: it is the effect on the product that gives us the information. Knowing this, we can now branch the machine off into two halves, one for $j > k$ and the other for $j < k$. It is now just a case of ensuring that the difference between j and k is added to the binary value of the (now specified) b or a in the product. $\square$

We now consider some subsemigroups of the bicyclic monoid that will be useful in the next subsection. First though, a lemma and a proposition. If S is a semigroup, then we denote its set of idempotents $E(S)$.

Lemma 5.3.3. *Let S be an inverse semigroup; then, $E(S)$ is a subsemigroup of S.*

Proof. $E(S)$ is commutative in an inverse semigroup, from Theorem 3 in [49]. Let $e, f \in E(S)$; then, ef is in $E(S)$ as:

$$(ef)^2 = efef = eeff = ef.$$

$\square$

Proposition 5.3.4. *Let S be an inverse semigroup; then, $E(S)$ has an automatic presentation.*

Proof. $E(S)$ is clearly first-order definable. $\square$

Let B denote the bicyclic monoid. The idempotents of B are all the pairs $b^n a^n$, and so $E(S) = \{b^n a^m : n = m\}$. Let $E_m = \{b^0 a^0, \ldots, b^{m-1} a^{m-1}\} \subseteq B$. For $d \in \mathbb{N}$, non-zero, define

$$I_{(m,d)} = \{b^r a^s \in B : m \leq r, s \text{ and } r \equiv s \pmod{d}\} \subseteq B.$$

Now, define

$$B_{(m,d)} = E_m \cup I_{(m,d)}.$$

Lemma 5.3.5. *$B_{(m,d)}$ is a subsemigroup of B.*

Proof. We need to show that $B_{(m,d)}$ is *closed*, that is, show that the product of any two elements of $B_{(m,d)}$ is also in $B_{(m,d)}$.

First, E_m is closed. Assume $i \geq j$. Now, $b^i a^i \circ b^j a^j = b^i a^{j+(i-j)} = b^i a^i$. Similarly for $i < j$.

Second, $I_{(m,d)}$ is closed. Let $b^r a^s, b^u a^v \in I_{(m,d)}$. Assume $s \geq u$. Now, $b^r a^s \circ b^u a^v = b^r a^{v+(s-u)}$. By the definition of $I_{(m,d)}$, $s \equiv r \pmod{d}$ and $u \equiv v \pmod{d}$. So, $s - u \equiv r - v \pmod{d}$, and we can conclude that $v + (s-u) \equiv r \pmod{d}$. As $v + (s-u) \geq v \geq m$, $b^r a^{v+(s-u)} \in I_{(m,d)}$. Similarly for $s < u$.

Finally, we need to show that the product of a member of E_m with a member of $I_{(m,d)}$ is contained within $B_{(m,d)}$. Let $b^r a^s \in I_{(m,d)}$ and $b^i a^i \in E_m$. Note that, by definition, $s \geq m > i$. So, $b^r a^s \circ b^i a^i = b^r a^{i+(s-i)} = b^r a^s \in I_{(m,d)} \subseteq B_{(m,d)}$. Similarly, $b^i a^i \circ b^r a^s \in I_{(m,d)} \subseteq B_{(m,d)}$. □

Proposition 5.3.6. *$B_{(m,d)}$ has an automatic presentation, for all $m, d \in \mathbb{N}$.*

Proof. We can go via an interpretation into $(\mathbb{N}, +)$:

- The domain formula is $\phi(x, y) := (x = y \wedge x < m) \vee ((x \geq m \wedge y \geq m) \wedge \exists^{0 \bmod d} z(x + z = y \vee y + z = x))$, where

$$a \geq b := \exists c(a = b + c)$$

  and

$$a > b := a \geq b \wedge a \neq b.$$

- The co-ordinate map is $f(x, y) = b^x a^y$.
- Equality is $\theta_=(x_1, x_2; y_1, y_2) := x_1 = y_1 \wedge x_2 = y_2$.
- Composition is

$$\begin{aligned} \theta_\circ(x_1, x_2; y_1, y_2; z_1, z_2) := \quad & (x_2 \geq y_1 \wedge x_1 = z_1 \wedge z_2 = y_2 + (x_2 - y_1)) \\ \vee \quad & (x_2 < y_1 \wedge z_1 = x_1 + (y_1 - x_2) \wedge z_2 = y_2). \end{aligned}$$

□

For a comprehensive study of the subsemigroups of the bicyclic monoid see [23].

5.3.2 Fundamental ω-semigroups

As noted in the proof of Lemma 5.3.3, the set of idempotents in an inverse semigroup is commutative. Following [41], we call this set the *semilattice of idempotents* of the semigroup.

An inverse semigroup is an *ω-semigroup* if its semilattice of idempotents is isomorphic to $\mathbb{N}$ under the reverse order (i.e. $1 > 2$, etc.).

One of the most important congruences on an inverse semigroup is the *maximum idempotent-separating congruence.* It is so called because it is the maximal congruence that, when restricted to the semilattice of idempotents, is equality. It can be defined as:

$$a \ \mu \ b := \forall e \in E(S), \ \ aea^{-1} = beb^{-1}$$

If this congruence is equality *everywhere*, i.e. $a \ \mu \ b$ if and only if $a = b$, the semigroup is called *fundamental.*

Proposition 5.3.7. *Let S be a fundamental ω-semigroup; then, S has an automatic presentation.*

Proof. As shown in [41], if S is a fundamental ω-semigroup then either $S \cong B$ or $S \cong B_{(m,d)}$ for some m and d. So, S has an automatic presentation by either Proposition 5.3.1 or 5.3.6. $\square$

5.4 Miscellaneous

This section will round up the remaining miscellaneous results.

5.4.1 Maximum Group Homomorphic Image

Following the classification for finitely generated groups in Chapter 3, it makes sense to investigate (finitely generated) groups related to semigroups - if we can show that the semigroup having an automatic presentation implies that the group does too, we know that the group must be virtually abelian.

The *maximum group homomorphic image* of a semigroup, if it exists, is the largest group such that there is a surjective homomorphism onto the group from the semigroup. The congruence associated to this homomorphic image is called the *minimum group congruence.* See [15], or [41], Section 5.3, for more information. In some cases, the minimum group congruence is naturally first-order definable. The following definitions are required first.

Definition 5.4.1. *Let S be a semigroup, with E its set of idempotents. A subset K of S is:*

- unitary *if for all $s \in S$ and $k \in K$, $sk \in K$ or $ks \in K \Rightarrow s \in K$;*
- dense *if for all $s \in S$ there exists $x, y \in S$ such that $sx \in K, ys \in K$;*
- reflexive *if for all $a, b \in S$, $ab \in K \Rightarrow ba \in K$.*

The subsemigroup generated by K is denoted $\langle K \rangle$.

Definition 5.4.2. *Let S be a semigroup, with E its set of idempotents. S is:*

- *regular if for all $s \in S$ there exists $s' \in S$ such that $ss's = s$.*
- *π-regular if for all $s \in S$, there exists $n \in N$ and $s' \in S$ such that $s^n s' s^n = s^n$.*
- *strongly π-inverse if it is π-regular and E is commutative.*

- *a unitary dense E-semigroup if E is a subsemigroup, and E is unitary and dense.*
- *a strongly $\langle E \rangle$ unitary dense monoid if it is a monoid, and $\langle E \rangle$ is reflexive, unitary and dense.*

Using a variety of results from the literature, we get the following immediately:

Proposition 5.4.3. *Let S be either*

- *a regular semigroup;*
- *a strongly π-inverse semigroup;*
- *a unitary dense E-semigroup; or*
- *a strongly $\langle E \rangle$ unitary dense monoid.*

Assume S has an automatic presentation; then, the maximum group homomorphic image of S exists and, if it is finitely generated, it is virtually abelian.

