TOPICS IN COMBINATORIAL SEMIGROUP THEORY

Victor Maltcev

A Thesis Submitted for the Degree of PhD
at the
University of St. Andrews

2012

Topics in Combinatorial Semigroup Theory

Victor Maltcev
Ph.D. Thesis

February 13, 2012

Declarations

I, Victor Maltcev, hereby certify that this thesis, which is approximately 37,000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

I was admitted as a research student and as a candidate for the degree of Doctor of Philosophy in September 2006; the higher study for which this is a record was carried out in the University of St Andrews between 2006 and 2011.

Date: Signature of candidate:

We hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Date: Signature of supervisor:

Name: Prof Nik Ruškuc

Date: Signature of supervisor:

Name: Dr James D. Mitchell

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand that the title and the abstract will be published, and that a copy of the work may be made and supplied to any

bona fide library or research worker, that our thesis will be electronically accessible for personal or research use unless exempt by award of an embargo as requested below, and that the library has the right to migrate our thesis into new electronic forms as required to ensure continued access to the thesis. We have obtained any third-party copyright permissions that may be required in order to allow such access and migration, or have requested the appropriate embargo below.

The following is an agreed request by candidate and supervisors regarding the electronic publication of this thesis:

Access to printed copy and electronic publication of thesis through the University of St Andrews.

Date: Signature of candidate:

Date: Signature of supervisor:

Name: Prof Nik Ruškuc

Date: Signature of supervisor:

Name: Dr James D. Mitchell

Abstract

In this thesis we discuss various topics from Combinatorial Semigroup Theory: automaton semigroups; finiteness conditions and their preservation under certain semigroup theoretic notions of index; Markov semigroups; word-hyperbolic semigroups; decision problems for finitely presented and one-relator monoids.

First, in order to show that general ideas from Combinatorial Semigroup Theory can apply to uncountable semigroups, at the beginning of the thesis we discuss semigroups with Bergman's property.

We prove that an automaton semigroup generated by a Cayley machine of a finite semigroup S is itself finite if and only if S is aperiodic, which yields a new characterisation of finite aperiodic monoids. Using this, we derive some further results about Cayley automaton semigroups.

We investigate how various semigroup finiteness conditions, linked to the notion of ideal, are preserved under finite Rees and Green indices. We obtain a surprising result that $\mathcal{J} = \mathcal{D}$ is preserved by supersemigroups of finite Green index, but it is not preserved by subsemigroups of finite Rees index even in the finitely generated case. We also consider the question of preservation of hopficity for finite Rees index. We prove that in general hopficity is preserved neither by finite Rees index subsemigroups, nor by finite Rees index extensions. However, under finite generation assumption, hopficity is preserved by finite Rees index extensions. Still, there is an example of a finitely generated hopfian semigroup with a non-hopfian subsemigroup of finite Rees index.

We prove also that monoids presented by confluent context-free monadic rewriting systems are word-hyperbolic, and provide an example of such a monoid, which does not admit a word-hyperbolic structure with uniqueness. This answers in the negative a question of Duncan & Gilman.

We initiate in this thesis a study of Markov semigroups. We investigate how the property of being Markov is preserved under finite Rees and Green indices.

For various semigroup properties P we examine whether P, $\neg P$ are

Markov properties, and whether P is decidable for finitely presented and one-relator monoids.

Contents

Acknowledgements

This thesis would be impossible from the very beginning to the end without the guidance and constant support by my supervisors Dr Alan Cain (unofficial), Dr James Mitchell and Prof Nik Ruškuc. Even in the darkest days of my life they were always willing to help me both mathematically and personally. These people became to me much more than just supervisors. From mathematical perspective, I was always amazed by elegance of Alan's theorems, by James's rule of simplifying the exposition of mathematical results as much as it is possible, and by Nik's clearness of thought when doing Mathematics.

A month-and-a-half of pleasant mathematical discussions were spent with Dr Vesna Kilibarda. This lead not only to obtaining mathematical results – we became good friends.

From time to time during my studies I would go to Dr Robert Gray's office and ask him questions about semigroups, and he always put aside his current work and discussed the questions with me.

I would like also to thank Dr Ganna Kudryavtseva with whom I was in touch via e-mails during all the time of the studies and our extensive discussions always lead to interesting questions and sometimes even results.

There are also some people with whom I did not collaborate on Mathematics, about whom I would like to say some warm words. It was a good friendly environment in the office with my office-mate Dr Andreas Distler. Zen-like absurd by Dr Yann Peresse at 'Friday biscuits' was very funny and witty. Runs with Dr Aidan Naughton taught me that it is possible to run long and fast simultaneously.

My last thank goes specially to Nik who made my studies possible and introduced me to the world of Combinatorial Semigroup Theory – the most important, in my opinion, branch of Semigroup Theory.

Finally, I am indebted to the University of St Andrews for granting me support with the ORS Awards Scheme and the University Maintenance Stipend.

Chapter 1

Introduction

In rough terms, Combinatorial Semigroup Theory studies finitely generated semigroups, and the ways to present all their elements. Basically, this branch of Mathematics appears quite naturally if one asks oneself:

How knowing some abstract semigroup can I convey this semigroup to another person?

Of course, if one thinks, say, about a matrix semigroup, or a semigroup of mappings of a set into itself, then it is possible to give a realisation of that semigroup via matrices or mappings respectively. But what if one does not know for sure if the semigroup can be realised by some 'convenient' means? One of the most natural ways then is to find a generating set for the semigroup, consider the set of all words over this set, and try to explain to another person all instances when one word is equal to another. If one succeeds in this, then the other person can reconstruct the semigroup uniquely. This idea leads to the notion of the *semigroup presentation* – central in Combinatorial Semigroup Theory, which we are now to define.

1.1 Presentations

Let A be some alphabet. Denote by A^+ and A^* the free semigroup and the free monoid over A. By a *presentation* we simply mean a pair $\langle A : R\rangle$, where $R \subseteq A^* \times A^*$ is a set of *relations*.

Definition 1.1.1. Let A be a set and $R \subseteq A^+ \times A^+$. We say that a semigroup S is given by the presentation $\mathrm{Sg}\langle A : R\rangle$, if S is isomorphic to A^+/ρ, where ρ is the minimal congruence on A^+ containing R. (One defines the monoid presentation $\mathrm{Mon}\langle A : R\rangle$ analogously.)

There is an easy way to understand when two words u and v from A^+ are equal in $S = \mathrm{Sg}\langle A : R\rangle$: $u =_S v$ if and only if there exists a chain

$u = x_0 \sim x_1 \sim \cdots \sim x_p = v$, where $p \geq 0$, $x_i \in A^+$, and $x \sim y$ for $x, y \in A^+$ by definition means that x and y allow decompositions (as words) $x = s\alpha t$ and $y = s\beta t$ such that either $(\alpha, \beta) \in R$ or $(\beta, \alpha) \in R$. The proof of this can be found in any standard text, we provide here the reference [51].

Hence, basically Definition 1.1.1 means that the relations R which hold in S are the building blocks for *all* the possible relations which hold in S.

So, in principle it is possible that one having a semigroup, can convey to another person the semigroup by means of a presentation. But how can that other person work with the received presentation? One of the efficient methods to do so is to look at the presentation as at the correspondent *rewriting system*.

1.2 Rewriting Systems

A *(string) rewriting system* is simply a pair (A, R), where A is an alphabet and $R \subseteq A^* \times A^*$. Each pair $(l, r) \in R$ is called a *rewriting rule*. Then the reduction $\to_R$ is defined as follows: $u \to_R v$ if $u = xly$ and $v = xry$ for some $x, y \in A^*$ and $(l, r) \in R$; and $\to_R^*$ denotes the reflexive transitive closure of $\to_R$. A word $w \in A^*$ is called *reducible* with respect to R if it contains a subword l for some $(l, r) \in R$; otherwise w is called *irreducible*.

The rewriting system (A, R) is *noetherian*, or *terminating*, if there is no infinite chain $w_1 \to_R w_2 \to_R w_3 \to_R \cdots$. (A, R) is *confluent* if whenever $w \to_R^* u$ and $w \to_R^* v$, there exists w' such that $u \to_R^* w'$ and $v \to_R^* w'$. Confluent noetherian systems are called *complete*.

The importance of complete rewriting systems (A, R) is in the fact that the irreducibles of this system form the set of *normal forms* for the monoid $\mathrm{Mon}\langle A : R\rangle$. It is quite obvious to see that every finitely generated monoid admits a complete rewriting system. Indeed, one just needs to fix an order on the generators and then rewrite every word w to the minimum word u in the correspondent shortlex order with $w = u$ in the semigroup. Of course, one normally gets an infinite rewriting system in this way, and such systems would be of low practical use.

Also, having a rewriting system defining the monoid, there is a completion procedure of the system – the so-called *Knuth-Bendix procedure*. This procedure will not always terminate, i.e. it is possible that using this procedure, starting on a finite rewriting system, we will not be able to find a finite complete rewriting system. Nonetheless, using the mere principle of the completion procedure, sometimes it is possible to find infinite though convenient rewriting systems for the monoids under consideration. All this makes rewriting systems a powerful tool to study finitely

generated monoids. Since later in the text we will heavily use the machinery of rewriting systems, we give some more definitions we will use throughout: The rewriting system (A, R) is

1. *length-reducing* if $|r| < |l|$ for all $(l, r) \in R$;
2. *special* if $r = 1$ – the emptyword for all $(l, r) \in R$;
3. *monadic* if $r \in A \cup \{1\}$ for all $(l, r) \in R$.

A good reference to read about rewriting systems is [9].

1.3 Rees and Green Indices

Some of the first results in Combinatorial *Group* Theory are the so-called Reidemeister–Schreier-type results. They deal with *(group) finiteness conditions* – the properties of groups which hold for all finite groups. These results are concerned with the following question: is a finiteness condition P preserved by finite index subgroups and finite index extensions? In particular, from the results of Reidemeister and Schreier (see [52]) it follows that finite generation, finite presentability and solubility of the word problem are preserved both by finite index subgroups and supergroups.

Another strand of results in Combinatorial Group Theory related to the notion of index are various theorems, which in effect give us certain characterisations when a finitely generated group has a certain nice property, i.e. of the following type: 'A group has property P if and only if it has a subgroup of finite index with property Q'. The examples of such statements are the celebrated Gromov's Growth Theorem and Muller–Schupp Theorem (we choose these as examples since the properties P from them are closely related to the topics we will discuss in the thesis).

The first theorem refers to the notion of the (word) growth. Let A be a finite generating set for a group G. Let a_n be the number of elements in $A \cup \cdots \cup A^n$. Then a_n is an increasing sequence. It is quite easy to see that the growth rate of this sequence does not change when one changes A to another finite generating set for G, and this is what is known as the *(word) growth rate* of G. It had been known for a while that every nilpotent finitely generated group has polynomial growth, until Gromov proved a remarkable theorem stating that actually polynomial growth implies virtual nilpotency:

Theorem 1.3.1 (Gromov, [36]). *A finitely generated group has polynomial growth if and only if it has a nilpotent subgroup of finite index.*

Another remarkable theorem, involving quite a lot of various branches of Mathematics, which also gives us a characterisation of a nice property for finitely generated groups, is the following:

Theorem 1.3.2 (Muller & Schupp, [66]). *A finitely generated group has context-free word problem if and only if it has a free subgroup of finite index.*

In order to prove analogous results in Combinatorial Semigroup Theory, one naturally asks what could be a suitable notion of index for semigroups? Depending on the problem we have in mind to solve, there appeared several notions of index for semigroups. For instance, Grigorchuk [34] invented a certain notion of index to prove an analog of Gromov's Growth Theorem for cancellative semigroups, but the analog of Reidemeister–Schreier Theorem is no longer true for this index. Or, say, there exists a notion of the so-called syntactic index introduced by Ruškuc and Thomas [76], which applied to groups becomes the 'normal' group index, but which fails to provide Reidemeister–Schreier-type results for general semigroups.

In this thesis we will concentrate on two successful definitions of index for semigroups which enable us to prove Reidemeister–Schreier-type results. The first one is very easy to define:

Definition 1.3.3. Let T be a subsemigroup of a semigroup S. The *Rees index* of T in S is $|S \setminus T| + 1$.

The first mention of Rees index in the literature is due to Jura [47]. Even though admitting a subsemigroup of finite Rees index is a fairly restrictive property, it has provided a fertile ground for research, and has thrown up a few surprises. In [75] it is proved that the main combinatorial finiteness conditions, such as finite generation, presentability, and solvability of the word problem, are all preserved both under finite Rees subsemigroups and extensions. The proof for finite presentability is surprisingly complicated, and to date no fundamentally simpler proof has been found. The related question of the existence of finite complete rewriting system has been settled only very recently, see [84]. Some related cohomological finiteness conditions are considered in [57] and [83], residual finiteness is treated in [76]. Some surprising behaviour in relation to the ideal structure we will encounter in Chapter 4.

Notwithstanding all the mentioned results about finite Rees index, and that it does appear very often in Semigroup Theory, Rees index still does not generalise the group index. To cure this situation, Gray and Ruškuc propose in [33] the so-called *Green index*. To define it, we need to explain what the *Green relations* are – a fundamental notion in Semigroup Theory.

Definition 1.3.4. Let S be a semigroup. Let 1 be a newly adjoined element to S which represents the identity and makes the set $S^1 = S \cup \{1\}$ become the monoid in which the multiplication extends that in S. The *Green relations* $\mathcal{R}, \mathcal{L}$ and $\mathcal{J}$ in S are binary relations on S defined as follows: for $a, b \in S$

$$\begin{aligned} a\mathcal{R}b &\iff aS^1 = bS^1 \\ a\mathcal{L}b &\iff S^1a = S^1b \\ a\mathcal{J}b &\iff S^1aS^1 = S^1bS^1. \end{aligned}$$

Define also $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$ and $\mathcal{D} = \mathcal{R} \circ \mathcal{L}$.

One can show that all the five defined relations are indeed equivalence relations, that $\mathcal{D} = \mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$, and $\mathcal{D} \subseteq \mathcal{J}$ see [45]. The $\mathcal{R}$-class containing $a \in S$ will be denoted by R_a. Similarly, one defines L_a, H_a, D_a and J_a.

The importance of Green relations in Semigroup Theory is in the fact that in some sense they endow the semigroup with a coordinate system: one can decompose the semigroup into $\mathcal{D}$-classes and in each $\mathcal{D}$-class work according to the arguably the most fundamental statement in Semigroup Theory:

Theorem 1.3.5 (Green's Lemma, [45])**.** *Let S be a semigroup and $a, b \in S$.*

1. *If $a\mathcal{R}b$ and $s, s' \in S^1$ are such that $as = b$ and $bs' = a$, then the mappings*

$$\rho_s : x \mapsto xs \quad \textit{and} \quad \rho_{s'} : x \mapsto xs'$$

   are mutually inverse bijections from L_a onto L_b and vice versa. Moreover, for any $x \in L_a$ one has $x\mathcal{R}x\rho_s$, i.e. ρ_s moves an element $x \in L_a$ within the $\mathcal{R}$-class containing x.

2. *If $a\mathcal{L}b$ and $s, s' \in S^1$ are such that $sa = b$ and $s'b = a$, then the mappings*

$$\lambda_s : x \mapsto sx \quad \textit{and} \quad \lambda_{s'} : x \mapsto s'x$$

   are mutually inverse bijections from R_a onto R_b and vice versa. Moreover, for any $x \in R_a$ one has $x\mathcal{L}x\lambda_s$, i.e. λ_s moves an element $x \in R_a$ within the $\mathcal{L}$-class containing x.

We are now ready to define Green index. For this we require the following:

Definition 1.3.6. Let T be a subsemigroup of a semigroup S. For $u, v \in S$ define:

$$\begin{aligned} u\mathcal{R}^T v &\iff uT^1 = vT^1 \\ u\mathcal{L}^T v &\iff T^1 u = T^1 v, \end{aligned}$$

and $\mathcal{H}^T = \mathcal{R}^T \cap \mathcal{L}^T$.

This definition was introduced by Wallace [82]. Gray and Ruškuc prove in [33] that each of $\mathcal{R}^T$, $\mathcal{L}^T$ and $\mathcal{H}^T$ is an equivalence relation on S; and call their equivalence classes by the (T-)*relative* $\mathcal{R}$-, $\mathcal{L}$-, and $\mathcal{H}$-classes, respectively. Furthermore, they prove that these relations respect T, in the sense that each $\mathcal{R}^T$-, $\mathcal{L}^T$-, and $\mathcal{H}^T$-class lies either wholly in T or wholly in $S \setminus T$. This prompted Gray and Ruškuc to make the following definition:

Definition 1.3.7. Let T be a subsemigroup in a semigroup S. The *Green index* of T in S is $|(S \setminus T)/\mathcal{H}^T| + 1$.

The authors of [33] also show that relative Green relations behave similarly to the Green relations:

Proposition 1.3.8 ([33, Proposition 4])**.** *Let T be a subsemigroup in a semigroup S.*

1. *The relation $\mathcal{R}^T$ is a left congruence on S, and $\mathcal{L}^T$ is a right congruence.*

2. *For each relative $\mathcal{H}^T$-class H either $H^2 \cap H = \varnothing$, or $H^2 \cap H = H$ in which case H is a subgroup of S.*

3. *$\mathcal{R}^T$ and $\mathcal{L}^T$ commute, so we may define $\mathcal{D}^T = \mathcal{R}^T \circ \mathcal{L}^T = \mathcal{L}^T \circ \mathcal{R}^T$.*

4. *Let $u, v \in S$ be such that $u\mathcal{R}^T v$, and let $p, q \in T^1$ such that $up = v$ and $vq = v$. Then the mapping ρ_p given by $x \mapsto xp$ is an $\mathcal{R}^T$-class preserving bijection from L_u^T to L_v^T while the mapping ρ_q given by $x \mapsto xq$ is an $\mathcal{R}^T$-class preserving bijection from L_v^T to L_u^T, and is the inverse of the mapping ρ_p.*

But the most important feature of the Green index is that it generalises the group index in the following sense:

Proposition 1.3.9. *A subgroup H of a group G has finite (group) index in G if and only if H has finite Green index in G. (Note, however, that in this situation the group and Green indices of H in G may differ.)*

As one would expect, many finiteness conditions are preserved when passing to subsemigroups or extensions of finite Green index: finite generation, solubility of word problem, being finite. The papers [13] and [33] have largely been devoted to proving results of this type for finiteness conditions shared by groups and semigroups, thus reinforcing the role of Green index as a common generalisation of group and Rees indices.

1.4 Further Notation, Notions and Facts

In this section we collect some further general information we will need later on.

For a semigroup S, a subset $I \subseteq S$ is called a *right ideal* if $IS \subseteq I$. *Left ideals* and *(two-sided) ideals* are defined analogously. In particular, $a\mathcal{R}b$ means exactly that the right ideals generated by a and b coincide: $aS^1 = bS^1$. This enables one to define the order on $\mathcal{R}$-classes of S:

$$R_a \leq R_b \Longleftrightarrow aS^1 \subseteq bS^1.$$

One defines the orders on the sets of all $\mathcal{L}$-classes and $\mathcal{J}$-classes in a similar fashion. A semigroup S is said to have a property $\min_R$ if there are no infinite chains $R_{a_1} > R_{a_2} > R_{a_3} > \cdots$. Obviously, $\min_R$ and similarly defined $\min_L$ and $\min_J$ are finiteness conditions.

Another important notion related to ideals is the notion of *stability*:

Definition 1.4.1. [51, Proposition 3.7] A $\mathcal{J}$-class J of a semigroup S is said to be *right stable* if it satisfies one (and hence all) of the following equivalent conditions:

(i) The set of all $\mathcal{R}$-classes in J has a minimal element.

(ii) There exists $q \in J$ satisfying the following property: $q\mathcal{J}qx$ if and only if $q\mathcal{R}qx$ for all $x \in S$.

(iii) Every $q \in J$ satisfies the property stated in (ii).

(iv) Every $\mathcal{R}$-class in J is minimal in the set of $\mathcal{R}$-classes in J.

We say that the whole semigroup S is *right stable* if every $\mathcal{J}$-class of S is right stable. The notion of left stability is defined dually. A $\mathcal{J}$-class or a semigroup are said to be (*two-sided*) *stable* if they are both left and right stable.

Roughly speaking, this definition means that if in the set of all $\mathcal{R}$-classes, contained within a fixed $\mathcal{J}$-class, there is a minimal element, then every of the considered $\mathcal{R}$-classes is minimal and so all of these $\mathcal{R}$-classes are pairwise incomparable. Thus, a $\mathcal{J}$-class J is right stable if and only if all the $\mathcal{R}$-classes contained in J are pairwise incomparable.

It is clear that stability is a finiteness condition, and that $\min_R$ implies right stability. Also note that stability implies the finiteness condition $\mathcal{J} = \mathcal{D}$, see [51]. A convenient way to realise what is stability in algebraic sense is due to

Lemma 1.4.2 ([51, Proposition 3.10])**.** *Let S be a semigroup. Then S is right stable if and only if $R_a \leq R_{ba}$ implies $R_a = R_{ba}$ for all $a, b \in S$.*

An element a of a semigroup S is said to be *regular* in S if $a \in aSa$. A semigroup is called *regular* if all its elements are regular. An *inverse* semigroup is a regular semigroup in which every two idempotents commute. A useful fact is that if at least one element in a $\mathcal{D}$-class is regular, then *all* the elements from this $\mathcal{D}$-class are regular, see [45].

By a *deterministic automaton* we will mean a 5-tuple $\mathcal{A} = (Q, A, \delta, q_0, F)$, where Q is a finite set of states, A is a finite set of symbols, $F \subseteq Q$ is a set of final states, $q_0 \in Q$ is the initial state, and $\delta : Q \times A \to Q$ is a transition function. Feeding an automaton with a word $w \in A^*$, it enters the state q_0 and reads the first letter of w, say a. Then it moves to the state $\delta(q_0, a)$ and starts reading the word w', where $w = aw'$. The automaton proceeds reading the letters of w, and after $|w|$ steps moves to some state $q \in Q$. We say that $\mathcal{A}$ accepts w if $q \in F$, otherwise we say that $\mathcal{A}$ rejects w. The set of all words accepted by $\mathcal{A}$ is denoted by $L(\mathcal{A})$ and is called the language accepted by $\mathcal{A}$. The languages accepted by automata are called *regular languages* and they can be characterised by Kleene's Theorem as exactly those which admit regular expressions, see [43] for more details. For every regular language it is possible to find the so-called *minimal*, or *trim* automaton which accepts the language. Roughly speaking, such minimal automata do not have surplus states, see [43] for details.

Finally, a *context-free grammar* is quadruple $\Gamma = (N, T, P, S)$ where N is a finite set of non-terminal symbols, T is a finite set of terminal symbols, $S \in N$ is the start symbol, and P is a finite set of productions. We assume that N and T are disjoint. Each production is of the form $A \Rightarrow \alpha$, where $\alpha \in (N \cup T)^*$. As with rewriting systems, for $\alpha, \beta \in (N \cup T)^*$ we write $\alpha \Rightarrow \beta$ if $\alpha = \gamma A \delta$ and $\beta = \gamma \pi \delta$, where $\gamma, \delta, \pi \in (N \cup T)^*$ and $A \Rightarrow \pi$ is a production from P. If β can be reached from α by a finite number of successive applications of $\Rightarrow$, we will write $\alpha \Rightarrow^* \beta$. The language accepted

by Γ is $L(\Gamma) = \{w \in T^* : S \Rightarrow^* w\}$. The languages accepted by context-free grammars are called *context-free languages*. Every regular language is context-free. More information about context-free languages can be found in [43].

To read more about general Semigroup Theory we refer the reader to the standard texts [18, 19, 38, 45]. We also would suggest to read the theses [10] and [74] which have a similar spirit to the current one.

1.5 Structure of the Thesis

We start with Chapter 2 where we show that the typical ideas of Combinatorial Semigroup Theory apply to uncountable semigroups. We discuss there the finiteness condition of the *Bergman's property* and provide various examples of semigroups which have or do not have this property. In the process we invent some machinery, e.g. length functions, and using them prove that certain algebraic versions of cofinality are preserved by finite Rees index subsemigroups and extensions.

Next we move to Chapter 3 where we study the class of automaton semigroups generated by the *Cayley automaton machines*. The latter objects appeared in the 1960s, and we use a relatively modern machinery of *wreath recursions* to yield various characterisation theorems. One of them involves the class of all finite aperiodic semigroups.

In Chapter 4 we investigate the preservation under finite Green and Rees indices of the following finite conditions: stability, $\mathcal{J} = \mathcal{D}$, having finitely many ideals, $\min_R$, $\min_J$, and π-regularity. In particular we obtain a surprising result that $\mathcal{J} = \mathcal{D}$ is preserved by finite Green index extensions, but there is a finitely presented semigroup with $\mathcal{J} = \mathcal{D}$ and with a subsemigroup of Rees index 2 in which $\mathcal{J} = \mathcal{D}$ does not hold any longer.

Chapter 5 deals with hopficity. We prove that hopficity in general is not preserved by finite Rees index subsemigroups and extensions. Then we prove that under the finite generation assumption, hopficity is preserved by finite Rees index extensions, but still we find a finitely generated hopfian semigroup with a non-hopfian subsemigroup of Rees index 2.

In Chapter 6 we prove that monoids presented by confluent context-free monadic rewriting systems are word-hyperbolic. We also show that the monoid $\mathrm{Mon}\langle a, b, c, d : ab^n c^n d = 1 \quad n \geq 1\rangle$ does not admit a word-hyperbolic structure with uniqueness, thus answering a question of Duncan & Gilman of whether every word-hyperbolic monoid admits a word-hyperbolic structure with uniqueness.

In Chapter 7 we study the finiteness condition of *the property of being*

Markov, closely related to the notion of hyperbolicity for groups. We show the interaction of the property of being Markov with various notions of hyperbolicity for semigroups, and investigate how markovicity is preserved under Rees and Green indices.

In the final Chapter 8 for various semigroup properties P we investigate whether P and $\neg P$ are Markov properties, and whether P is decidable for finitely presented and one-relator monoids. All our results are collected in a single table.

We close the thesis with Chapter 9 consisting of the open problems suggested by the research we provide in the text.

Chapter 2

The Bergman Property for Semigroups

In this chapter, we study the Bergman property for semigroups and the associated notions of cofinality and strong cofinality. A large part of the chapter is devoted to determining when the Bergman property, and the values of the cofinality and strong cofinality, can be passed from semigroups to subsemigroups and vice versa.

The results of this chapter were obtained in collaboration with James Mitchell and Nik Ruškuc and appeared in [59].

2.1 Introduction

In this chapter, we will consider the notion of Bergman's property for semigroups. This property has already been studied by several authors for groups, and we begin by discussing Bergman's property and related notions in this context.

Let G be a group. If U is a (group) generating set for G, then

$$G = \bigcup_{i=1}^{\infty} (U \cup U^{-1})^i$$

where $(U \cup U^{-1})^i = \{\, u_1 u_2 \cdots u_i \,:\, u_1, u_2, \ldots, u_i \in U \cup U^{-1} \,\}$. It is not always true that for a group G and a generating set U for G that

$$G = \bigcup_{i=1}^{j} (U \cup U^{-1})^i$$

for some $j \in \mathbb{N}$. For example, the free group $FG(X)$ on any set X does not satisfy this property. A group G is *group Cayley bounded* with respect to a subset U if there exists $n \in \mathbb{N}$ such that $G = V \cup \cdots \cup V^n$ where

$V = U \cup U^{-1}$. In other words, the minimum distance between any two elements in the Cayley graph of G with respect to U is at most n. So, the free group $FG(X)$ is not group Cayley bounded with respect to X but is group Cayley bounded with respect to itself. More surprisingly, there are examples of non-finitely generated groups G that are group Cayley bounded with respect to every generating set. One of the first examples of such a group was provided by Bergman in [8] where it was shown that the symmetric group $\mathrm{Sym}(\Omega)$ is group Cayley bounded with respect to every generating set for all sets Ω. Consequently, a group is said to have the *group Bergman property* if it is Cayley bounded with respect to every generating set. Droste and Göbel [22] give sufficient conditions for a permutation group to have the group Bergman property. Examples of groups satisfying their conditions are: the symmetric groups, and the homeomorphism groups of Cantor's discontinuum $\mathfrak{C}$, the rationals $\mathbb{Q}$, and the irrationals $\mathbb{I}$. Other notable examples of groups satisfying the group Bergman property are: the infinite cartesian power of any finite perfect group, the full groups of measure-preserving and ergodic transformations on the unit interval [23], ω_1-existentially closed groups [20], and the groups of measure-preserving homeomorphisms of the Cantor space or Lipschitz homeomorphisms of the Baire space, and certain closed oligomorphic subgroups of $\mathrm{Sym}(\mathbb{N})$ [48].