Proof. The minimum group congruence exists, and is first-order definable, for each of these classes - see [31] and [51] - and so by Corollary 2.3.6 the maximum group homomorphic image, if finitely generated, will have an automatic presentation. □

Corollary 5.4.4. *Let S be the free inverse monoid on the (finite) set A; then, S has an automatic presentation if and only if $|A| = 1$.*

Proof. The maximum group homomorphic image of S is the free group on A - see [18]. By Exercise 42, Chapter 5 of [41], if $|A| = 1$ then

$$S \cong \{(r, s, k) \in \mathbb{Z}^3 : r \geq 0, s \geq 0, -s \leq k \leq r\}$$

with

$$(r, s, k)(r', s', k') = (\max\{r, r' + k\}, \max\{s, s' - k\}, s + s').$$

As addition, subtraction, $\geq$, max, etc. can all be checked by a finite automaton, it is clear that S has an automatic presentation. If $|A| \neq 1$, then the free group on A is not virtually abelian - the result then follows from the above proposition as S is an inverse (and therefore regular) semigroup. $\square$

5.4.2 Semigroups with One Defining Relation

Proposition 5.4.5. *A semigroup S with one defining relation has an automatic presentation if and only if S is generated by two elements, say a and b, and defined by one of:*

$$\begin{aligned} a &= b; & ab &= ba;\ ab = b^k;\ ba = b^k; \\ ab &= aba; & ba &= aba;\ ab = bab^2; \\ ba &= b^2ab; & a &= bab;\ a^2 = b^2. \end{aligned}$$

Proof. According to [72], these are exactly the semigroups with decidable first-order theory. The proof involves a first-order interpretation into $(\mathbb{N}, +)^k$ for some appropriate $k \in N$, and hence they all have an automatic presentation. $\square$

5.4.3 Infinitely Generated Semigroups

There has been some interest in the literature in considering infinitely generated semigroups. The following results represent most of what is known.

Proposition 5.4.6 (Blumensath [5])**.** $(\mathbb{N}, \times)$ *does not have an automatic presentation.*

Remark 5.4.7. In Remark 2.3.8, we mentioned that structures presentable by tree automata have been considered. It is noted in [5] that, as $(\mathbb{N}, \times)$ has a tree-automatic presentation, the preceding proposition serves to separate the two different types of presentation.

Theorem 5.4.8 (Khoussainov, Nies, Rubin, Stephan [43]). *Let M be a monoid containing $(\mathbb{N}, \times)$ as a submonoid; then, M does not have an automatic presentation.*

Corollary 5.4.9 (Khoussainov, Nies, Rubin, Stephan [43]). *The free abelian group of countably infinite rank does not have an automatic presentation.*

Proof. The free abelian group of countably infinite rank, or equivalently $(\mathbb{Q}^+, \times)$, contains $(\mathbb{N}, \times)$ as a submonoid. $\square$

Corollary 5.4.10 (Khoussainov, Nies, Rubin, Stephan [43]). *The monoid of $k \times k$ matrices over $\mathbb{N}$ does not have an automatic presentation.*

Open Question 5.4.11 (Khoussainov, Nerode [42]). Does the group of rationals, $(\mathbb{Q}, +)$, have an automatic presentation?

There are some infinitely generated groups known to have automatic presentations:

Proposition 5.4.12 (Khoussainov, Nies, Rubin, Stephan [43]). *The Prüfer groups $\mathbb{Q}_p/\mathbb{Z}$ all have automatic presentations.*

We can place this result into a potentially interesting context.

Definition 5.4.13. *A group G is* finitely cogenerated *if there exists a finite subset $F \subseteq G$ such that for every non-trivial subgroup $H \leq G$, $H \cap F \neq \emptyset$.*

Proposition 5.4.14 (De Cornulier, Guyot, Pitsch [17]). *Let G be an abelian group; then, G is finitely cogenerated if and only if*

$$G \cong C_1 \times \ldots \times C_m \times P_1 \times \ldots \times P_n$$

where C_i is a finite cyclic group, and P_j is a Prüfer group.

Corollary 5.4.15. *Let G be an abelian group; if G is finitely cogenerated, then G has an automatic presentation.*

In the case of semigroups, it is easy to produce pathological examples.

Definition 5.4.16.

- *A* null *semigroup is a semigroup with zero, such that the product of any two elements is the zero.*
- *A* semilattice *is a commutative semigroup where all elements are idempotents.*

Proposition 5.4.17.

- *(Infinitely generated) null semigroups have automatic presentations.*
- *(Infinitely generated) finitely related semilattices have automatic presentations.*

Proof. In null semigroups, composition is trivial.

Let $G = \{a_i : i \in \mathbb{N}\}$ be the set of generators for the finitely related semilattice S. As the number of relations is finite,

$$R = \{a_i \in G : a_i \text{ features in a relation}\}$$

is finite. Without loss of generality, assume $R = \{a_1, \ldots, a_n\}$. As the semigroup generated by $G \setminus R$ involves no relations, $S \cong \langle R \rangle \times \langle G \setminus R \rangle$. $\langle R \rangle$ is finite, so has an automatic presentation. $G \setminus R$ is coded in binary, with position $k = 1$ if a_{n+k} is present, $k = 0$ otherwise. The composition automaton accepts words where for every tuple if there is a 1 in either the first or second position, then there is a 1 in the third. By closure under direct products, the result is finished. □

Note that for the above classes of semigroups, finitely generated implies finite.

Chapter 6

Cayley Graphs and Automatic Groups

6.1 Automatic Groups and Semigroups

Let S be a semigroup, generated by a set X. Denote the set of (non-trivial) words over X by X^+. Members of X^+ naturally correspond to members of S ($x_1x_2 \ldots x_n \mapsto x_1 \circ x_2 \circ \ldots \circ x_n$) - we shall denote this relationship $\phi : X^+ \rightarrow S$. As such, it is natural to consider S with respect to formal language theory. This is particularly the case as there is much redundancy in X^+ - it is likely that many words will map onto the same element. Let $L \subseteq X^+$ be a language such that $\phi|_L$ is a bijection, so L contains a unique representative for each element in S. Then, L is called a *cross section* of S. If L is regular, then L is a *rational cross section.*

Although having a rational cross section gives us a concrete grasp on the members of S, it gives us only indirect access to composition in S. If we wish to stick with regularity, insisting that full composition also be regular in *any* sense seems likely to leave us just with finite semigroups (although see [30] for a context-free approach). One approach has been to consider just composing with generators. We could insist that, along with a rational cross section L, we have an automaton for each generator accepting pairs $(u, v) \in L^2$ where $\bar{u}\bar{x} = \bar{v}$. This gives us the concept of an *automatic semigroup.*

Originally defined for groups [27], the definition naturally translates to semigroups as explained in [12]. Here is the definition as it appears in [27, 12]:

Definition 6.1.1. *Let S be a semigroup, generated by a finite set X, and let $\phi : X^+ \to S$ be the natural map.*

S is automatic *if there is a regular language $L \subseteq X^+$ such that $\phi|_L$ is surjective, where:*

- *$L_= = \{(w_1, w_2) \in L^2 : \phi(w_1) = \phi(w_2)\}$ is regular; and,*
- *$L_x = \{(w_1, w_2) \in L^2 : \phi(w_1 x) = \phi(w_2)\}$ is regular, for each $x \in X$.*

Remark 6.1.2. To fit in with our earlier discussion it seems natural to insist that L be a rational cross section, i.e. insist that ϕ be bijective. However, the resulting definition would be equivalent - see [12] for details. Definition 6.1.1 is the normal format given, and allows for more scope when looking to show that a particular semigroup is automatic.

Before proceeding, we need to introduce a new structure.

Definition 6.1.3. *Let S be a semigroup, with generating set X. Let $C(S)$ be a (directed, edge-labelled) graph with:*

- *vertex set S; and,*
- *an edge from $s \in S$ to $t \in S$ labelled $x \in X$ if and only if $s \circ x = t$.*

Then, $C(S)$ is called the Cayley graph *of S with respect to X.*

In order to draw out the connections between automatic semigroups and automatic presentations, here is an equivalent definition of automatic semigroups in terms of automatic presentations.