A semigroup S is said to be *semigroup Cayley bounded* with respect to a generating set U if $S = U \cup U^2 \cup \cdots \cup U^n$ for some $n \in \mathbb{N}$. We will say that a semigroup S has the *semigroup Bergman property* if it is semigroup Cayley bounded with respect to every generating set.

Note that we must make separate definition of these notions for semigroups because the definition for groups involve inverses. The fact that the definitions of these two properties for semigroups and groups are not the same, accounts for the use of the word 'group' in the definitions above.

After making these definitions it is most natural to ask the following questions. Are there natural examples of semigroups that satisfy the semigroup Bergman property? In particular, do the semigroup theoretic analogues of the symmetric group satisfy the semigroup Bergman property? Groups are natural examples of semigroups, so how does the semigroup Bergman property compare with the group Bergman property? In this chapter we attempt to answer these questions.

If a group satisfies the semigroup Bergman property, then it certainly satisfies the group Bergman property. It is not known if the converse is true or not. However, the majority of the groups that are known to satisfy the group Bergman property, such as those groups mentioned above, also satisfy the semigroup Bergman property; for more details see Corollary

2.2.5.

To answer the first of the questions above, let us introduce the *full transformation semigroup* of all self-maps of a set Ω, denoted by $\mathrm{Self}(\Omega)$. Every semigroup can be embedded into a full transformation semigroup $\mathrm{Self}(\Omega)$ for some set Ω. As such $\mathrm{Self}(\Omega)$ plays an analogous role in semigroup theory as that played by $\mathrm{Sym}(\Omega)$ in group theory. Other counterparts of $\mathrm{Self}(\Omega)$ and $\mathrm{Sym}(\Omega)$ are $\mathrm{SymInv}(\Omega)$, $\mathrm{Part}(\Omega)$, and $\mathrm{Bin}(\Omega)$ the semigroups of all injective partial self-maps (the so-called *symmetric inverse semigroup*), partial self-maps, and binary relations, respectively, on Ω.

Most notable among the semigroups that we will show to satisfy the semigroup Bergman property are: $\mathrm{Self}(\Omega)$, $\mathrm{SymInv}(\Omega)$, $\mathrm{Bin}(\Omega)$, $\mathrm{Part}(\Omega)$, semigroups of continuous functions on the rationals $\mathbb{Q}$, irrationals $\mathbb{I}$, Cantor's discontinuum, and the finitary power semigroup of $\mathrm{SymInv}(\Omega)$ (see Section 2.4). Equally notable for not satisfying the semigroup Bergman property are: the Baer-Levi semigroup on $\mathbb{N}$, the finitary power semigroups of $\mathrm{Self}(\Omega)$, $\mathrm{Bin}(\Omega)$, $\mathrm{Part}(\Omega)$, and the semigroup of bounded self-maps of $\mathbb{Q}$ (see Section 2.5). The techniques used in resolving these specific examples are based on the more general results in Sections 2.2 and 2.3.

2.2 Cofinality and Strong Cofinality

We require the following notions analogous to those with the same names introduced by Macpherson and Neumann [54] and Droste and Göbel [22].

First of all, we will identify any cardinal λ with the least ordinal with cardinality equal to λ. Hence, we may follow the usual convention that λ is the collection of all ordinals less than λ.

A sequence of sets $(U_i)_{i<\lambda}$, for some cardinal λ, such that $U_i \subseteq U_j$ for all $i \leq j < \lambda$ is called a *chain*. Let S be a non-finitely generated semigroup. Then the *cofinality* of S is the least cardinal λ such that there exists a chain of proper subsemigroups $(U_i)_{i<\lambda}$ of S where $S = \bigcup_{i<\lambda} U_i$. We will denote the cofinality of S by $\mathrm{cf}(S)$ and refer to subsemigroups $(U_i)_{i<\mathrm{cf}(S)}$ satisfying the above property as a *cofinal chain* for S. Obviously, the above definition of cofinality cannot be applied to finitely generated semigroups. The *strong cofinality* of S is the least cardinal λ such that there exists a chain of proper subsets $(U_i)_{i<\lambda}$ of S where for all $i < \lambda$ there exists $j < \lambda$ such that $U_iU_i \subseteq U_j$ and $S = \bigcup_{i<\lambda} U_i$. The strong cofinality of S is denoted by $\mathrm{scf}(S)$ and a *strong cofinal chain* is defined analogously to a cofinal chain. It is clear that $\mathrm{scf}(S) \leq \mathrm{cf}(S)$.

The following technical lemma shows that the notions of cofinality and strong cofinality used here, when applied to a group, are equivalent to

those used in [8], [22], and [54]. Lemma 2.2.1 and Corollary 2.2.5 follow by similar arguments as those given on page 435 and in the proofs of Theorems 5 and 6 in [8]. We include the proofs of these results for the sake of completeness.

Lemma 2.2.1. *Let G be a non-finitely generated group. Then*

(i) $\mathrm{cf}(G)$ *is the least cardinal of a cofinal chain of subgroups for G;*

(ii) $\mathrm{scf}(G)$ *is the least cardinal λ of a strong cofinal chain $(U_i)_{i<\lambda}$ for G satisfying $U_i = U_i^{-1}$ for all $i < \lambda$.*

Proof. To prove Part (i), let λ be the least cardinal of a cofinal chain of subgroups for G and let $\kappa = \mathrm{cf}(G)$. By definition, $\mathrm{cf}(G) = \kappa \leq \lambda$. To prove that the converse inequality holds, note that there exists a chain of proper subsemigroups $(V_i)_{i<\kappa}$ of G where $G = \bigcup_{i<\kappa} V_i$. Hence

$$G = G^{-1} = \bigcup_{i<\kappa} V_i^{-1}$$

and so

$$G = G \cap G^{-1} = \bigcup_{i<\kappa} V_i \cap V_i^{-1}.$$

Although there may be $i < \kappa$ such that $V_i \cap V_i^{-1} = \emptyset$, after some point all the terms in $(V_i \cap V_i^{-1})_{i<\kappa}$ are nonempty. Thus we may assume without loss of generality that all the terms in $(V_i \cap V_i^{-1})_{i<\kappa}$ are nonempty. Hence $(V_i \cap V_i^{-1})_{i<\kappa}$ is a chain of proper subgroups of G and the proof is complete.

The proof of part (ii) is analogous and omitted. □

The following proposition relates cofinality, strong cofinality and the semigroup Bergman property. The proposition is analogous to [22, Proposition 2.2] and although the proof is similar we include it for completeness.

Proposition 2.2.2. *Let S be a non-finitely generated semigroup. Then*

(i) $\mathrm{scf}(S) > \aleph_0$ *if and only if S has the semigroup Bergman property and* $\mathrm{cf}(S) > \aleph_0$*;*

(ii) *if* $\mathrm{scf}(S) > \aleph_0$*, then* $\mathrm{scf}(S) = \mathrm{cf}(S)$.

Proof. **Part (i).** ($\Rightarrow$) Since $\mathrm{cf}(S) \geq \mathrm{scf}(S)$ it follows immediately that $\mathrm{cf}(S) > \aleph_0$. Let U be any generating set for S and let $V_i = U \cup U^2 \cup \cdots \cup U^i$. Then $(V_i)_{i\in\mathbb{N}}$ is a chain of proper subsets of S such that $V_iV_i \subseteq V_{2i}$. Since U is a generating set for S, it also follows that $S = \bigcup_{i\in\mathbb{N}} V_i$. Hence, since

$\mathrm{scf}(S) > \aleph_0$, not all the subsets V_i can be proper and so there exists $j \in \mathbb{N}$ such that $S = V_j$ and so S is Cayley bounded with respect to U.

($\Leftarrow$) Seeking a contradiction, assume that $\mathrm{scf}(S) = \aleph_0$ and $(U_i)_{i\in\mathbb{N}}$ is a strong cofinal chain for S. Then $S = \bigcup_{i\in\mathbb{N}} U_i$ and so certainly $S = \bigcup_{i\in\mathbb{N}} \langle U_i \rangle$. Since $\mathrm{cf}(S) > \aleph_0$ it follows that $\langle\, U_r \,\rangle = S$ for some $r \in \mathbb{N}$. Hence since S has the semigroup Bergman property $S = U_r \cup U_r^2 \cup \cdots \cup U_r^n$ for some n. But $(U_i)_{i\in\mathbb{N}}$ is a strong cofinal chain and so $U_r \cup U_r^2 \cup \cdots \cup U_r^n \subseteq U_j$ for some j. Thus $S \subseteq U_j$, a contradiction.

Part (ii). Let $\mathrm{scf}(S) = \kappa$ and let $(U_i)_{i<\kappa}$ be a strong cofinal chain for S. Without loss of generality assume that $U_iU_i \subseteq U_{i+1}$ for all $i < \kappa$. If I is the set of all limit ordinals less than κ, then for any $i \in I$, $V_i = \bigcup_{j<i} U_j$ is a proper subsemigroup of S. Thus

$$\mathrm{scf}(S) \leq \mathrm{cf}(S) \leq |I| \leq \kappa = \mathrm{scf}(S)$$

giving equality throughout. □

The following lemma will be used later in the chapter as it gives a convenient way of proving that a semigroup has uncountable strong cofinality. The idea behind it is taken from [8] and [49]; we include a proof for completeness.

Lemma 2.2.3. *Let S be a non-finitely generated semigroup. Then $\mathrm{scf}(S) > \aleph_0$ if and only if every function $\Phi : S \to \mathbb{N}$ satisfying*

$$(st)\Phi \leq (s)\Phi + (t)\Phi + k_\Phi, \tag{2.1}$$

for all $s, t \in S$ and some constant $k_\Phi \in \{0, 1, 2, \ldots\}$, is bounded above.

Proof. ($\Rightarrow$) Let $\Phi : S \to \mathbb{N}$ be any function satisfying (2.1) and let

$$U_n = \{\, s \in S \,:\, (s)\Phi \leq n \,\}.$$

Then $S = \bigcup_{n\in\mathbb{N}} U_n$ and $U_mU_n \subseteq U_{m+n+k_\Phi}$. Hence, since $\mathrm{scf}(S) > \aleph_0$, we have that $S = U_n$ for some n. Thus n is the required upper bound for Φ.

($\Leftarrow$) By Proposition 2.2.2(i), it suffices to prove that $\mathrm{cf}(S) > \aleph_0$ and S has the semigroup Bergman property. Seeking a contradiction, assume that $\mathrm{cf}(S) = \aleph_0$. Then there exists a cofinal chain $(S_n)_{n\in\mathbb{N}}$ for S. Define $\Phi : S \to \mathbb{N}$ by

$$(s)\Phi = \min\{\, n \,:\, s \in S_n \,\}.$$

The function Φ satisfies (2.1) with $k_\Phi = 0$ but is unbounded above, a contradiction. Hence $\mathrm{cf}(S) > \aleph_0$.

Again in order to produce a contradiction, assume that there exists a generating set U for S such that S is not Cayley bounded with respect to U. As in the previous paragraph, define $\Phi : S \to \mathbb{N}$ by

$$(s)\Phi = \min\{\, n \,:\, s \in U^n \,\}.$$

Again, Φ satisfies (2.1) with $k_\Phi = 0$ but is unbounded above, a contradiction. Thus S satisfies the semigroup Bergman property and the proof is complete. □

The following notion and the subsequent lemma yield a convenient method for proving that a semigroup has uncountable strong cofinality. A semigroup S is called *strongly distorted* if there exists a sequence $(a_n)_{n\in\mathbb{N}}$ of natural numbers and $N_S \in \mathbb{N}$ such that for all sequences $(s_n)_{n\in\mathbb{N}}$ of elements from S there exist $t_1, t_2, \ldots, t_{N_S} \in S$ such that each s_n can be written as a product of length at most a_n in the letters $t_1, \ldots, t_{N_S}$. The following lemma was suggested to us by Y. de Cornulier and a similar result appears in Khelif [49, Theorem 6].

Lemma 2.2.4. *If S is non-finitely generated and strongly distorted, then* $\mathrm{scf}(S) > \aleph_0$.

Proof. Let $\Phi : S \longrightarrow \mathbb{N}$ be any function satisfying (2.1) and seeking a contradiction assume that Φ is unbounded above. Let $(a_n)_{n\in\mathbb{N}}$ and $N_S \in \mathbb{N}$ be as given in the definition of a strongly distorted semigroup S and assume without loss of generality that $(a_n)_{n\in\mathbb{N}}$ is strictly increasing. Then there exist $s_1, s_2, \ldots \in S$ such that $(s_n)\Phi > a_n^2$ for all n. Since S is strongly distorted there exist $t_1, \ldots, t_{N_S} \in S$ such that each s_n can be written as a product of length at most a_n in the letters $t_1, \ldots, t_{N_S}$. But if $M = \max\{(t_1)\Phi, \ldots, (t_{N_S})\Phi\}$, then

$$(s_n)\Phi \leq a_n \cdot k_\Phi + a_n \cdot M < a_n^2$$

for all sufficiently large n, a contradiction. Thus Φ is bounded above and so, by Lemma 2.2.3, $\mathrm{scf}(S) > \aleph_0$. □

In light of Proposition 2.2.2 we observe that for a non-finitely generated semigroup S there are four possibilities:

(i) $\mathrm{cf}(S) = \mathrm{scf}(S) > \aleph_0$ and so S satisfies the semigroup Bergman property;

(ii) $\mathrm{cf}(S) > \aleph_0 = \mathrm{scf}(S)$ and so S does not satisfy the semigroup Bergman property;

(iii) $\mathrm{cf}(S) = \mathrm{scf}(S) = \aleph_0$ and S satisfies the semigroup Bergman property;

(iv) $\mathrm{cf}(S) = \mathrm{scf}(S) = \aleph_0$ and S does not satisfy the semigroup Bergman property.

Of course, the next question is: are there examples of semigroups that satisfy each of these four cases? Finding an example that satisfies case (iv) is routine. For example, the free semigroup on an infinite set X has countable cofinality and does not satisfy the semigroup Bergman property. The next corollary relates the group and semigroup Bergman properties, and consequently provides several examples of semigroups that satisfy case (i) above.

Corollary 2.2.5. *If a group G has $\mathrm{scf}(G) > \aleph_0$, then G satisfies both the group and semigroup Bergman properties.*

In particular, $\mathrm{Sym}(\Omega)$, the homeomorphism groups of $\mathfrak{C}$, $\mathbb{Q}$, and $\mathbb{I}$, and the infinite cartesian power of any finite perfect group satisfy both the group and semigroup Bergman properties.

Proof. Since $\mathrm{scf}(G) > \aleph_0$ it follows from Propostion 2.2.2(i) that G satisfies the semigroup Bergman property. Now, by Lemma 2.2.1 the least cardinal of a cofinal chain of subgroups for G is greater than $\aleph_0$. Hence by [22, Proposition 2.2] G satisfies the group Bergman property.

By Lemma 2.2.1 and Droste and Göbel [22] it follows that $\mathrm{scf}(G) > \aleph_0$ when G is any of the groups $\mathrm{Sym}(\Omega)$ or the homeomorphism groups of $\mathfrak{C}$, $\mathbb{Q}$, or $\mathbb{I}$. Again by Lemma 2.2.1 and de Cornulier [20], the infinite cartesian power G of any finite perfect group satisfies $\mathrm{scf}(G) > \aleph_0$. □

The following example stems from [22] and provides a semigroup satisfying case (ii) above.

Example 2.2.6. Let $\mathrm{BSym}(\mathbb{Q})$ denote the group of all permutations $f \in \mathrm{Sym}(\mathbb{Q})$ where there exists $k \in \mathbb{N}$ such that $|x - (x)f| < k$ for all $x \in \mathbb{Q}$, called the *bounded permutation group* on $\mathbb{Q}$. Droste and Göbel [22] proved that the least cardinal of a cofinal chain of subgroups for $\mathrm{BSym}(\mathbb{Q})$ is uncountable but that $\mathrm{BSym}(\mathbb{Q})$ does not satisfy the group Bergman property. By [22, Proposition 2.2] and Lemma 2.2.1, $\mathrm{cf}(\mathrm{BSym}(\mathbb{Q})) > \aleph_0$ and $\mathrm{scf}(\mathrm{BSym}(\mathbb{Q})) = \aleph_0$. Thus by Proposition 2.2.2(i), $\mathrm{BSym}(\mathbb{Q})$ does not satisfy the semigroup Bergman property. So, $\mathrm{BSym}(\mathbb{Q})$ is an example of a (semi)group that satisfies case (ii) above.

It remains to find an example of semigroup satisfying case (iii). Khelif [49] provided an example of a group G where the least cardinal of a cofinal chain of subgroups for G is $\aleph_0$ and that satisfies the group Bergman property. Using the same reasoning as in Example 2.2.6 we deduce that

Khelif's group satisfies (iii). However, Khelif's construction is somewhat too complicated to include here. Moreover it is straightforward to directly construct examples of semigroups, that are not groups, with countable cofinality and that satisfy the semigroup Bergman property.

The following examples are trivial but are included for the sake of completeness.

Example 2.2.7. A semigroup S of *left zeros* satisfies $xy = x$ for all $x, y \in S$. The unique generating set for such a semigroup S is S itself. Therefore every semigroup of left zeros has the semigroup Bergman property. If S is infinite, then S is not finitely generated. Hence if (the generating set) S is partitioned into $S_1, S_2, \ldots$, then $(\langle\, S_1, \ldots, S_i \,\rangle)_{i\in\mathbb{N}} = (S_1 \cup \cdots \cup S_i)_{i\in\mathbb{N}}$ is a cofinal chain for S. Hence $\mathrm{cf}(S) = \aleph_0$.

Example 2.2.8. A *rectangular band* R is the direct product $I \times \Lambda$ of arbitrary sets I and Λ with multiplication $(i, \lambda)(j, \mu) = (i, \mu)$. Every generating set for R must for all $i \in I$ and $\mu \in \Lambda$ contain elements of the form (i, λ) and (j, μ) for some $\lambda \in \Lambda$ and $j \in I$. Therefore if $R = \langle\, U \,\rangle$, then $R = U^2$ and R has the semigroup Bergman property. Moreover, if R is infinite, then, as in Example 2.2.7, $\mathrm{cf}(R) = \aleph_0$.

An element s of an arbitrary semigroup S is *indecomposable* if $s \neq xy$ for all $x, y \in S$. The indecomposable elements of S must be contained in every generating set. If S is Cayley bounded with respect to a generating set consisting of indecomposable elements, then S satisfies the semigroup Bergman property.

Example 2.2.9. Let S be the semigroup defined by the presentation

$$\mathrm{Sg}\langle A : abc = ab \quad (a, b, c \in A)\rangle$$

for some infinite set of generators A. Then every element in A is indecomposable in S and $S = A \cup A^2$. Hence S has the semigroup Bergman property and $\mathrm{cf}(S) = \aleph_0$, as in Example 2.2.7.

Example 2.2.10. Let S be the set $\mathbb{N}\times\mathbb{N}$ with componentwise addition. Then the set

$$(\{1\} \times \mathbb{N}) \cup (\mathbb{N} \times \{1\})$$

is a generating set for S consisting of indecomposable elements. Therefore S has the semigroup Bergman property and $\mathrm{cf}(S) = \aleph_0$, as in Example 2.2.7.

Example 2.5.7 is a further semigroup having uncountable cofinality and not having the semigroup Bergman property. However, this example relies on results from Section 2.4 and so cannot be included here.

2.3 Subsemigroups, ideals, and homomorphic images

In this section we give the main tools that will provide a method to find the cofinality and strong cofinality of the semigroup $\mathrm{Self}(\Omega)$ of all self-maps of any infinite set Ω, and several other fundamental semigroups.

Theorem 2.3.1. *Let S be a non-finitely generated semigroup that is Cayley bounded with respect to the union of a subsemigroup T and a finite set F. Then $\mathrm{cf}(T) \leq \mathrm{cf}(S)$ and $\mathrm{scf}(T) \leq \mathrm{scf}(S)$.*

Proof. We will prove the theorem for strong cofinality. The proof for cofinality follows by an analogous argument.

Let $\lambda = \mathrm{scf}(S)$ and $(S_i)_{i<\lambda}$ be a strong cofinal chain for S. Set $T_i = S_i \cap T$ for all $i < \lambda$. We will prove that $T_i \subsetneq T$ for all i. Assuming the contrary, there exists $i < \lambda$ such that $T_i = T$. Since S is Cayley bounded with respect to $T \cup F$, there exists $n \in \mathbb{N}$ such that $S = (T \cup F) \cup (T \cup F)^2 \cup \cdots \cup (T \cup F)^n$. The set F is finite and so there exists $j < \lambda$ such that $F \subseteq S_j$. Thus $T \cup F = T_i \cup F$ is a subset of $S_{\max(i,j)}$. Since $(S_i)_{i<\lambda}$ is a strong cofinal chain, it follows that $S = S_m$ for some $m > \max(i, j)$, a contradiction. So, we have shown that for all $i < \lambda$, the set T_i is properly contained in T.

To conclude, $T_iT_i = (S_i \cap T)(S_i \cap T) \subseteq S_iS_i \cap T \subseteq S_k \cap T = T_k$, for some $k > i$. Therefore $\mathrm{scf}(T) \leq \lambda$. □

Theorem 2.3.2. *Let T be a subsemigroup of finite Rees index in a non-finitely generated semigroup S. Then $\mathrm{cf}(T) = \mathrm{cf}(S)$ and $\mathrm{scf}(T) = \mathrm{scf}(S)$.*

Furthermore, if T satisfies the semigroup Bergman property, then S does also.

Although Theorem 2.3.2 is similar to Theorem 2.3.1 it is somewhat harder to prove. The proof of Theorem 2.3.2 requires Lemma 2.2.3 and the following technical lemma.

Lemma 2.3.3. *Let T be a subsemigroup of a non-finitely generated semigroup S with $S \setminus T$ finite and $T \cap \langle S \setminus T \rangle \neq \emptyset$. Then $T \cap \langle S \setminus T \rangle$ is finitely generated.*

Proof. It is shown in [47] that if U is a finitely generated semigroup and $V \leq U$ with $U \setminus V$ finite, then V is finitely generated also.

So, $T \cap \langle S \setminus T \rangle = \langle S \setminus T \rangle \setminus (S \setminus T) \leq \langle S \setminus T \rangle$. By assumption, $S \setminus T$ is finite and so $T \cap \langle S \setminus T \rangle$ has finite complement in $\langle S \setminus T \rangle$ and $\langle S \setminus T \rangle$ is finitely generated. Thus $T \cap \langle S \setminus T \rangle$ is finitely generated. □

Equipped with Lemmas 2.2.3 and 2.3.3 we can now give the proof of Theorem 2.3.2.

Proof of Theorem 2.3.2. Recall that T is a subsemigroup of a non-finitely generated semigroup S with $S \setminus T$ finite. Assume without loss of generality that S has an identity 1_S and that $1_S \in S \setminus T$. Note that T is not finitely generated, otherwise S would be finitely generated. The proof has three parts.

Part 1: cf(*T*)=cf(*S*).

The cofinality of T is at most the cofinality of S by Theorem 2.3.1; that is,

$$\mathrm{cf}(T) \leq \mathrm{cf}(S).$$

It remains to prove the opposite inequality: $\mathrm{cf}(T) \geq \mathrm{cf}(S)$. Let $\mathrm{cf}(T) = \lambda$ and let $(T_i)_{i<\lambda}$ be a cofinal chain for T. From this cofinal chain, we will construct a chain with length λ of proper subsemigroups of S whose union is S.

The first step is to give an alternate cofinal chain $(U_i)_{i<\lambda}$ for T that involves $S \setminus T$. Define

$$U_i = \{\, t \in T \;:\; (\forall x, y \in S \setminus T)\ (xty \in T_i \cup (S \setminus T))\,\}.$$

To prove that $(U_i)_{i<\lambda}$ is a chain, let $i \leq j$ and let $t \in U_i$. Then $xty \in T_i \leq T_j$ whenever $xty \in T$, $x, y \in S \setminus T$. Thus U_i is contained in U_j and so $(U_i)_{i<\lambda}$ is a chain. Next we prove that the union of the sets U_i, $i < \lambda$, equals T. Let $t \in T$. Then there are only finitely many products xty in T where $x, y \in S \setminus T$. Hence there exists $i < \lambda$ such that all these products are in T_i. Hence $t \in U_i$ and so $\bigcup_{i<\lambda} U_i = T$.

It remains to prove that U_i is a proper subsemigroup of T for all $i < \lambda$. Let $i < \lambda$, $s, t \in U_i$, and $x, y \in S \setminus T$ such that $xsty \in T$. Of course such x and y exist since $1_S \in S \setminus T$. If either xs or $ty \in S \setminus T$, then $(xs)ty = xs(ty) \in T$ and so $xsty \in T_i$. On the other hand, if $xs, ty \in T$, then $xs1_S, 1_Sty \in T$ and so $xs1_S, 1_Sty \in T_i$. But T_i is a subsemigroup and so $xsty \in T_i$. Thus $st \in U_i$ and U_i is a subsemigroup. If $x = y = 1_S$ and $t \in U_i$, then $xty \in T$ and so $t = xty \in T_i$. Hence U_i is contained in T_i and as such is a proper subsemigroup of T.

Now, let us construct a cofinal chain for S using the chain $(U_i)_{i<\lambda}$. Let S_i, $i < \lambda$, be the subsemigroup of S generated by U_i and $S \setminus T$; that is, $S_i = \langle U_i, S \setminus T \rangle$. Clearly, $(S_i)_{i<\lambda}$ is a chain and $\bigcup_{i<\lambda} S_i = S$. So, to prove that $(S_i)_{i<\lambda}$ is a cofinal chain for S it suffices to show that every S_i is properly contained in S. We will do this by showing that $S_i \cap T \leq T_i$ for all $N < i < \lambda$ for some N.

By Lemma 2.3.3, $T \cap \langle\, S \setminus T \,\rangle$ is finitely generated and so there exists $N < \lambda$ such that for all $i > N$ we have $T \cap \langle S \setminus T \rangle \subseteq U_i$. If $t \in S_i \cap T$ for some

$i > N$, then there exist $w_1, w_2, \ldots, w_{k+1} \in \langle\, S \setminus T \,\rangle$ and $u_1, u_2, \ldots, u_k \in U_i$ such that

$$t = w_1 u_1 w_2 u_2 \cdots u_k w_{k+1}, \tag{2.2}$$

and $2k+1$ is the least length of such a product. If $w_j \in \langle S \setminus T \rangle \cap T$, then, since $i > N$, $w_j \in U_i$ and the product (2.2) could be shortened. So, we conclude that $w_1, w_2, \ldots, w_{k+1} \in S \setminus T$. Consider the products $w_m u_m, w_n u_n w_{n+1} \in S$ where $1 \leq m, n \leq k$. If either product lies in $S \setminus T$, then again (2.2) could be shortened. Hence $w_m u_m, w_n u_n w_{n+1} \in T$, and by the definition of U_i, $w_m u_m, w_n u_n w_{n+1} \in T_i$. But T_i is a subsemigroup of T and so $t \in T_i$.

We conclude that $S_i \cap T \leq T_i$ and so if $S = S_i$ for some i, then $T = S \cap T = S_i \cap T \leq T_i < T$, a contradiction. Hence S_i is a proper subsemigroup of S. We have shown that $\mathrm{cf}(T) \geq \mathrm{cf}(S)$ and this part of the proof is concluded.

Part 2: scf(*T*)=scf(*S*).

If $\mathrm{scf}(S) = \aleph_0$, then by Theorem 2.3.1 we have $\aleph_0 \leq \mathrm{scf}(T) \leq \mathrm{scf}(S) = \aleph_0$, giving equality throughout. Assume that $\mathrm{scf}(S) > \aleph_0$. Then if $\mathrm{scf}(T) > \aleph_0$, we could deduce that $\mathrm{scf}(T) = \mathrm{cf}(T) = \mathrm{cf}(S) = \mathrm{scf}(S)$, by Proposition 2.2.2(ii) and the first part of the theorem. So, we are left with the task of proving that $\mathrm{scf}(T) > \aleph_0$.