Definition 6.1.4. *Let S be a semigroup, generated by a finite set X, and let $\phi : X^+ \to S$ be the natural map. Let $C(S)$ be the Cayley graph of S with respect to X.*

S is automatic *if $C(S)$ has an automatic presentation (L, ψ) such that $L \subseteq X^+$ and $\psi = \phi|_L$.*

Remark 6.1.5. The significant aspect, of course, is that for automatic presentations in general, L may be any language; here, it is restricted to being from a pre-specified source, and corresponding to the structure in a pre-specified way.

6.1.1 Automatic Presentations versus Automatic Groups

The theory of automatic groups was mentioned in the introduction as one of the motivations for studying structures with automatic presentations. Naturally the connections between the two notions have been remarked upon elsewhere; see [7] for example, or [42] for the comments following Proposition 2.11 there (which we have quoted as Proposition 3.2.3 above).

We make some further comments on the relationship between these concepts here. It is proved in [27] that a finitely generated abelian group is automatic. The proof is constrained to using encodings of elements as words in the generators (see Definition 6.1.4, and in particular the following remark), but only needs to produce automata representing composition with generators; on the other hand, the proof in [42] that such a group has an automatic presentation permits a different encoding of the elements but needs an automaton recognizing composition of any elements in the group.

We have a similar issue with automatic groups and automatic presentations for Cayley graphs. As can be seen in Definition 6.1.4, if G is an automatic group, then we have an automatic presentation for the Cayley graph $C(G)$ of G where the encodings of the elements are again words in the generators of G; however, in general an automatic presentation for $C(G)$ need not use such an encoding.

This distinction is significant. Let H be the *Heisenberg group*, i.e. the group of matrices

$$\left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z} \right\}.$$

It is noted in [7] that the Cayley graph $C(H)$ has an automatic presentation, but that H is not an automatic group. As H is finitely generated but not virtually abelian, it also does not have an automatic presentation (as a group) by Theorem 3.4.5.

We also note that the choice of generating set for a group is not significant when considering whether its Cayley graph has an automatic presentation:

Proposition 6.1.6. *If G is a group with finite generating sets X and Y, then the Cayley graph of G with respect to X has an automatic presentation if and only if the Cayley graph of G with respect to Y has an automatic presentation.*

Proof. If $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_n\}$, then we can demonstrate a sequence of finite generating sets for G:

$$X, X \cup \{y_1\}, X \cup \{y_1, y_2\}, \ldots, X \cup \{y_1, y_2, \ldots, y_{n-1}\}, X \cup Y,$$

$$\{x_1, x_2, \ldots, x_{m-1}\} \cup Y, \{x_1, x_2, \ldots, x_{m-2}\} \cup Y, \ldots, \{x_1\} \cup Y, Y$$

Note that we have only added or deleted one generator at a time.

It is easy to see that deleting a redundant generator does not affect the existence of an automatic presentation for a Cayley graph: we are simply omitting one of the relations in our structure. On the other hand, if we have a generating set $A = \{a_1, \ldots, a_k\}$ and we add a new generator b, then we can note that $b = a_{i_1} a_{i_2} \ldots a_{i_k}$ with $a_{i_j} \in A$, and the new relation R_b we have introduced is first-order definable with respect to A, i.e.

$$R_b = \{(x, y) : x \circ a_{i_1} a_{i_2} \ldots a_{i_k} = y\}.$$

□

Restricting ourselves to finitely generated groups, let `AutoPres` represent the class of groups with automatic presentations, let `Automatic` represent the class of automatic groups, and finally let `CayleyAutoPres` represent the class of groups whose Cayley graphs have automatic presentations. We have

Theorem 6.1.7. `AutoPres` $\subsetneq$ `Automatic` $\subsetneq$ `CayleyAutoPres`.

Proof. All virtually abelian groups are automatic, but there are plenty of groups (such as free groups) that are automatic but do not have automatic presentations; this gives the first (proper) inclusion. The automata required for automatic groups give automatic presentations for the Cayley graphs of these groups; however, as noted previously the Cayley graph of the Heisenberg group has an automatic presentation, but the Heisenberg group is not automatic. This gives the second (proper) inclusion. □

6.2 Unary Presentations for Cayley Graphs

We consider once again automatic presentations with a single symbol. The following is from [5]:

Proposition 6.2.1. *Let G be a finitely generated group; then, $C(G)$ has a unary automatic presentation if and only if G is virtually cyclic.*

This proposition gives an interesting connection with the word problem for groups:

Definition 6.2.2. *Let G be a group, with generating set X. Let $\phi : X^+ \to G$ be the natural mapping. The* word problem *for G is the language*

$$WP(G, X) = \{w \in X^+ : \phi(w) = 1\}$$

i.e. those strings of generators whose product is the identity.

The word problem $WP(G, X)$ is called one counter *if it is accepted by a one counter pushdown automaton.*

See [58] for more on the word problem for groups, and [4] for information on one counter pushdown automata.

Theorem 6.2.3 (Herbst [35])**.** *A finitely generated group has a one-counter word problem if and only if it is virtually cyclic.*

Corollary 6.2.4. *A finitely generated group has a one-counter word problem if and only if its Cayley graph has a unary automatic presentation.*

6.3 Connections with Automatic Semigroups

Theorem 6.1.7 draws out the connections between groups with automatic presentation and automatic groups. The following results attempt a similar analysis with respect to semigroups.

As may be expected considering the extent of semigroups that are not groups, there is no direct generalisation of Theorem 6.1.7 (or the classification of Theorem 3.4.5 - see Proposition 5.3.1) for the class of all semigroups. In [39], a finitely generated commutative semigroup that is not automatic is demonstrated; by Theorem 5.1.1, all finitely generated commutative semigroups have an automatic presentation. As such, there are semigroups that have an automatic presentation but are not automatic. There are clearly semigroups (in particular groups) that are automatic but do not have an automatic presentation. The class of finitely generated semigroups with automatic presentations and the class of automatic semigroups are, then, incomparable. Both of these classes are contained in the class of finitely generated semigroups whose Cayley graph has an automatic presentation.

It may be possible to generalise Theorem 6.1.7 if we restrict the class of semigroups to cancellative semigroups. As with groups, we will consider only finitely generated semigroups. Let `AutoPresCancSemi` represent the class of cancellative semigroups with automatic presentations, let `AutomaticCancSemi` represent the class of automatic cancellative semigroups, and finally let `CayleyAutoPresCancSemi` represent the class of cancellative semigroups whose Cayley graphs have automatic presentations.

Conjecture 6.3.1.

$$\texttt{AutoPresCancSemi} \subsetneq \texttt{AutomaticCancSemi} \subsetneq \texttt{CayleyAutoPresCancSemi}$$

The second containment is clear:

Lemma 6.3.2.

$$\texttt{AutomaticCancSemi} \subsetneq \texttt{CayleyAutoPresCancSemi}$$

Proof. As in Theorem 6.1.7, the automata required for automatic semigroups give automatic presentations for the Cayley graphs of these semigroups; the group example makes the containment proper. □

To finish proving this conjecture, it is enough to prove the following:

Conjecture 6.3.3. *All finitely generated subsemigroups of finitely generated virtually abelian groups are automatic.*

We have seen, in Theorem 4.2.6, that if $S \in$ `AutoPresCancSemi` then S is a finitely generated subsemigroup of a finitely generated virtually abelian group - Conjecture 6.3 would then give the first inclusion, any group example making it proper.

The following result, from [9], goes part way to solving the conjecture:

Theorem 6.3.4 (Cain). *Let S be a finitely generated subsemigroup of an abelian group; then, S is automatic.*

6.4 Algorithms

One of the oft-mentioned motivations for the study of automatic groups (and semigroups) is the decidability results which fall out of the definition. We show here that, for some of the results, it is only the existence of appropriate automata that is needed - the use of words over generators is, perhaps slightly surprisingly, unnecessary.