Let $\Psi : T \to \mathbb{N}$ be any function satisfying

$$(st)\Psi \leq (s)\Psi + (t)\Psi + k_\Psi$$

for all $s, t \in T$ and for some constant $k_\Psi \in \{0, 1, 2, \ldots\}$. By Lemma 2.2.3, it suffices to prove that Ψ is bounded. We proceed in a similar fashion as in the proof of the previous part of the theorem. That is, we define $\Phi : T \to \mathbb{N}$ using Ψ and subsequently define $\Upsilon : S \to \mathbb{N}$ satisfying (2.1). Let $\Phi : T \to \mathbb{N}$ be defined by

$$(t)\Phi = \max\{\, (xty)\Psi \;:\; x, y \in S \setminus T,\; xty \in T \,\}.$$

Note that Φ is well-defined since the set $\{\, (xty)\Psi \;:\; x, y \in S \setminus T,\; xty \in T \,\}$ is non-empty and finite. To prove that Φ satisfies (2.1) let $s, t \in T$. Then

$$(st)\Phi = \max\{\, (x \cdot st \cdot y)\Psi \;:\; x, y \in S \setminus T,\; x \cdot st \cdot y \in T \,\}.$$

The set $\{\, (x \cdot st \cdot y)\Psi \;:\; x, y \in S \setminus T,\; x \cdot st \cdot y \in T \,\}$ is the union of the following three sets

$$A = \{\, (xs \cdot t \cdot y)\Psi \;:\; x, y \in S \setminus T,\; xs \cdot t \cdot y \in T, xs \in S \setminus T \,\},$$

$$B = \{\ (x \cdot s \cdot ty)\Psi\ :\ x, y \in S \setminus T,\ x \cdot s \cdot ty \in T, ty \in S \setminus T\ \},$$
$$C = \{\ (xs \cdot ty)\Psi\ :\ x, y \in S \setminus T,\ xs \cdot ty \in T, xs, ty \in T\ \}.$$

So,

$$\begin{aligned}(st)\Phi &\leq \max\{\ \max A,\ \max B,\ \max C\ \} \\ &\leq \max\{(t)\Phi, (s)\Phi, (s)\Phi + (t)\Phi + k_\Psi\} = (s)\Phi + (t)\Phi + k_\Psi,\end{aligned}$$

and Φ satisfies (2.1).

As the final step in the proof, define $\Upsilon : S \to \mathbb{N}$ by

$$(s)\Upsilon = \begin{cases}(s)\Phi & \text{if } s \in T \\ 1 & \text{if } s \in S \setminus T.\end{cases}$$

Note that $(t)\Upsilon = (t)\Phi \geq (t)\Psi$ for all $t \in T$. So, to prove that Ψ is bounded it suffices to prove that Υ satisfies (2.1). Let $s, t \in S$. Then there are four cases to consider.

Firstly, if $s, t \in T$, then Υ trivially satisfies (2.1) with constant k_Ψ since Φ does.

Secondly, let

$$M = \max\{\ (st)\Upsilon\ :\ s, t \in S \setminus T\ \}.$$

Then for all $s, t \in S \setminus T$ we have that if $st \in S \setminus T$, then $(st)\Upsilon = 1 < (s)\Upsilon + (t)\Upsilon + M$. On the other hand, if $st \in T$, then $(st)\Upsilon = (st)\Phi \leq M$. In either case,

$$(st)\Upsilon \leq (s)\Upsilon + (t)\Upsilon + M.$$

Thirdly, let $s \in S \setminus T$ and $t \in T$. If $st \in S \setminus T$, then $(st)\Upsilon = 1 \leq (s)\Upsilon + (t)\Upsilon$. Otherwise, $(st)\Upsilon = (st)\Phi = (x \cdot st \cdot y)\Psi$ for some $x, y \in S \setminus T$ with $x \cdot st \cdot y \in T$, from the definitions of Φ and Υ. Let

$$P = \{\ (us \cdot t \cdot v)\Psi\ :\ us, u, v \in S \setminus T,\ ustv \in T\ \}$$

$$Q = \{\ (us \cdot t \cdot v)\Psi\ :\ us \in T,\ u, v \in S \setminus T,\ ustv \in T\ \}.$$

Then $\max\{P\} \leq (t)\Phi = (t)\Upsilon$ from the definition and for all $(us \cdot t \cdot v)\Psi \in Q$

$$(us \cdot t \cdot v)\Psi \leq (us \cdot t)\Phi \leq (us)\Phi + (t)\Phi + k_\Psi \leq M + (t)\Phi + k_\Psi.$$

This implies that $\max\{Q\} \leq M + (t)\Phi + k_\Psi = M + (t)\Upsilon + k_\Psi$. Hence

$$(st)\Upsilon \leq \max\{\ P, Q\ \} \leq (t)\Upsilon + M + k_\Psi \leq (s)\Upsilon + (t)\Upsilon + M + k_\Psi.$$

Finally, if $s \in T$ and $t \in S \setminus T$, then $(st)\Upsilon \leq (s)\Upsilon + (t)\Upsilon + M + k_\Psi$ follows by symmetry.

Therefore Υ satisfies (2.1) with constant $M + k_\Psi$, and the proof of this part of the theorem is complete.

Part 3: if T satisfies the semigroup Bergman property, then S does also.

Let U be any generating set for S. We must prove that S is Cayley bounded with respect to U. Since $S \setminus T$ is finite, there exists $m \in \mathbb{N}$ such that $S \setminus T \subseteq U \cup U^2 \cup \cdots \cup U^m = V$. Obviously V generates S. By the Schreier Theorem for semigroups [17, Theorem 3.1] or [47], the set

$$X = \{\, xvy \,:\, x, y \in S \setminus T,\ v \in V,\ xv, xvy \in T \,\}$$

generates T. Clearly $X \subseteq V \cup V^2 \cup V^3$. But T satisfies the semigroup Bergman property and so $T = X \cup X^2 \cup \cdots \cup X^n$ for some $n \in \mathbb{N}$. Thus

$$S = (S \setminus T) \cup T = V \cup V^2 \cup \cdots \cup V^{3n} = U \cup U^2 \cup \cdots \cup U^{3mn},$$

as required. □

In light of Theorems 2.3.1 and 2.3.2, it is natural to ask: do the equalities $\mathrm{cf}(S) = \mathrm{cf}(T)$ and $\mathrm{scf}(S) = \mathrm{scf}(T)$ hold when S is a non-finitely generated semigroup that is Cayley bounded with respect to the union of a subsemigroup T and a finite set F? Perhaps the simplest case not covered by Theorem 2.3.2, is when $S = (T \cup F)^2$. We will show in Examples 2.5.4 and 2.5.5 that the conclusions of Theorem 2.3.2 no longer hold even for this simple case.

The other question we should ask is: if T is a subsemigroup of S such that $S \setminus T$ is finite and S has the semigroup Bergman property, then does T have the semigroup Bergman property too? Unfortunately, we do not know the answer to this question.

It was noted by Bergman in [8] that the group Bergman property is preserved by homomorphisms. However, as the following lemma demonstrates this is no longer true for the semigroup Bergman property.

Lemma 2.3.4. *Let S be a semigroup. Then there exists a semigroup T such that S is a homomorphic image of T and T satisfies the semigroup Bergman property.*

Proof. The presentation

$$\mathrm{Sg}\langle A : a_s a_t = a_{st} \quad (s, t \in S)\rangle$$

derived from the Cayley table of S where $A = \{\, a_s \,:\, s \in S \,\}$, defines a semigroup isomorphic to S. Let T be the semigroup defined by the presentation

$$\mathrm{Sg}\langle A : a_s a_t a_u = a_{st} a_u \quad (s, t, u \in S)\rangle.$$

The semigroup S satisfies the relations in the presentation for T. Thus S is a homomorphic image of T.

Now, the set A consists of indecomposable elements in T and so, by the comments preceding Example 2.2.9, every generating set for T contains A. But $A \cup A^2 = T$ and so T satisfies the semigroup Bergman property. $\square$

Although not all homomorphisms preserve the semigroup Bergman property, one distinguished type does. A *Rees quotient* of a semigroup S by an ideal I is the quotient of S by the congruence with (at most) one non-singleton class $I \times I$, denoted S/I.

Lemma 2.3.5. *Let S be a semigroup and I an ideal of S. Then*

(i) *if S has semigroup Bergman property, then so does the Rees quotient S/I;*

(ii) *if I and S/I have the semigroup Bergman property, then so does S.*

Proof. **Part (i).** Let $U = V \cup \{0\}$ be any generating set for S/I where $V \subseteq S \setminus I$. Since I is an ideal, $V \cup I$ generates S. But S satisfies the semigroup Bergman property and so $S = (V \cup I) \cup (V \cup I)^2 \cup \cdots \cup (V \cup I)^n$ for some n. Thus $S/I = (V \cup \{0\}) \cup (V \cup \{0\})^2 \cup \cdots \cup (V \cup \{0\})^n$, as required.

Part (ii). Let U be any generating set for S. Then $\langle\, U \setminus I, 0 \,\rangle = S/I$ and so $S \setminus I \subseteq (U \setminus I) \cup (U \setminus I)^2 \cup \cdots \cup (U \setminus I)^n$ for some n.

Assume, without loss of generality, that $S \setminus I$ contains an identity for S. By [17, Theorem 3.1], the set

$$V = \{\, xuy \;:\; x, y \in S \setminus I,\; u \in U,\; xu, xuy \in I \,\}$$

generates I; Thus $I = V \cup V^2 \cup \cdots \cup V^m$ for some m.

To conclude, $V \subseteq (S \setminus I)U(S \setminus I) \subseteq U \cup U^2 \cup \cdots \cup U^{3n}$. It follows that

$$S = (S \setminus I) \cup I \subseteq U \cup U^2 \cup \cdots \cup U^{3mn},$$

as required. $\square$

The converse of Lemma 2.3.5(i) obviously does not hold (if $I = S$, then S/I has the semigroup Bergman property). Example 2.5.6 shows that the converse of Lemma 2.3.5(ii) also does not hold.

2.4 Positive Examples

In this section we apply the results of the previous sections to prove that various standard semigroups satisfy the semigroup Bergman property. In Section 2.5, we provide some negative examples, that is, natural semigroups that do not satisfy the Bergman property.

Theorem 2.4.1. *Let Ω be an infinite set and let S be any of* $\mathrm{Self}(\Omega)$, $\mathrm{SymInv}(\Omega)$, $\mathrm{Part}(\Omega)$ *or* $\mathrm{Bin}(\Omega)$. *Then* $\mathrm{scf}(S) > |\Omega|$ *and so S satisfies the semigroup Bergman property.*

Proof. By [54, Theorem 1.1] and Lemma 2.2.1, $\mathrm{cf}(\mathrm{Sym}(\Omega)) > |\Omega|$. Hence, by Proposition 2.2.2(i) and since $\mathrm{Sym}(\Omega)$ satisfies the Bergman property [8], $\mathrm{scf}(\mathrm{Sym}(\Omega)) > \aleph_0$. It follows, by Proposition 2.2.2(ii), that $\mathrm{scf}(\mathrm{Sym}(\Omega)) = \mathrm{cf}(\mathrm{Sym}(\Omega)) > |\Omega| \geq \aleph_0$.

It follows by [39, Proposition 1.7 and Theorem 4.5] and [4, Theorem 3.4] that there exist $f, g \in S$ such that $f\,\mathrm{Sym}(\Omega)g = S$. Thus, $S = (\mathrm{Sym}(\Omega) \cup \{f, g\})^3$. Hence, by Theorem 2.3.1, $\mathrm{scf}(S) \geq \mathrm{scf}(\mathrm{Sym}(\Omega)) > |\Omega| \geq \aleph_0$. In particular, by Proposition 2.2.2(i), S satisfies the semigroup Bergman property.

An alternative proof can be obtained using Lemma 2.2.4. It follows from the way how the main results were proved in [79], and from the proof of [39, Proposition 4.2] that for all sequences $(f_n)_{n\in\mathbb{N}}$ of elements from S there exist $f, g \in S$ such that every f_n is a product of f and g with length bounded by a linear function. Hence S is strongly distorted and so, by Lemma 2.2.4, $\mathrm{scf}(S) > \aleph_0$. □

Mesyan [63, Proposition 4] proved that $\mathrm{cf}(\mathrm{Self}(\Omega)) > \aleph_0$ using an elementary diagonal argument, and an alternative proof of Theorem 2.4.1 can be obtained using a similar argument. In Galvin [29] it was shown that the symmetric group on an infinite set is strongly distorted. Hence Bergman's original theorem follows immediately by Lemma 2.2.4.

It was proved in [5] and [65] that the semigroups, appearing in the following theorem are strongly distorted, so the proof of our next result follows immediately from Lemma 2.2.4.

Theorem 2.4.2. *Let S be one of the following semigroups: the linear functions of an infinite dimensional vector space, the endomorphism semigroup of the random graph, the continuous functions on the unit interval* $[0, 1]$, *the Lebesgue, or Borel measurable functions on* $[0, 1]$, *the order endomorphisms of* $[0, 1]$, *or the Lipschitz functions on* $[0, 1]$. *Then* $\mathrm{scf}(S) > \aleph_0$ *and S has the Bergman property.*

Next, following de Cornulier [11, Theorem 3.1], we consider a further class of semigroups that satisfy the semigroup Bergman property. The notions of algebraically and existentially closed groups were introduced by Scott [78] in 1950 and an extensive analysis can be found in [40]. Neumann considered these notions for semigroups in [68]. Analogous notions have been considered in the more general context of model theory.

Let $\mathbb{S}$ be the class of all semigroups and let κ be an infinite cardinal. Then $S \in \mathbb{S}$ is *κ-algebraically closed in* $\mathbb{S}$ if every set E of equations, with $|E| < \kappa$ and coefficients from S, that is solvable in some $T \in \mathbb{S}$ containing S, already has a solution in S. The analogous notions for groups and inverse semigroups can be obtained by replacing every occurrence of $\mathbb{S}$ in the preceding sentences with the class of all groups $\mathbb{G}$ or the class of all inverse semigroups $\mathbb{I}$. Recall that a semigroup S is *inverse* if for all $x \in S$ there exists a unique x^{-1} such that $xx^{-1}x = x$ and $x^{-1}xx^{-1} = x^{-1}$. Note that equations over $\mathbb{G}$ or $\mathbb{I}$ can include inverses of coefficients and variables.