Let S be a semigroup, generated by a set X. Recall the natural mapping $\phi : X^+ \to S$ from earlier. The *word problem* of S is the problem of deciding whether two words in X^+ are mapped to the same element in S. If this problem is decidable for a particular semigroup, we say that the semigroup has a decidable word problem. Similarly, if the word problem of a semigroup is, say, decidable in polynomial time, we say the semigroup has a polynomial time word problem.

Proposition 6.4.1. *Let S be a finitely generated semigroup whose Cayley graph has an automatic presentation; then, S has a quadratic word problem.*

Proof. Let S have generating set $\{x_1, \dots, x_k\}$. Let $(C, X_1, \dots, X_k)$ be the Cayley Graph of S with respect to this generating set. Let (L, θ) be an automatic presentation of C, and for each x_i let $\bar{x}_i \in L$ be some word such that $\theta(\bar{x}_i) = x_i$. Let $l = \max\{|\bar{x}_1|, \dots, |\bar{x}_k|\}$. Let c denote the maximum number of states of the automata in this presentation, i.e. the automata for L, $L_=$, L_{X_1},...,L_{X_k}.

Let $x_{r_1}x_{r_2}\dots x_{r_m}$ and $x_{s_1}x_{s_2}\dots x_{s_n}$ be words over the generators of S. The following algorithm decides, as required, if $x_{r_1}x_{r_2}\dots x_{r_m} = x_{s_1}x_{s_2}\dots x_{s_n}$.

Find $u_2 \in L$ such that $\text{conv}(\bar{x}_{r_1}, u_2) \in L_{X_{r_2}}$ with $|u_2| \leq |\bar{x}_{r_1}| + c$.

For $i = 3$ to n:

Find $u_i \in L$ such that $\text{conv}(u_{i-1}, u_i) \in L_{X_{r_i}}$ with $|u_i| \leq |u_{i-1}| + c$.

Go to the next i.

Find $v_2 \in L$ such that $\text{conv}(\bar{x}_{s_1}, v_2) \in L_{X_{s_2}}$ with $|v_2| \leq |\bar{x}_{s_1}| + c$.

For $j = 3$ to m:

Find $v_j \in L$ such that $\text{conv}(v_{j-1}, v_j) \in L_{X_{s_j}}$ with $|v_j| \leq |v_{j-1}| + c$.

Go to the next j.

If $(u_n, v_m) \in L_=$, then

$$x_{r_1}x_{r_2}\dots x_{r_m} = x_{s_1}x_{s_2}\dots x_{s_n}$$

else

$$x_{r_1}x_{r_2}\dots x_{r_m} \neq x_{s_1}x_{s_2}\dots x_{s_n}.$$

This algorithm is in $O(\max\{n, m\}^2)$: we can then find each u_i and v_i in $O((i-1)c + l)$; we can compare (u_n, v_m) in $O((\max\{n, m\} - 1)c)$; and so the algorithm is in

$$\begin{aligned}
& O(c + l + 2c + l + \ldots + (\max\{n, m\} - 1)c + l) \\
= \;& O([(\max\{n, m\} - 1)\max\{n, m\}/2]c + (\max\{n, m\} - 1)l) \\
= \;& O(\max\{n, m\}^2).
\end{aligned}$$

□

Appendix A

Automata Construction for Virtually Abelian Groups

A.1 Preliminaries

In Chapter 3, it is proved that all finitely generated virtually abelian groups have automatic presentations - Theorem 3.2.4. We now follow up the promise of Remark 3.2.6 by showing how to construct appropriate automata.

First, some results on binary computation. The algorithm for binary addition of n numbers looks like this:

Algorithm A.1.1. *INPUT:*

$$\begin{aligned} b_1 &= d_{1,1} \ldots d_{1,l} \\ b_2 &= d_{2,1} \ldots d_{2,l} \\ &\vdots \\ b_n &= d_{n,1} \ldots d_{n,l} \end{aligned}$$

$b_i \in \{0,1\}^\star, d_{i,j} \in \{0,1\}$

ALGORITHM:

Let $c_0 = 0$

FOR $i = 1$ *to* $l + 1$

Let $t_i = \Sigma_{j=1}^{n} d_{j,i} + c_{i-1}$

IF t_i *is even THEN* $a_i = 0$ *ELSE* $a_i = 1$

Let $c_i = \frac{t_i - a_i}{2}$

NEXT i

OUTPUT:

$$a = a_1 \ldots a_{l+1}$$

We need to show that there is a bound on the values of the c_i - these will be the basis for the states of the constructed automata.

Proposition A.1.2. *Keep notation as for the algorithm above, in particular let* n *be the (fixed) amount of numbers being input. Let* $\bar{c}_i$ *be the maximum attainable value of* c_i *in any run of the algorithm, if such a maximum is defined. Then:*

$$\begin{aligned} \bar{c}_0 &= 0 \\ \bar{c}_{i+1} &= \frac{n + \bar{c}_i}{2} \end{aligned}$$

Proof. We shall proceed by induction. The base case, $\bar{c}_0 = 0$, is trivial.

Now, assume that $\bar{c}_k$ is the maximum attainable value of c_k in any run of the algorithm.

Note that $c_{k+1} = \frac{t_{k+1} - a_{k+1}}{2}$, so to find the maximum possible value for c_{k+1} we need to maximise $t_{k+1} - a_{k+1}$.

Now $t_{k+1} = \Sigma_{j=1}^{n} d_{j,k+1} + c_k$, so the maximum possible value for t_{k+1} is $n + \bar{c}_k$. We need to show that this is the maximum possible value for $t_{k+1} - a_{k+1}$.

First, consider the case when $t_{k+1} \le (n-2) + \bar{c}_k$. Increasing t_{k+1} by 2 has no effect on a_{k+1}, and as such this will produce an increased value of $t_{k+1} - a_{k+1}$. So, the maximum possible value of $t_{k+1} - a_{k+1}$ must occur with $t_{k+1} > (n-2) + \bar{c}_k$.

Assume $n + \bar{c}_k$ is even.

$$\begin{aligned} t_{k+1} = (n-1) + \bar{c}_k &\Rightarrow t_{k+1} - a_{k+1} = (n-1) + \bar{c}_k + 1 = n + \bar{c}_k \\ t_{k+1} = n + \bar{c}_k &\Rightarrow t_{k+1} - a_{k+1} = n + \bar{c}_k \end{aligned}$$

Assume $n + \bar{c}_k$ is odd.

$$\begin{aligned} t_{k+1} = (n-1) + \bar{c}_k &\Rightarrow t_{k+1} - a_{k+1} = (n-1) + \bar{c}_k \\ t_{k+1} = n + \bar{c}_k &\Rightarrow t_{k+1} - a_{k+1} = n + \bar{c}_k - 1 = (n-1) + \bar{c}_k \end{aligned}$$

All cases covered, we may conclude that the maximum possible value for $t_{k+1} - a_{k+1}$ is $n + \bar{c}_k$. □

Theorem A.1.3. *Let $n \ge 1$. For all i, $\bar{c}_i \le n - 1$.*

Proof. Assume for some i we have $\bar{c}_i = \frac{n+\bar{c}_{i-1}}{2} \ge n$. Then,

$$\begin{aligned} \tfrac{n+\bar{c}_{i-1}}{2} &\ge n \\ \therefore\ n + \bar{c}_{i-1} &\ge 2n \\ \therefore\ \bar{c}_{i-1} &\ge n. \end{aligned}$$

So, by induction, if there is an i such that $\bar{c}_i$ is greater than or equal to n, then $\bar{c}_j > n$ for $j < i$. But $n \ge 1$ and $\bar{c}_0 = 0$, a contradiction.

We have proved so far that $\bar{c}_i < n$. $\bar{c}_i$ is integer-valued though, so we can derive $\bar{c}_i \le n - 1$ as required. □

We are now in a position to work towards the main result. We begin by investigating the structure of finitely generated virtually abelian groups.

Let G be a finitely generated virtually abelian group. Let

$$A = \langle x_1, x_2, \dots, x_n \rangle$$

be a normal subgroup of G of finite index isomorphic to $\mathbb{Z}^n$ and then let $T = \{t_1, t_2, \dots, t_k\}$ be a set of coset representatives for A in G. Each element of G is of the form $t_i x_1^{a_1} \dots x_n^{a_n}$, $a_i \in \mathbb{Z}$, $t_i \in T$. Group composition, then, has the form $t_i x_1^{a_1} \dots x_n^{a_n} \circ t_j x_1^{b_1} \dots x_n^{b_n} = t_k x_1^{c_1} \dots x_n^{c_n}$. It is clear, as A is normal, that the important aspect of this composition is the action of t_j. Let $g_i : \mathbb{Z}^n \to \mathbb{Z}^n$ be the function $g_i(a_1, a_2 \dots, a_n) = (a'_1, a'_2 \dots, a'_n)$ given by $x_1^{a_1} \dots x_n^{a_n} t_i = t_i x_1^{a'_1} \dots x_n^{a'_n}$.

Proposition A.1.4. *g_i is an automorphism of $\mathbb{Z}^n$.*

Proof. Well-defined and injective:

$$\begin{aligned}
(a_1, \dots, a_n) = (b_1, \dots, b_n) &\Leftrightarrow x_1^{a_1} \dots x_n^{a_n} = x_1^{b_1} \dots x_n^{b_n} \\
&\Leftrightarrow x_1^{a_1} \dots x_n^{a_n} t_i = x_1^{b_1} \dots x_n^{b_n} t_i \\
&\Leftrightarrow t_i x_1^{a'_1} \dots x_n^{a'_n} = t_i x_1^{b'_1} \dots x_n^{b'_n} \\
&\Leftrightarrow g_i(a_1, \dots, a_n) = g_i(b_1, \dots, b_n)
\end{aligned}$$

Surjective:

Consider $(a_1, \dots a_n) \in \mathbb{Z}^n$.

$$\begin{aligned}
& A && \lhd G \\
\Rightarrow \quad & t_i A && = A t_i \\
\Rightarrow \quad & t_i x_1^{a_1} \dots x_n^{a_n} && = x_1^{b_1} \dots x_n^{b_n} t_i \\
\Rightarrow \quad & (a_1, \dots a_n) && = g_i(b_1, \dots, b_n).
\end{aligned}$$

Homomorphic:

Let

$$\begin{aligned}(c_1, \dots, c_n) &= g_i(a_1 + b_1, \dots, a_n + b_n)\\ (a'_1, \dots, a'_n) &= g_i(a_1, \dots, a_n)\\ (b'_1, \dots, b'_n) &= g_i(b_1, \dots, b_n).\end{aligned}$$

We have

$$\begin{aligned}t_i x_1^{c_1} \dots x_n^{c_n} &= x_1^{a_1+b_1} \dots x_n^{a_n+b_n} t_i\\ &= x_1^{a_1} x_1^{b_1} \dots x_n^{a_n} x_n^{b_n} t_i\\ &= x_1^{a_1} \dots x_n^{a_n} x_1^{b_1} \dots x_n^{b_n} t_i\\ &= x_1^{a_1} \dots x_n^{a_n} t_i x_1^{b'_1} \dots x_n^{b'_n}\\ &= t_i x_1^{a'_1} \dots x_n^{a'_n} x_1^{b'_1} \dots x_n^{b'_n}\\ &= t_i x_1^{a'_1+b'_1} \dots x_n^{a'_n+b'_n}.\end{aligned}$$

So

$$\begin{aligned}g_i(a_1 + b_1, \dots, a_n + b_n) &= (c_1, \dots, c_n)\\ &= (a'_1 + b'_1, \dots a'_n + b'_n)\\ &= (a'_1, \dots a'_n) + (b'_1, \dots b'_n)\\ &= g_i(a_1, \dots, a_n) + g_i(b_1, \dots, b_n).\end{aligned}$$

□

Proposition A.1.5. $\mathrm{Aut}(\mathbb{Z}^n) = \mathrm{GL}(n, \mathbb{Z})$

Proof. For our requirements, we need only demonstrate that members of $\mathrm{Aut}(\mathbb{Z}^n)$ can be represented as matrices. View $\mathbb{Z}^n$ as an n-dimensional vector space over $\mathbb{Z}$, and let $\theta \in \mathrm{Aut}(\mathbb{Z}^n)$. We shall say that

$$\theta((0, \dots, 1, \dots, 0)) = (a_{1,i}, \dots, a_{n,i})$$

where 1 is in the ith position.

Then,

$$\begin{aligned}
\theta((\delta_1,\ldots,\delta_n)) &= \delta_1\theta((1,\ldots,0)) + \ldots + \delta_n\theta((0,\ldots,1)) \\
&= \delta_1(a_{1,1},\ldots,a_{1,n}) + \ldots + \delta_n(a_{n,1},\ldots,a_{n,n}) \\
&= (\delta_1 a_{1,1},\ldots,\delta_1 a_{1,n}) + \ldots + (\delta_n a_{n,1},\ldots,\delta_n a_{n,n}) \\
&= (\delta_1 a_{1,1} + \ldots + \delta_n a_{n,1},\ldots,\delta_1 a_{1,n} + \ldots + \delta_n a_{n,n}) \\
&= (\delta_1,\ldots,\delta_n)\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{pmatrix}.
\end{aligned}$$

□

A.2 Construction

Proposition A.2.1. *If G is a finite extension of $\mathbb{Z}^n$, then G has an automatic presentation.*

Proof. If G is a finite extension of $\mathbb{Z}^n$, then $\mathbb{Z}^n \lhd G$, $|G : \mathbb{Z}^n| = m \in \mathbb{N}$. As before, let T be a set of coset representatives of $\mathbb{Z}^n$ in G, i.e. $|T| = m$. Each element of G is then of the form

$$t_i x_1^{a_1} \ldots x_n^{a_n}$$

with

$$t_i \in T,\ a_i \in \mathbb{Z}.$$

We first need to construct a language to represent these elements. Let the alphabet be

$$\begin{aligned} & \{t_i : i \in \{0, 1, \dots, |T| - 1\}\} \\ \cup \ & \{(\pm_1, \dots, \pm_n) : \pm_j \in \{+, -\}\} \\ \cup \ & \{(\beta_1, \dots \beta_n) : \beta_k \in \{0, 1\}\}. \end{aligned}$$

We now demonstrate how each element is represented.

- The first symbol is t_i.
- The second symbol is $(\pm_1, \dots, \pm_n)$, where $\pm_i = +$ if $a_i \geq 0$ and $\pm_i = -$ if $a_i \leq 0$.
- The absolute value of each a_i is then converted to binary. Let $a_{i_1} \dots a_{i_{l_i}}$ represent this conversion, $a_{j_k} \in \{0, 1\}$. Let $l = \max\{l_1, \dots l_n\}$. The $m + 2$th symbol of the word is then $(\beta_1, \dots \beta_n)$ where $\beta_i = a_{i_m}$ for $m \leq l_i$ and 0 otherwise.
- Repeat for all $m \leq l$.

Although this may seem slightly complicated, it is actually straightforward: for example $tx_1^3 x_2^{-4}$ is represented by:

	$+$	1	1	0
t	$-$	0	0	1

Note that there are multiple representations when some a_i is 0; either $+$ or $-$ and any number of zeros. It is clear that an equality checking automaton is easily constructible. As $|T|$ and $a_1, \dots, a_n$ are finite, the language of the representations for elements is clearly accepted by a finite automaton.