Theorem 2.4.3. *Let S be an ω_1-algebraically closed semigroup, inverse semigroup, or group where ω_1 denotes the first uncountable cardinal. Then $\mathrm{scf}(S) > \aleph_0$ and S has the semigroup Bergman property.*

Proof. We will prove that S is strongly distorted.

Let $f_1, f_2, \ldots \in S$ and assume without loss of generality that S is a subsemigroup of $T = \mathrm{Self}(\Omega)$, $\mathrm{SymInv}(\Omega)$, or $\mathrm{Sym}(\Omega)$, respectively, for some infinite set Ω. As in the proof of Theorem 2.4.1, by the way how the theorems [29, Theorem 3.3] and [39, Proposition 4.2] were proved, and by the main results in [79], it follows that there exist $f, g \in T$ such that every f_n is a product of f and g with length bounded by a linear function. Since S is an ω_1-algebraically closed semigroup, it follows that there exist $f', g' \in S$ such that every f_n is a product of f' and g' with length bounded by a linear function. Hence S is strongly distorted and so by Lemma 2.2.4, $\mathrm{scf}(S) > \aleph_0$. □

Theorem 2.4.4. *Let $\mathcal{C}_{\mathbb{Q}}, \mathcal{C}_{\mathbb{I}}$ and $\mathcal{C}_{\mathfrak{C}}$ denote the semigroups of all continuous functions from the rationals $\mathbb{Q}$ to $\mathbb{Q}$, from the irrationals $\mathbb{I}$ to $\mathbb{I}$, and from the Cantor's discontinuum $\mathfrak{C}$ to $\mathfrak{C}$, respectively, and let $S \in \{\mathcal{C}_{\mathbb{Q}}, \mathcal{C}_{\mathbb{I}}, \mathcal{C}_{\mathfrak{C}}\}$. Then $\mathrm{scf}(S) > \aleph_0$ and so S satisfies the semigroup Bergman property.*

In order to prove Theorem 2.4.4 we require the following straightforward lemma.

Lemma 2.4.5. *Let $p \in \mathbb{R} \cup \{-\infty\}$ and $q \in \mathbb{R}$ with $p < q$. Then there exists an order preserving piecewise linear bijection from $\mathbb{Q}$ to $\mathbb{Q} \cap (p, q)$.*

Proof of Theorem 2.4.4. We will prove the theorem in the case that $S = \mathcal{C}_{\mathbb{Q}}$. The proofs in the other two cases are analogous.

Seeking a contradiction, assume that $(U_i)_{i\in\mathbb{N}\cup\{0\}}$ is a strong cofinal chain for $\mathcal{C}_{\mathbb{Q}}$. Let $p \in \mathbb{R} \setminus \mathbb{Q}$ be arbitrary but fixed. Then define $\Sigma_0 = (-\infty, p) \cap \mathbb{Q}$ and for $n \geq 1$ define

$$\Sigma_n = (p + n - \frac{1}{2}, p + n) \cap \mathbb{Q}.$$

Let $\mathcal{C}_{\Sigma_n}$ denote the semigroup of continuous functions on Σ_n. Then we will prove that

$$U_n|_{\Sigma_n} = \{\, f \in \mathcal{C}_{\Sigma_n} \ : \ f = g|_{\Sigma_n},\ g \in U_n \,\} \neq \mathcal{C}_{\Sigma_n}$$

for all $n \in \mathbb{N} \cup \{0\}$.

Assume otherwise, that is, there exists $n \in \mathbb{N} \cup \{0\}$ such that $U_n|_{\Sigma_n} = \mathcal{C}_{\Sigma_n}$. Then for some $n \geq 0$, by Lemma 2.4.5, there exists an order preserving continuous bijection $f : \mathbb{Q} \to \Sigma_n$. Since f is piecewise linear, f^{-1} is also an order preserving continuous bijection, and so f^{-1} can be extended to $g \in \mathcal{C}_{\mathbb{Q}}$. Thus $fU_ng = \mathcal{C}_{\mathbb{Q}}$ and so there exists $m \geq n$ such that $\mathcal{C}_{\mathbb{Q}} = U_m$, a contradiction.

Therefore for all $n \geq 0$ there exists $f_n \in \mathcal{C}_{\Sigma_n}$ such that $f_n \notin U_n|_{\Sigma_n}$. Let $f \in \mathcal{C}_{\mathbb{Q}}$ be any extension of the function defined by $x \mapsto xf_n$ for all $x \in \Sigma_n$ and for all n. Then $f \notin \bigcup_{n\in\mathbb{N}\cup\{0\}} U_n$, a contradiction. □

The *finitary power semigroup* of a semigroup S is the set of all finite subsets of S with multiplication $X \cdot Y = \{\, xy \ : \ x \in X \ \&\ y \in Y \,\}$. We will denote this semigroup by $\mathcal{P}(S)$.

The following theorem was initially motivated by the search for an example with the properties of the semigroup given in Example 2.5.5, as discussed after the proof of Theorem 2.3.2. Although very similar, of the four semigroups S appearing in Theorem 2.4.1, somewhat unexpectedly, only one has the property that $\mathcal{P}(S)$ has the semigroup Bergman property and the other three do not, see Theorem 2.5.2.

Theorem 2.4.6. *Let Ω be an infinite set. Then $\mathcal{P}(\mathrm{SymInv}(\Omega))$ satisfies the semigroup Bergman property.*

We will prove Theorem 2.4.6 in a series of lemmas. Although the next lemma is straightforward we state it explicitly because of its usefulness.

Lemma 2.4.7. *Let T be a subsemigroup of S and $\mathrm{scf}(T) > \aleph_0$. Then for any generating set U of S we have $T \subseteq U \cup U^2 \cup \cdots \cup U^n$ for some $n \in \mathbb{N}$.*

Proof. Let $V_i = U \cup U^2 \cup \cdots \cup U^i$. Since $S = \bigcup_{i\in\mathbb{N}} V_i$, we have that $T = \bigcup_{i\in\mathbb{N}} V_i \cap T$. It is clear that $V_i \subseteq V_{i+1}$ and that $V_i^2 \subseteq V_{2i}$. Hence $V_n \cap T = T$ for some n, from the assumption that $\mathrm{scf}(T) > \aleph_0$. Therefore $T \subseteq V_n$, as required. □

The following notion was first defined in [26]. Let S be a semigroup. Then a product $X_1X_2\cdots X_r$ in $\mathcal{P}(S)$ is said to be *without surplus elements* if for all $i \in \{1,\ldots,r\}$ and for all $x \in X_i$

$$X_1X_2\cdots X_r \neq X_1\cdots X_{i-1}(X_i \setminus \{x\})X_{i+1}\cdots X_r.$$

Lemma 2.4.8. *Let $X \in \mathcal{P}(S)$ such that $X = Y_1Y_2\cdots Y_r$ for some $Y_1, Y_2, \ldots, Y_r \in \mathcal{P}(S)$. Then there exist $Z_1, Z_2, \ldots, Z_r \in \mathcal{P}(S)$ such that $Z_i \subseteq Y_i$, $|Z_i| \leq |X|$, and $X = Z_1Z_2\cdots Z_r$ is without surplus elements.*

Moreover, if $|Z_i| = |X|$ for some i, then $|Z_j| = 1$ for all $j \neq i$.

For a proof see [26, Lemma 3.1].

The following lemma is similar to Lemma 2.4.8 but is more specific to our considerations.

Lemma 2.4.9. *Let $X \in \mathcal{P}(\mathrm{Sym}(\Omega))$ such that $X = Y_1Y_2\cdots Y_r$ is without surplus elements for some $Y_1, Y_2, \ldots, Y_r \in \mathcal{P}(\mathrm{SymInv}(\Omega))$. Then there exist $Z_1, Z_2, \ldots, Z_r \in \mathcal{P}(\mathrm{Sym}(\Omega))$ with $|Z_i| = |Y_i|$ for all i and $X = Z_1Z_2\cdots Z_r$.*

Proof. Let $y_1 \in Y_1, y_2 \in Y_2, \ldots, y_r \in Y_r$ be some fixed elements. Then $y_1y_2\cdots y_r \in \mathrm{Sym}(\Omega)$. The sets $\Omega_1, \Omega_2, \ldots, \Omega_{r+1}$ are defined by $\Omega_1 = \Omega$ and $\Omega_i = (\Omega)y_1y_2\cdots y_{i-1}$. Then $\Omega_{r+1} = \Omega$. From the definition of Ω_i, the restriction $y_i|_{\Omega_i}$ is a bijection from Ω_i to Ω_{i+1}.

Take now arbitrary $z_i \in Y_i$. Then $z_i|_{\Omega_i}$ is a bijection from Ω_i to Ω_{i+1} also. Otherwise $y_1y_2\cdots y_{i-1}z_iy_{i+1}\cdots y_r \notin \mathrm{Sym}(\Omega)$, a contradiction. Hence

$$z_1z_2\cdots z_r = z_1|_{\Omega_1}z_2|_{\Omega_2}\cdots z_r|_{\Omega_r}.$$

Note that if $z_i \neq t_i \in Y_i$, then $z_i|_{\Omega_i} \neq t_i|_{\Omega_i}$ since $Y_1Y_2\cdots Y_r$ is without surplus elements.

So, if $g_i : \Omega \to \Omega_i$, $2 \leq i \leq r$, is a bijection and $g_1 = g_{r+1}$ is the identity, then

$$z_1z_2\cdots z_r = (g_1 \cdot z_1|_{\Omega_1} \cdot g_2^{-1})(g_2 \cdot z_2|_{\Omega_2} \cdot g_3^{-1})\cdots(g_r \cdot z_r|_{\Omega_r} \cdot g_{r+1}^{-1}).$$

Now, $g_i \cdot z_i|_{\Omega_i} \cdot g_{i+1}^{-1} \in \mathrm{Sym}(\Omega)$ for all i. So, let $Z_i = \{\, g_i \cdot z_i|_{\Omega_i} \cdot g_{i+1}^{-1} \,:\, z_i \in Y_i \,\}$. It remains to show that $|Z_i| = |Y_i|$ for all i. In fact, if $z_i \neq t_i \in Y_i$, then $z_i|_{\Omega_i} \neq t_i|_{\Omega_i}$ and so $g_i \cdot z_i|_{\Omega_i} \cdot g_{i+1}^{-1} \neq g_i \cdot t_i|_{\Omega_i} \cdot g_{i+1}^{-1}$. □

An element $X \in \mathcal{P}(\mathrm{Sym}(\Omega))$ is said to be *power indecomposable* if it cannot be given as a product of finite sets Y and Z from $\mathrm{Sym}(\Omega)$ where $|Y|, |Z| < |X|$. In [28, Lemma 2] it is shown that a set $X \in \mathcal{P}(\mathrm{Sym}(\Omega))$ is power indecomposable if and only if X satisfies

(i) $x \neq yz^{-1}t$ for all distinct $x, y, z, t \in X$;

(ii) $x \neq yz^{-1}y$ for all distinct $x, y, z \in X$.

Moreover, in [28, Lemma 3] it is proved that for all $n \in \mathbb{N}$ there exists a set satisfying conditions (i) and (ii) with size n.

Proof of Theorem 2.4.6. We will prove that $\mathcal{P}(\mathrm{SymInv}(\Omega)$ has the semigroup Bergman property. Let $\mathfrak{U}$ be any generating set for $\mathcal{P}(\mathrm{SymInv}(\Omega))$. We will start by showing that it suffices to prove that there exists $n \in \mathbb{N}$ such that

$$\mathcal{P}(\mathrm{Sym}(\Omega)) \subseteq \mathfrak{U} \cup \mathfrak{U}^2 \cup \cdots \cup \mathfrak{U}^n. \tag{2.3}$$

Of course, there exist subsemigroups of $\mathcal{P}(\mathrm{SymInv}(\Omega))$ isomorphic to $\mathrm{SymInv}(\Omega)$ and $\mathrm{Sym}(\Omega)$, i.e. those consisting of singletons. For the sake of simplicity we will denote these subsemigroups by $\mathrm{SymInv}(\Omega)$ and $\mathrm{Sym}(\Omega)$, respectively.

If Ω is an infinite set, then a subset Σ is called a *moiety* if $|\Sigma| = |\Omega \setminus \Sigma| = |\Omega|$. Let Σ be a moiety in Ω and $f : \Omega \to \Sigma$ be bijective. Then, by [39, Theorem 4.5], it follows that $\{f\}\,\mathrm{Sym}(\Omega)\{f^{-1}\} = \mathrm{SymInv}(\Omega)$. So, we deduce that $\{f\}\mathcal{P}(\mathrm{Sym}(\Omega))\{f^{-1}\} = \mathcal{P}(\mathrm{SymInv}(\Omega))$. By Theorem 2.4.1, $\mathrm{scf}(\mathrm{SymInv}(\Omega)) > \aleph_0$, and so by Lemma 2.4.7 there exists $m \in \mathbb{N}$ such that

$$\mathrm{SymInv}(\Omega) \subseteq \mathfrak{U} \cup \mathfrak{U}^2 \cup \cdots \cup \mathfrak{U}^m. \tag{2.4}$$

In particular, $\{f\}, \{f^{-1}\} \in \mathfrak{U} \cup \mathfrak{U}^2 \cup \cdots \cup \mathfrak{U}^m$. Hence to prove that $\mathcal{P}(\mathrm{SymInv}(\Omega))$ is Cayley bounded with respect to $\mathfrak{U}$ it suffices to prove that (2.3) holds for some n.