Now we need to show that group composition is accepted by a finite automaton. Composition is of the form $t_i x_1^{a_1} \dots x_n^{a_n} . t_j x_1^{b_1} \dots x_n^{b_n} = t_k x_1^{c_1} \dots x_n^{c_n}$

given by:

$$\begin{aligned} t_i x_1^{a_1}\dots x_n^{a_n}.t_j x_1^{b_1}\dots x_n^{b_n} &= t_i t_j x_1^{a'_1}\dots x_n^{a'_n} x_1^{b_1}\dots x_n^{b_n} \\ &= t_i t_j x_1^{a'_1+b_1}\dots x_n^{a'_n+b_n}. \end{aligned}$$

Now, $t_i t_j \in G$, so $t_i t_j = t_k x_1^{c_1}\dots x_n^{c_n}$

$$\begin{aligned} t_i t_j x_1^{a'_1+b_1}\dots x_n^{a'_n+b_n} &= (t_k x_1^{c_1}\dots x_n^{c_n}) x_1^{a'_1+b_1}\dots x_n^{a'_n+b_n} \\ &= t_k x_1^{a'_1+b_1+c_1}\dots x_n^{a'_n+b_n+c_n}. \end{aligned}$$

Let there first be a state labelled S, the start state. Add $|T|^2$ new states, and add a transition from S onto each of them. Label each transition with a different member of $\{(t_u, t_v, t_w) : t_u.t_v = t_w x_1^{c_1}\dots x_n^{c_n}\}$ and name the state it reaches similarly. This allows each combination of coset representatives to be dealt with separately.

Now, from each of the states (t_u, t_v, t_w) create 2^{3n} transitions, each to a new state(i.e. one for every possible combination of signs, as can be deduced from the labels specified next). In each batch of 2^{3n} use a different member of

$$\{(\pm_1^1, \dots, \pm_n^1)(\pm_1^2, \dots, \pm_n^2)(\pm_1^3, \dots, \pm_n^3) : \pm_j^i \in \{+, -\}\}$$

to name each transition, and name the state reached

$$[(t_u, t_v, t_w); (\pm_1^1, \dots, \pm_n^1)(\pm_1^2, \dots, \pm_n^2)(\pm_1^3, \dots, \pm_n^3)]$$

depending on the two arrows traversed to reach it.

For each of these states, complete the following:

1. If the state's name starts (t_u, t_v, t_w), and $t_u.t_v = t_w x_1^{c_1}\dots x_n^{c_n}$, we need to ensure that we 'add on' the extra $x_1^{c_1}\dots x_n^{c_n}$. First, we enumerate the sign of the c_i's:

$$c_i^{\pm} = \begin{cases} 0 & \text{if } c_i \geq 0 \\ 1 & \text{if } c_i < 0 \end{cases}$$

Then, convert the absolute value of each of the c_i's into binary. This gives:

$$c_i = b_1^i b_2^i \dots b_{l_i}^i$$

where l_i is the length of c_i in binary and $b_j^i \in \{0,1\}$. For later on, let $m = \max\{l_1, \dots, l_n\}$ and then set $b_j^i = 0$ for $l_i < j \leq m$.

Now we need to encode the signs of the elements that make up the composition. Let

$$\psi_j^k = \begin{cases} 0 & \text{if } \pm_j^k = + \\ 1 & \text{if } \pm_j^k = - \end{cases}.$$

Also, let $\begin{pmatrix} a_{11}^i & \dots & a_{1n}^i \\ \vdots & \ddots & \vdots \\ a_{1n}^i & \dots & a_{nn}^i \end{pmatrix}$ be the matrix representing the action of t_i on $\mathbb{Z}^n$ (Proposition A.1.5).

2. For every different combination of $x_i \in \{0,1\}, y_j \in \{0,1\}$, create a new transition from

$$[(t_u, t_v, t_w); (\pm_1^1, \dots, \pm_n^1)(\pm_1^2, \dots, \pm_n^2)(\pm_1^3, \dots, \pm_n^3)]$$

to a (possibly new) state uniquely labelled

$$[\delta_1, \dots, \delta_n; b_2]$$

marking the transition

$$((x_1, \dots, x_n)(y_1, \dots, y_n)(z_1, \dots, z_n)).$$

The b_2 in the name of the new state(s) indicates that this is the binary digit of the c_i that should be taken into account on exiting the state, and the δ_q represent the value carried on each of the n calculations.

We need to determine the value of the z_p and the δ_q.

With $1 \leq p \leq n$,

$$\bar{z_p} = (-1)^{\psi_p^3}[(a_{p1}^v(-1)^{\psi_1^1}x_1 + (-1)^{c_1^\pm}b_1^1) +$$

$$\ldots + (a_{pj}^v(-1)^{\psi_j^1}x_j + (-1)^{c_j^\pm}b_1^j) +$$

$$\ldots + (a_{pn}^v(-1)^{\psi_n^1}x_n + (-1)^{c_n^\pm}b_1^n) + (-1)^{\psi_p^2}y_p].$$

This isn't as complicated as it looks: it involves tallying up the first binary digit from each relevant party, taking into account signs etc. Recall that the ψ^1, ψ^2, ψ^3 represent the signs of the x, y and z respectively, the a^v represent the action of t_v and the b represent any extra added on from the product of t_u and t_v.

Then,

$$\begin{aligned} z_p &= \begin{cases} 0 & \text{if } \bar{z_p} = 2k, \ k \in \mathbb{Z} \\ 1 & \text{if } \bar{z_p} = 2k+1, \ k \in \mathbb{Z} \end{cases} \\ \delta_q &= ||\lfloor \frac{\bar{z_p}}{2} \rfloor||. \end{aligned}$$

3. Now we need to repeat for b_2.

   For every different combination of $x_i \in \{0,1\}, y_j \in \{0,1\}$, create a new transition from every

   $$[\delta_1, \ldots, \delta_n; b_2]$$

   to a (possibly new) state uniquely labelled

   $$[\delta_1', \ldots, \delta_n'; b_3]$$

marking the transition

$$((x_1, \ldots, x_n)(y_1, \ldots, y_n)(z_1, \ldots, z_n)).$$

We again need to determine the value of the z_p and the δ'_q.

With $1 \leq p \leq n$, let

$$\bar{z_p} = (-1)^{\psi_p^3}[(a_{p1}^v(-1)^{\psi_1^1}x_1 + (-1)^{c_1^{\pm}}b_2^1)+$$

$$\ldots + (a_{pj}^v(-1)^{\psi_j^1}x_j + (-1)^{c_j^{\pm}}b_2^j)+$$

$$\ldots + (a_{pn}^v(-1)^{\psi_n^1}x_n + (-1)^{c_n^{\pm}}b_2^n) + (-1)^{\psi_p^2}y_p + \delta_p].$$

This is the same as before, but with a possible carry added.

Then,

$$\begin{aligned} z_p &= \begin{cases} 0 & \text{if } \bar{z_p} = 2k, \ k \in \mathbb{Z} \\ 1 & \text{if } \bar{z_p} = 2k+1, \ k \in \mathbb{Z} \end{cases} \\ \delta'_p &= ||\lfloor \frac{\bar{z_p}}{2} \rfloor||. \end{aligned}$$

4. Now we need to repeat for every $b_k, k < m$.

   For every different combination of $x_i \in \{0, 1\}, y_j \in \{0, 1\}$, create a new transition from every

   $$[\delta_1, \ldots, \delta_n; b_k]$$

   to a new state uniquely labelled

   $$[\delta'_1, \ldots, \delta'_n; b_{k+1}]$$

marking the transition

$$((x_1, \ldots, x_n)(y_1, \ldots, y_n)(z_1, \ldots, z_n)).$$

We need to determine the value of the z_p and the δ'_q.

With $1 \leq p \leq n$, let

$$\bar{z}_p = (-1)^{\psi_p^3}[(a_{p1}^v(-1)^{\psi_1^1}x_1 + (-1)^{c_1^{\pm}}b_k^1)+$$

$$\ldots + (a_{pj}^v(-1)^{\psi_j^1}x_j + (-1)^{c_j^{\pm}}b_k^j)+$$

$$\ldots + (a_{pn}^v(-1)^{\psi_n^1}x_n + (-1)^{c_n^{\pm}}b_k^n) + (-1)^{\psi_p^2}y_p + \delta_p].$$

Then,

$$\begin{aligned} z_p &= \begin{cases} 0 & \text{if } \bar{z}_p = 2k,\ k \in \mathbb{Z} \\ 1 & \text{if } \bar{z}_p = 2k+1,\ k \in \mathbb{Z} \end{cases} \\ \delta'_p &= ||\lfloor \frac{\bar{z}_p}{2} \rfloor||. \end{aligned}$$

5. We now have an automaton dangling on the b_m state; we need to make the changeover to an automaton purely based on carrying, taking account of the last digit of the c_i. So:

   For every different combination of $x_i \in \{0,1\}, y_j \in \{0,1\}$, create a new transition from every

$$[\delta_1, \ldots, \delta_n; b_m]$$

   to a (possibly new) state uniquely labelled

$$[\delta'_1, \ldots, \delta'_n]$$

marking the transition

$$((x_1, \ldots, x_n)(y_1, \ldots, y_n)(z_1, \ldots, z_n)).$$

We need to determine the value of the z_p and the δ'_q.

With $1 \leq p \leq n$, let

$$\bar{z_p} = (-1)^{\psi_p^3}[(a_{p1}^v(-1)^{\psi_1^1}x_1 + (-1)^{c_1^\pm}b_m^1)+$$

$$\ldots + (a_{pj}^v(-1)^{\psi_j^1}x_j + (-1)^{c_j^\pm}b_m^j)+$$

$$\ldots + (a_{pn}^v(-1)^{\psi_n^1}x_n + (-1)^{c_n^\pm}b_m^n) + (-1)^{\psi_p^2}y_p + \delta_p].$$

Then,

$$\begin{aligned} z_p &= \begin{cases} 0 & \text{if } \bar{z_p} = 2k, \; k \in \mathbb{Z} \\ 1 & \text{if } \bar{z_p} = 2k+1, \; k \in \mathbb{Z} \end{cases} \\ \delta'_p &= |\lfloor \frac{\bar{z_p}}{2} \rfloor|. \end{aligned}$$

6. Now follow this subroutine:

   (a) For every different combination of $x_i \in \{0, 1\}, y_j \in \{0, 1\}$, create a new transition from some

   $$[\delta_1, \ldots, \delta_n]$$

   to a (possibly new) state uniquely labelled

   $$[\delta'_1, \ldots, \delta'_n]$$

marking the transition

$$((x_1,\ldots,x_n)(y_1,\ldots,y_n)(z_1,\ldots,z_n)).$$

We need to determine the value of the z_p and the δ'_q.

With $1 \leq p \leq n$, let

$$\bar{z}_p = (-1)^{\psi_p^3}[a^v_{p1}(-1)^{\psi_1^1}x_1+$$

$$\ldots + a^v_{pj}(-1)^{\psi_j^1}x_j+$$

$$\ldots + a^v_{pn}(-1)^{\psi_n^1}x_n + (-1)^{\psi_p^2}y_p + \delta_p].$$

This is the same as before, but without any extra added.

Then,

$$\begin{aligned} z_p &= \begin{cases} 0 & \text{if } \bar{z}_p = 2k,\ k \in \mathbb{Z} \\ 1 & \text{if } \bar{z}_p = 2k+1,\ k \in \mathbb{Z} \end{cases} \\ \delta'_p &= ||\lfloor \frac{\bar{z}_p}{2} \rfloor||. \end{aligned}$$

(b) Repeat for each $[\delta_1,\ldots,\delta_n]$.

7. Finally, make state $[0,\ldots,0]$ a final state. Any calculation leaving nothing carried must be correct.

As the matrix action of the coset representatives is fixed, the actual calculations are just large binary additions. By Theorem A.1.3, the number carried on each calculation is bounded, and so the number of states in this automaton is finite. $\square$

Remark A.2.2. Allowing any combination of signs seems like it may lead to problems - clearly $((+),(+),(-))$ is not allowed when constructing the automaton for $\mathbb{Z}$. However, this is implicitly accounted for - the only calculation which could possibly end up carrying nothing would be the addition of two 0's. As such, down the $((+),(+),(-))$ path will only lead to a final state if the calculation is merely addition of 0's. This is allowed by the representation.

Corollary A.2.3. *All finitely generated virtually abelian groups have an automatic presentation.*

Proof. Let G be a finitely generated virtually abelian group. As $\mathbb{Z}^n \lhd G$, for which see Remark 3.2.5, the result follows directly. $\square$

Bibliography

[1] H. Ayik and N. Ruškuc. Generators and relations of Rees matrix semigroups. *Proc. Edinburgh Math. Soc.*, 42:481–495, 1999.

[2] K. Barthelmann. When can an equational simple graph be generated by hyperedge replacement? In *Proc. 23rd MFCS '98*, volume 1450 of *Lecture Notes in Comp. Sci.*, pages 543–552. Springer-Verlag, 1998.

[3] W. Baur, G. Cherlin, and A. Macintyre. Totally categorical groups and rings. *J. Algebra*, 57:407–440, 1979.

[4] J. Berstel. *Transductions and Context-Free Languages.* Teubner, Stuttgart, 1979.

[5] A. Blumensath. *Automatic Structures.* Diploma thesis, RWTH Aachen, 1999.

[6] A. Blumensath. Prefix-recognizable graphs and monadic second order logic. Technical Report AIB-06-2001, RWTH Aachen, 2001.

[7] A. Blumensath and E. Grädel. Finite presentations of infinite structures: Automata and interpretations. *Theory of Computing Systems*, 37(6):641–674, 2004.

[8] J. R. Buchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik Grundlagen Math.*, 6:66–92, 1960.

[9] A. J. Cain. *Presentations for Subsemigroups of Groups.* PhD thesis, University of St. Andrews, 2005.

[10] H. Calbrix. La théorie monadique du second ordre du monoïde inversif libre est indécidable. *Bull. Belg. Math. Soc.*, 4:53–65, 1997.

[11] C. M. Campbell, E. F. Robertson, N. Ruškuc, and R. M.Thomas. Automatic completely-simple semigroups. *Acta Math. Hungar.*, 95:201–215, 2002.

[12] C. M. Campbell, E. F. Robertson, N. Ruškuc, and R. M. Thomas. Automatic semigroups. *Theor. Comput. Sci.*, 250:365–391, 2001.

[13] L. Carroll. *Alice's Adventures in Wonderland.* Penguin, 1994.

[14] D. Caucal. On infinite transition graphs having a decidable monadic second-order theory. *Theor. Comput. Sci.*, 290(1):79–115, 2003.

[15] A. H. Clifford and G. B. Preston. *Algebraic Theory of Semigroups*, volume I. Amer. Math. Soc., 1961.

[16] A. H. Clifford and G. B. Preston. *Algebraic Theory of Semigroups*, volume II. Amer. Math. Soc., 1967.

[17] Y. D. Cornulier, L. Guyot, and W. Pitsch. On the isolated points in the space of groups. *J. Algebra*, to appear.

[18] T. Deis, J. Meakin, and G. Sénizergues. Equations in free inverse monoids. preprint.

[19] C. Delhommé. Non-automaticity of ω^ω. preprint.

[20] C. Delhommé, V. Goranko, and T. Knapik. Automatic linear orderings. preprint, 2003.

[21] C. Delhommé, T. Knapik, and D. G. Thomas. Using transitive-closure logic for deciding linear properties of monoids. In *Proceedings of Mathematical Foundations of Computer Science*, volume 2747 of *Lecture Notes in Comp. Sci.*, pages 378–387, 2003.

[22] L. Descalço and N. Ruškuc. On automatic rees matrix semigroups. *Comm. Algebra*, 30:1207–1226, 2002.

[23] L. Descalço and N. Ruškuc. Subsemigroups of the bicyclic monoid. *Internat. J. Algebra Comput.*, 15:37–57, 2005.

[24] P. Dubreil. Sur le problèmes d'immersion et la théorie des modules. *Comptes Rendus Mathématique, Académie des Sciences, Paris*, 216:625–627, 1943.