Let $\mathfrak{V}$ denote the power indecomposable elements in $\mathcal{P}(\mathrm{Sym}(\Omega))$. We now prove that $\mathcal{P}(\mathrm{Sym}(\Omega)) \subseteq \{f\}\mathfrak{V}\{f^{-1}\}$. Let $X = \{x_1, x_2, \ldots, x_t\} \in \mathcal{P}(\mathrm{Sym}(\Omega))$ be arbitrary. Then there exist $y_1, y_2, \ldots, y_t \in \mathrm{Sym}(\Sigma)$ such that $x_i = fy_if^{-1}$ for all i. As mentioned in the comments just before the proof, by [28, Lemma 3] there exists a set $\{z_1, z_2, \ldots, z_t\} \in \mathcal{P}(\mathrm{Sym}(\Omega \setminus \Sigma))$ that does satisfy conditions (i) and (ii). Let $v_i \in \mathrm{Sym}(\Omega)$ be defined by

$$(\alpha)v_i = \begin{cases} (\alpha)y_i & \alpha \in \Sigma \\ (\alpha)z_i & \alpha \in \Omega \setminus \Sigma. \end{cases}$$

Then $V = \{v_1, v_2, \ldots, v_t\}$ satisfies conditions (i) and (ii) and so $V \in \mathfrak{V}$. It follows that $X = fVf^{-1} \in \{f\}\mathfrak{V}\{f^{-1}\}$ and so $\mathcal{P}(\mathrm{Sym}(\Omega)) \subseteq \{f\}\mathfrak{V}\{f^{-1}\}$ as required.

Finally, we will prove that $\mathfrak{V} \subseteq \mathrm{SymInv}(\Omega)\mathfrak{U}\,\mathrm{SymInv}(\Omega)$. Let $V \in \mathfrak{V}$. Then there exist $U_1, U_2, \ldots, U_r \in \mathfrak{U}$ such that $V = U_1U_2\cdots U_r$ for some r. Then by Lemma 2.4.8 there exist $X_1, X_2, \ldots, X_r$ such that $X_i \subseteq U_i$, $|X_i| \leq |V|$ and $V = X_1X_2\cdots X_r$ is without surplus elements and if $|X_i| = |V|$ for some i, then $|X_j| = 1$ for all $j \neq i$. Hence by Lemma 2.4.9 there exist $Y_1, Y_2, \ldots, Y_r \in \mathcal{P}(\mathrm{Sym}(\Omega))$ such that $V = Y_1Y_2\cdots Y_r$ and $|Y_i| = |X_i|$ for all i. But $V \in \mathfrak{V}$ and so there exists i such that $|Y_i| = |V|$. Thus $|X_i| = |V|$ and $|X_j| = 1$ for all $j \neq i$. So,

$$V \subseteq X_1\cdots X_{i-1}U_iX_{i+1}\cdots X_r \subseteq U_1U_2\ldots U_r = V.$$

Hence $V = X_1\cdots X_{i-1}U_iX_{i+1}\cdots X_r \in \mathrm{SymInv}(\Omega)\mathfrak{U}\,\mathrm{SymInv}(\Omega)$. Therefore

$$\mathcal{P}(\mathrm{Sym}(\Omega)) \subseteq \{f\}\mathfrak{V}\{f^{-1}\} \subseteq \mathrm{SymInv}(\Omega)\mathfrak{U}\,\mathrm{SymInv}(\Omega) \subseteq \mathfrak{U}\cup\mathfrak{U}^2\cup\cdots\cup\mathfrak{U}^{2m+1}.$$

Thus (2.3) is satisfied with $n = 2m + 1$, as required. □

It is natural to ask if it is possible to construct new semigroups with the semigroup Bergman property from semigroups that are known to have the property. It is known [20] that the infinite cartesian power of infinitely many copies of a finite group G has the group Bergman property if and only if G is perfect. If G, in the previous sentence, is replaced with an infinite group, then no such necessary and sufficient conditions are known. In fact, very little is known even for specific examples of infinite groups, see [20]. The situation for semigroups is perhaps even worse. However, as our final positive example shows, the cartesian product of at most $|\Omega|$ copies of $\mathrm{Self}(\Omega)$ has the semigroup Bergman property.

Theorem 2.4.10. *Let Ω be an infinite set, let S be any of* $\mathrm{Self}(\Omega)$, $\mathrm{SymInv}(\Omega)$, $\mathrm{Part}(\Omega)$ *or* $\mathrm{Bin}(\Omega)$, *and let T denote the cartesian product $\Pi_{i\in I}S$ where I is an index set. Then*

(i) *if Ω is countable, then $\mathrm{scf}(T) > \aleph_0$ and so T satisfies the semigroup Bergman property;*

(ii) *if $|I| \leq |\Omega|$, then $\mathrm{scf}(T) > \aleph_0$ and so T satisfies the semigroup Bergman property.*

Proof. **Part (i).** Let S_i be a semigroup of transformations or binary relations isomorphic to S acting on a set Ω_i. Then we may assume without loss of generality that $T = \Pi_{i\in I}S_i$. Then, as in the proof of Theorem 2.4.1, for all $i \in I$ there exist $f_i, g_i \in S_i$ such that $f_i\,\mathrm{Sym}(\Omega_i)g_i = S_i$.

Hence $(f_i)_{i\in I}\Pi_{i\in I}\operatorname{Sym}(\Omega_i)(g_i)_{i\in I} = T$ and so, by Theorem 2.3.1, $\operatorname{scf}(T) \geq \operatorname{scf}(\Pi_{i\in I}\operatorname{Sym}(\Omega_i))$. Finally, it was shown in [22, Lemma 3.5] that

$$\operatorname{scf}(\Pi_{i\in I}\operatorname{Sym}(\Omega_i)) > \aleph_0,$$

and so the proof is complete.

Part (ii). We will prove that $\operatorname{scf}(T) \geq \operatorname{scf}(S)$ by showing that T is Cayley bounded with respect to a finite set and a subsemigroup isomorphic to S. Let Ω_i with $|\Omega_i| = |\Omega|$, $i \in I$, partition Ω and let $f_i : \Omega \to \Omega_i$ be arbitrary bijections for all $i \in I$. If $g_i \in S$, then there exists $h_i : \Omega_i \to \Omega$ such that $g_i = f_i h_i$. So,

$$(g_i)_{i\in I} = (f_i h_i)_{i\in I} = (f_i)_{i\in I}(h)_{i\in I},$$

where $h \in S$ satisfies $(\alpha)h = (\alpha)h_i$ whenever $\alpha \in \Omega_i$. Thus T is the product of the fixed element $(f_i)_{i\in I}$ in T and the subsemigroup U consisting of all constant sequences of elements from S. That is, $T = (f_i)_{i\in I}U$. Hence, by Theorem 2.3.1, $\operatorname{scf}(T) \geq \operatorname{scf}(U)$. Now, $U \cong S$ and so $\operatorname{scf}(U) > \aleph_0$, as required. □

2.5 Negative Examples

In this section we apply the results of the previous sections to prove that various standard semigroups do not satisfy the semigroup Bergman property. If $f \in \operatorname{Self}(\Omega)$, then denote the image (or range) of f by $\operatorname{im}(f)$.

Theorem 2.5.1. *Let $\mathcal{BL}(\mathbb{N})$ denote the so-called Baer-Levi semigroup of injective mappings f in $\operatorname{Self}(\mathbb{N})$ such that $\mathbb{N}\setminus\operatorname{im}(f)$ is infinite. Then $\operatorname{cf}(\mathcal{BL}(\mathbb{N})) = \aleph_0$ and $\mathcal{BL}(\mathbb{N})$ does not satisfy the semigroup Bergman property.*

Proof. Let $S_n = \{\, f \in \mathcal{BL}(\mathbb{N}) \,:\, \{1, 2, \ldots, n\} \not\subseteq \operatorname{im}(f) \,\}$. Then $(S_n)_{n\in\mathbb{N}}$ forms a cofinal chain for $\mathcal{BL}(\mathbb{N})$ and so $\operatorname{cf}(\mathcal{BL}(\mathbb{N})) = \aleph_0$.

It remains to prove that $\mathcal{BL}(\mathbb{N})$ does not satisfy the semigroup Bergman property. We start by making a simple observation that will be used many times in the rest of the proof. Let Σ, Γ be infinite subsets of $\mathbb{N}$ where $\mathbb{N} \setminus \Gamma$ is infinite. Then any injection $f : \Sigma \to \Gamma$ can be extended to an element of $\mathcal{BL}(\mathbb{N})$.

We will give a generating set U for $\mathcal{BL}(\mathbb{N})$ such that $\mathcal{BL}(\mathbb{N})$ is not Cayley bounded with respect to U. Let $p_1, p_2, \ldots$ denote the prime numbers in ascending order. Then for every $n \in \mathbb{N}$ let $f_n \in \mathcal{BL}(\mathbb{N})$ such that

$$if_n = \begin{cases} i & i < n \text{ or } i = p_n^m \text{ for some } m > 1 \\ n & i = p_n. \end{cases}$$

Note that since $p_n \geq n+1$ for all n we may assume that $n+1 \notin \mathrm{im}(f_n)$. Define

$$U_n = \{\, f \in \mathcal{BL}(\mathbb{N}) \;:\; n \notin \mathrm{im}(f) \text{ and } if = i \text{ when } i < n \,\}.$$

Then set

$$U = \bigcup_{n \in \mathbb{N}} U_n \cup \{f_1, f_2, \ldots\}.$$

The semigroup $\mathcal{BL}(\mathbb{N})$ can be given as the union of the sets

$$V_n = \{\, f \in \mathcal{BL}(\mathbb{N}) \;:\; n \notin \mathrm{im}(f) \text{ and } \{1, 2, \ldots, n-1\} \subseteq \mathrm{im}(f) \,\},$$

where $V_1 = \{\, f \in \mathcal{BL}(\mathbb{N}) \;:\; 1 \notin \mathrm{im}(f) \,\}$.

We will prove that U is a generating set for $\mathcal{BL}(\mathbb{N})$ by showing that $V_n \subseteq U^{2n-1}$ for all n using induction. The base case when $n = 1$ follows from the fact that $V_1 = U_1 \subseteq U$. Assume that $n \geq 1$. Then the inductive hypothesis states that $V_n \subseteq U^{2n-1}$. Let $f \in V_{n+1}$ and let $\mathrm{im}(f) \setminus \{1, 2, \ldots, n\} = \{x_1, x_2, \ldots\}$. Then define $g : \mathbb{N} \to \mathbb{N}$ by

$$ig = \begin{cases} p_n^{j+1} & if = x_j \\ p_n & if = n \\ if & if < n \end{cases}$$

and let $h \in \mathcal{BL}(\mathbb{N})$ be any mapping satisfying $n+1 \notin \mathrm{im}(h)$ and

$$ih = \begin{cases} i & i < n+1 \\ x_j & i = p_n^{j+1} \end{cases}.$$

Then $g \in V_n$ and $h \in U_{n+1}$. Moreover, $gf_nh = f$ and so $f \in V_nU^2 \subseteq U^{2n+1}$. Hence $V_{n+1} \subseteq U^{2n+1}$ and U is a generating set for $\mathcal{BL}(\mathbb{N})$.

It remains to prove that $\mathcal{BL}(\mathbb{N})$ is not Cayley bounded with respect to U. Let $n \in \mathbb{N}$ and $g_n \in \mathcal{BL}(\mathbb{N})$ be any element satisfying $(2^k)g_n = k$ for all $k \leq n$. We will prove that if

$$g_n = u_1 u_2 \cdots u_m$$

where $u_1, u_2, \ldots, u_m \in U$ and m is the least length of such a product, then $m \geq n$. It suffices to prove that the elements $f_1, f_2, \ldots, f_n$ occur in the product $u_1 u_2 \cdots u_m$.

To start, let $F_{(1,2,\ldots,r)}$ denote the pointwise stabilizer of $\{1, 2, \ldots, r\}$ in $\mathcal{BL}(\mathbb{N})$. That is, $f \in F_{(1,2,\ldots,r)}$ implies that $if = i$ for all $1 \leq i \leq r$. Note that

$$U \setminus \left[\bigcup_{i=1}^{r} U_i \cup \{f_1, f_2, \ldots, f_r\} \right] \subseteq F_{(1,2,\ldots,r)}$$

and that U_r is a left ideal in $F_{(1,2,\ldots,r-1)}$ (U_1 is a left ideal in $F_{(\emptyset)} = \mathcal{BL}(\mathbb{N})$).

The mapping g_n is not an element of $F_{(1)}$ since $2g_n = 1$ and g_n is injective. Hence there exists $j \in \{1, 2, \ldots, m\}$ such that $u_j \in \{f_1\} \cup U_1$. Assume that i_1 is the largest such number j. Now, either $u_{i_1} \in U_1$ or $u_{i_1} = f_1$. In the former, since U_1 is a left ideal in $\mathcal{BL}(\mathbb{N})$, we have that $u_1 \cdots u_{i_1} \in U_1$ and so $i_1 = 1$ since m is the least length of product as defined above. It follows that $u_2, u_3, \ldots, u_m \in F_{(1)}$ and so $1 \notin \mathrm{im}(g_n)$, a contradiction. Thus $u_{i_1} = f_1$.

So, $2 \notin \mathrm{im}(u_1 \cdots u_{i_1})$ and $u_{i_1+1}, \ldots, u_m \in U \setminus [\{f_1\} \cup U_1] \subseteq F_{(1)}$. If $u_{i_1+1}, \ldots, u_m \in U \setminus [\{f_1, f_2\} \cup U_1 \cup U_2] \subseteq F_{(1,2)}$, then $2 \notin \mathrm{im}(g_n)$, a contradiction. Hence there exists $j \in \{i_1 + 1, i_1 + 2, \ldots, m\}$ such that $u_j \in \{f_2\} \cup U_2$. Assume that i_2 is the largest such j. As above, either $u_{i_2} \in U_2$ or $u_{i_2} = f_2$. In the former, since U_2 is a left ideal in $F_{(1)}$, as before, $u_{i_1+1} \cdots u_{i_2} \in U_2$ and so $i_2 = i_1 + 1$. Hence $u_{i_1+2}, \ldots, u_m \in F_{(1,2)}$ and so $2 \notin \mathrm{im}(g_n)$, a contradiction. Thus $u_{i_2} = f_2$.

Repeating this process n times we deduce that $f_1, f_2, \ldots, f_n$ occur in the product $u_1 u_2 \cdots u_m$, as required. □

Theorem 2.5.2. *Let Ω be an infinite set and let $S \in \{\mathrm{Self}(\Omega), \mathrm{Part}(\Omega), \mathrm{Bin}(\Omega)\}$. Then $\mathcal{P}(S)$ does not satisfy the semigroup Bergman property.*

Proof. We will prove the theorem in the case that $S = \mathrm{Self}(\Omega)$. Let U denote the set of all finite subsets of $\mathrm{Self}(\Omega)$ with at most 2 elements. It was shown in [27, Proposition 5.7.3 and Example 5.7.4] and [73] that the set U generates $\mathcal{P}(\mathrm{Self}(\Omega))$. However for completeness we include a short proof of this fact and show that $\mathcal{P}(\mathrm{Self}(\Omega))$ is not Cayley bounded with respect to U.