[25] H.-D. Ebbinghaus and J. Flum. *Finite Model Theory.* Springer-Verlag, 1995.

[26] S. Eilenberg, C. C. Elgot, and J. C. Sheperdson. Sets recognized by n-tape automata. *Journal of Algebra*, 13(4), 1969.

[27] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston. *Word Processing in Groups.* Jones and Bartlett, 1992.

[28] Y. L. Eršov. Elementary group theories. *Soviet Math. Doklady*, 13:528–532, 1972.

[29] E. Fohry and D. Kuske. On graph products of automatic and biautomatic monoids. *Semigroup Forum*, 72:337–352, 2006.

[30] R. H. Gilman and A. J. Duncan. Word hyperbolic semigroups. *Math. Proc. Camb. Phil. Soc.*, 136(3):513–524, 2004.

[31] G. M. S. Gomes. A characterization of the group congruences on a semigroup. *Semigroup Forum*, 46:48–53, 1993.

[32] R. Grigorchuk. On growth in group theory. In *Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto 1990)*, pages 325–338. Math. Soc. Japan, 1991.

[33] R. I. Grigorchuk. Cancellative semigroups of power growth. *Math. Notes*, 43:175–183, 1988.

[34] M. Gromov. Groups of polynomial growth and expanding maps. *Publ. Math. d'IHES*, 53:53–78, 1981.

[35] T. Herbst. On a subclass of context-free groups. *RAIRO Inform. Théor. Appl.*, 25:255–272, 1991.

[36] W. Hodges. *Model Theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1993.

[37] B. Hodgson. *Théories décidables par automate fini.* PhD thesis, University of Montréal, 1976.

[38] B. Hodgson. Decidabilite par automate fini. *Ann. Sci. Math.*, 7:39–57, 1983.

[39] M. Hoffmann and R. M. Thomas. Automaticity and commutative semigroups. *Glasgow Math. J.*, 44:167–176, 2002.

[40] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages and Computation.* Addison-Wesley, 1979.

[41] J. M. Howie. *Fundamentals of Semigroup Theory*, volume 12 of *LMS Monographs New Series*. Oxford University Press, 1995.

[42] B. Khoussainov and A. Nerode. Automatic presentations of structures. In D. Leivant, editor, *Logic and Computational Complexity*, volume 960 of *Lecture Notes in Comp. Sci.*, pages 367–392. Springer-Verlag, 1995.

[43] B. Khoussainov, A. Nies, S. Rubin, and F. Stephan. Automatic structures: richness and limitations. In *Proceedings of the 19th IEEE Symposium on Logic in Computer Science*, pages 110–119. IEEE Computer Society, 2004.

[44] B. Khoussainov and S. Rubin. Graphs with automatic presentations over a unary alphabet. *Journal of Automata, Languages and Combinatorics*, 6(4), 2001.

[45] B. Khoussainov and S. Rubin. Some thoughts on automatic structures. *Journal of Automata, Languages and Combinatorics*, 8(2):287–301, 2003.

[46] B. Khoussainov, S. Rubin, and F. Stephan. On automatic partial orders. In *Proceedings of the 18th IEEE Symposium on Logic in Computer Science*, pages 168–177. IEEE Computer Society, 2003.

[47] B. Khoussainov, S. Rubin, and F. Stephan. Definability and regularity in automatic presentations of subsystems of arithmetic. In V. Diekert and M. Habib, editors, *21st Annual Symposium on Theoretical Aspects of Computer Science*, volume 2996 of *Lecture Notes in Comp. Sci.*, pages 440–451. Springer-Verlag, 2004.

[48] D. Kuske and M. Lohrey. First-order and counting theories of ω-automatic structures. In *Proceedings of FoSSaCS*, volume 3921 of *Lecture Notes in Comp. Sci.*, pages 322–336. Springer, 2006.

[49] M. V. Lawson. *Inverse Semigroups: the Theory of Partial Symmetries.* World Scientific, 1998.

[50] M. Leucker. Prefix-recognizable graphs and monadic logic. In E. Grädel, W. Thomas, and T. Wilke, editors, *Automata, Logics, and Infinite Games*, volume 2500 of *Lecture Notes in Comp. Sci.*, pages 263–283. Springer-Verlag, 2002.

[51] S. Li, D. Wang, and Y. Zhang. Semidirect products and wreath products of strongly π-inverse monoids. *Georgian Math. J.*, 3(3):293–300, 1996.

[52] M. Lohrey and N. Ondrusch. Inverse monoids: decidability and complexity of algebraic questions. Technical Report 2005/2, Universität Stuttgart, 2005.

[53] M. Lohrey and G. Sénizergues. When is a graph product of groups virtually-free? *International Journal of Algebra and Computation*, 2005.

[54] A. Mal'cev. A correspondence between rings and groups. In B. F. W. III, editor, *The Metamathematics of Algebraic Systems. Collected papers: 1936–1967*, volume 66 of *Studies in Logic and the Foundations of Mathematics*, chapter 15. North-Holland, 1971.

[55] A. I. Malcev. On the immersion of an algebraic ring into a field. *Math. Ann.*, 113:686–691, 1937.

[56] J. Meier. When is the graph product of hyperbolic groups hyperbolic? *Geometriae Dedicata*, 61:29–41, 1996.

[57] A. V. Meleshkin. Regular semigroups of polynomial growth (Russian). *Math. Zametki*, 47(2):58–64, 1990. English translation *Math. Notes* 47 (1990), 152-158.

[58] C. F. Miller III. Decision problems for groups - survey and reflections. In G. Baumslag and C. F. Miller III, editors, *Algorithms and Classification in Combinatorial Group Theory*, volume 23 of *MSRI Publications*, pages 1–59. Springer-Verlag, 1992.

[59] B. H. Neumann and T. Taylor. Subsemigroups of nilpotent groups. *Proceedings of the Royal Society. Series A*, 274:1–4, 1963.

[60] G. A. Noskov. The elementary theory of a finitely generated almost solvable group (Russian). *Izv. Akad. Nauk SSSR Ser. Mat.*, 47:498–517, 1983. English translation *Math. USSR Izv.* **22** (1984), 465–482.

[61] G. P. Oliver and R. M. Thomas. Automatic presentations for finitely generated groups. In V. Diekert and B. Durand, editors, *22^{nd} Annual Symposium on Theoretical Aspects of Computer Science (STACS'05), Stuttgart, Germany*, number 3404 in Lecture Notes in Comp. Sci., pages 693–704, 2005.

[62] L. Pelecq. *Isomorphismes et Automorphismes des graphes context-free, équationnels et automatiques.* PhD thesis, Bordeaux 1 university, 1997.

[63] D. J. S. Robinson. *A Course in the Theory of Groups.* Graduate Texts in Mathematics. Springer-Verlag, 2 edition, 1995.

[64] H. Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967.

[65] N. S. Romanovskiĭ. On the elementary theory of an almost polycyclic group (Russian). *Math. Sb.*, 111:135–143, 1980. English translation *Math. USSR Sb.* **39** (1981).

[66] J. J. Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, fourth edition, 1995.

[67] S. Rubin. Finite automata and well ordered sets. *New Zealand Journal of Computing*, 7(2), 1999.

[68] S. Rubin. *Automatic Structures*. PhD thesis, Auckland University, 2005.

[69] G. Sénizergues. Definability in weak monadic second-order logic of some infinite graphs. In *Dagstuhl Seminar on Automata Theory: Infinite Computations*, volume 28, page 16, 1992.

[70] M. A. Taitslin. Algorithmic problem for commutative semigroups. *Sov. Math. Dokl.*, 9(1):201–204, 1968.

[71] A. Tarski, A. Mostowski, and R. M. Robinson. *Undecidable Theories*. North-Holland, Amsterdam, 1953.

[72] Y. M. Vazhenin. Semigroups with one defining relation whose elementary theories are solvable (Russian). *Sibirsk. Mat. Zh.*, 24(1):40–49, 1983. English translation *Siberian Math. J.* 24 (1983) 1, 33-41.

Index