Let $\{f_1, f_2, \ldots, f_n\} \in \mathcal{P}(\mathrm{Self}(\Omega))$ be arbitrary. Then using induction we show that $\{f_1, f_2, \ldots, f_n\} \in \langle\, U \,\rangle$. If $n = 1$ or 2, then by definition $\{f_1, f_2, \ldots, f_n\} \in \langle\, U \,\rangle$. Otherwise, if $n > 2$, the inductive hypothesis states that every $n - 1$ element subset of $\mathrm{Self}(\Omega)$ lies in $\langle\, U \,\rangle$. Let $\Omega_1, \Omega_2, \ldots, \Omega_n$ be any disjoint subsets of Ω satisfying $|\Omega| = |\Omega_1| = |\Omega_2| = \cdots = |\Omega_n|$ and let $g_1 : \Omega \to \Omega_1, g_2 : \Omega \to \Omega_2, \ldots, g_n : \Omega \to \Omega_n$ be bijections. It suffices to prove that $\{g_1, g_2, \ldots, g_n\} \in \langle\, U \,\rangle$, since there exists $r \in \mathrm{Self}(\Omega)$ such that $\{g_1, g_2, \ldots, g_n\} \cdot \{r\} = \{f_1, f_2, \ldots, f_n\}$.

Let $\Sigma \subseteq \Omega$ be a moiety and let $f : \Omega \to \Sigma$ and $g : \Omega \to \Omega \setminus \Sigma$ be arbitrary bijections. Then there exist $\{h_1, h_2, \ldots, h_{n-1}\} \in \mathcal{P}(\mathrm{Self}(\Omega))$ such that $fh_i = g_i$ and $gh_i = g_{i+1}$ for all $1 \leq i \leq n - 1$. Thus

$$\{f, g\} \cdot \{h_1, h_2, \ldots, h_{n-1}\} = \{g_1, g_2, \ldots, g_n\}.$$

The proof is concluded by observing that any 2^n-element subset in $\mathcal{P}(\mathrm{Self}(\Omega))$ is the product of at least n subsets in U.

The proofs in the remaining two cases follow by analogous arguments. $\square$

The following theorem and its proof are analogues of [22, Theorem 3.6]; however the proof is somewhat more straightforward in the case presented here.

Theorem 2.5.3. *Let* $\mathrm{BSelf}(\mathbb{Q})$ *denote the subsemigroup of* $\mathrm{Self}(\mathbb{Q})$ *of elements* f *such that there exists* $k \in \mathbb{N}$ *such that* $|x - xf| \leq k$ *for all* $x \in \mathbb{Q}$*. Then* $\mathrm{cf}(\mathrm{BSelf}(\mathbb{Q})) > \aleph_0$ *and* $\mathrm{BSelf}(\mathbb{Q})$ *does not satisfy the semigroup Bergman property.*

Proof. Throughout the proof we will use the usual notation to denote rational intervals, i.e. $[a, b] = \{ c \in \mathbb{Q} \ : \ a \leq c \leq b \}$ and likewise for (a, b), $[a, b)$, and $(a, b]$. We begin by showing that $\mathrm{BSelf}(\mathbb{Q})$ does not satisfy the Bergman property.

Let U be the set of all elements f in $\mathrm{BSelf}(\mathbb{Q})$ such that $|x - xf| \leq 1$ for all $x \in \mathbb{Q}$. We will prove that U is a generating set for $\mathrm{BSelf}(\mathbb{Q})$.

With this aim in mind, let $f \in \mathrm{BSelf}(\mathbb{Q})$ such that $|x - xf| \leq k$ for some k. We will find $g, h \in \mathrm{BSelf}(\mathbb{Q})$ such that $f = gh$, $|x - xg| \leq (2/3)k$, and $|x - xh| \leq (2/3)k$. The image of f is infinite and countable and so we can enumerate the elements of $\mathrm{im}(f)$ as $x_1, x_2, \ldots$. Obviously, $x_m f^{-1} \cap x_n f^{-1} = \emptyset$ if $m \neq n$, and $x_n f^{-1} \subseteq [x_n - k, x_n + k]$.

Choose $y_1 \in [x_1 - (2/3)k, x_1 - (1/3)k]$, $z_1 \in [x_1 + (1/3)k, x_1 + (2/3)k]$ and for $n > 1$ choose

$$y_n \in [x_n - (2/3)k, x_n - (1/3)k] \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}$$

and

$$z_n \in [x_n + (1/3)k, x_n + (2/3)k] \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}.$$

Using the chosen elements y_n and z_n define a function $g : \mathbb{Q} \to \{y_1, z_1, y_2, z_2 \ldots\}$ by

$$xg = \begin{cases} y_n & x \in x_n f^{-1} \cap [x_n - k, x_n] \\ z_n & x \in x_n f^{-1} \cap [x_n, x_n + k]. \end{cases}$$

Define $h : \mathbb{Q} \to \mathbb{Q}$ by

$$xh = \begin{cases} x_n & x \in \{y_n, z_n\} \\ x & x \notin \{y_1, z_1, y_2, z_2 \ldots\}. \end{cases}$$

Hence we have shown that if $f \in \mathrm{BSelf}(\mathbb{Q})$ such that $|x - xf| \leq k$, then there exist $g, h \in \mathrm{BSelf}(\mathbb{Q})$ such that $f = gh$, $|x - xg| \leq (2/3)k$, and $|x - xh| \leq$

$(2/3)k$. We may repeat this process for g and h and subsequently their factors and their factors' factors and so on, until f is given as a product of elements of U. Therefore we have shown that the set U generates $\mathrm{BSelf}(\mathbb{Q})$. It is obvious that $\mathrm{BSelf}(\mathbb{Q})$ is not Cayley bounded with respect to U and so $\mathrm{BSelf}(\mathbb{Q})$ does not satisfy the semigroup Bergman property.

It remains to prove that $\mathrm{cf}(\mathrm{BSelf}(\mathbb{Q})) > \aleph_0$. Let

$$G = \{\, f \in \mathrm{BSelf}(\mathbb{Q}) \;:\; [4n, 4n+4)f \subseteq [4n, 4n+4) \text{ for all } n \in \mathbb{Z} \,\}$$

and

$$H = \{\, f \in \mathrm{BSelf}(\mathbb{Q}) \;:\; [4n+2, 4n+6)f \subseteq [4n+2, 4n+6) \text{ for all } n \in \mathbb{Z} \,\}.$$

It is straightforward to verify that

$$G \cong H \cong \prod_{i \in \mathbb{Z}} \mathrm{Self}([0,4)).$$

We will now prove that $U \subseteq GH$. Let $f \in U$ and $\mathrm{im}(f) = \{x_1, x_2, \ldots\}$. The proof follows a similar argument to that used to show that $\langle\, U \,\rangle = \mathrm{BSelf}(\mathbb{Q})$. Let $n \geq 1$. We will define elements $y_n, z_n \in \mathbb{Q}$, $n \in \mathbb{N}$, and functions

$$g_n : \{x_1, x_2, \ldots, x_n\}f^{-1} \to \{y_1, z_1, y_2, z_2, \ldots, y_n, z_n\}$$

that depend on x_n and extend g_{n-1} and h_{n-1}. There are three cases to consider.

If $x_n \in [4k, 4k+1)$, then $x_n f^{-1} \subseteq [4k-1, 4k+2)$ since $f \in U$. Elements of G take $[4k, 4k+2)$ to $[4k, 4k+4)$ and $[4k-1, 4k)$ to $[4k-4, 4k)$. Hence choose

$$y_n \in [4k, 4k+2) \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}$$

and

$$z_n \in [4k-1, 4k) \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}.$$

Define g_n by

$$xg_n = \begin{cases} xg_{n-1} & x \notin x_n f^{-1} \\ y_n & x \in x_n f^{-1} \cap [4k, 4k+2) \\ z_n & x \in x_n f^{-1} \cap [4k-1, 4k). \end{cases}$$

If $x_n \in [4k+i, 4k+i+1)$ where $i = 1$ or 2, then choose

$$y_n, z_n \in [4k+i, 4k+i+1) \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}$$

and define g_n by

$$xg_n = \begin{cases} xg_{n-1} & x \notin x_n f^{-1} \\ y_n & x \in x_n f^{-1}. \end{cases}$$

If $x_n \in [4k+3, 4k+4)$, then $x_n f^{-1} \subseteq [4k+2, 4k+5)$. Choose

$$y_n \in [4k+4, 4k+5) \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}$$

and

$$z_n \in [4k+2, 4k+4) \setminus \{y_1, z_1, y_2, z_2, \ldots, y_{n-1}, z_{n-1}\}.$$

Define g_n by

$$xg_n = \begin{cases} xg_{n-1} & x \notin x_n f^{-1} \\ y_n & x \in x_n f^{-1} \cap [4k+4, 4k+5) \\ z_n & x \in x_n f^{-1} \cap [4k+2, 4k+4). \end{cases}$$

Finally, define

$$h_n : \{y_1, z_1, y_2, z_2, \ldots, y_n, z_n\} \to \{x_1, x_2, \ldots, x_n\}$$

by

$$xh_n = x_n \text{ if } x \in \{y_n, z_n\}.$$

Repeating the previous procedure *ad infinitum* produces two functions $g : \mathbb{Q} \to \{y_1, z_1, y_2, z_2, \ldots\} \in G$ and $h : \mathbb{Q} \to \mathbb{Q} \in H$ where $f = gh$, as required.

If $(S_n)_{n\in\mathbb{N}}$ is a cofinal chain for $\mathrm{BSelf}(\mathbb{Q})$, then $(S_n \cap G)_{n\in\mathbb{N}}$ is a chain of subsemigroups whose union is G. We showed in Theorem 2.4.10 that $\mathrm{cf}(\prod_{i\in\mathbb{Z}} \mathrm{Self}([0,4))) > \aleph_0$. Thus there exists $M \in \mathbb{N}$ such that $G \subseteq S_M$. Likewise, there exists N such that $H \subseteq S_N$. Assume without loss of generality that $N > M$. We proved in the previous paragraph that $U \subseteq G.H \subseteq S_N$. But then $\mathrm{BSelf}(\mathbb{Q}) = \langle\, U \,\rangle = S_N$, a contradiction. Hence $\mathrm{cf}(\mathrm{BSelf}(\mathbb{Q})) > \aleph_0$ and the proof is complete. □

We stated in Section 2.3 that it is possible to find a non-finitely generated semigroup S with subsemigroup T and finite set F such that $S = (T \cup F)^2$, $\mathrm{cf}(S) > \mathrm{cf}(T)$, $\mathrm{scf}(S) > \mathrm{scf}(T)$, and S satisfies the semigroup Bergman property but T does not. Using Theorems 2.4.1 and 2.5.1 we can now state this example explicitly.

Example 2.5.4. Let $S = \mathrm{SymInv}(\mathbb{N})$ and T be the Baer-Levi semigroup $\mathcal{BL}(\mathbb{N})$. Obviously $T \leq S$. It is easy to verify that for any bijection f from a

moiety X in $\mathbb{N}$ to $\mathbb{N}$ we have $Tf = S$. Thus if $F = \{f\}$, then $(T \cup F)^2 = S$. Moreover, we showed in Theorems 2.4.1 and 2.5.1 that

$$\mathrm{cf}(S) \geq \mathrm{scf}(S) > \aleph_0 = \mathrm{cf}(T) \geq \mathrm{scf}(T),$$

and so S satisfies the semigroup Bergman property and T does not, as required.

The following example shows that it is not true that if $T \leq S$, T satisfies the semigroup Bergman property and $(T \cup F)^2 = S$, then S satisfies the semigroup Bergman property.

Example 2.5.5. Let Ω be an infinite set, $S = \mathcal{P}(\mathrm{Part}(\Omega))$, and $T = \mathcal{P}(\mathrm{SymInv}(\Omega))$. Then partition Ω into moieties Ω_α indexed by $\alpha \in \Omega$ and let $f \in \mathrm{Part}(\Omega)$ be the unique function satisfying $(\Omega_\alpha)f = \alpha$. Then it is straightforward to verify that $\mathrm{SymInv}(\Omega).f = \mathrm{Part}(\Omega)$ and so $T.f = S$. However, in Theorems 2.4.6 and 2.5.2 we showed that $T = \mathcal{P}(\mathrm{SymInv}(\Omega))$ does satisfy the semigroup Bergman property but $S = \mathcal{P}(\mathrm{Part}(\Omega))$ does not.

Recall that Lemma 2.3.5(ii) states that if S is a semigroup, I an ideal of S, and I and S/I satisfy the semigroup Bergman property, then S does also. The next example shows that there exists a semigroup satisfying the semigroup Bergman property that contains an ideal that does not satisfy it. Thus proving that the converse of Lemma 2.3.5(ii) does not hold.

Example 2.5.6. The union S of $\mathrm{Sym}(\mathbb{N})$ and $\mathcal{BL}(\mathbb{N})$ forms a subsemigroup of $\mathrm{Self}(\mathbb{N})$ and $I = \mathcal{BL}(\mathbb{N})$ is an ideal in S. In fact, for all $f \in I$ we have that $f.\mathrm{Sym}(\mathbb{N}) = I$. Thus if $(S_n)_{n\in\mathbb{N}}$ is a strong cofinal chain for S, then since $\mathrm{scf}(\mathrm{Sym}(\mathbb{N})) > \aleph_0$ there exists $M \in \mathbb{N}$ such that $\mathrm{Sym}(\mathbb{N}) \subseteq S_M$. But then there exists $f \in S_{M+1} \cap I$, and so $S \subseteq S_N$ for some N, a contradiction. Therefore $\mathrm{scf}(S) > \aleph_0$ and S has the semigroup Bergman property but by Theorem 2.5.1, I does not have the semigroup Bergman property.

The following examples have uncountable cofinality but do not satisfy the semigroup Bergman property.

Example 2.5.7. Let X be an infinite set and let S be the semi-direct product $X^* \rtimes \mathrm{Self}(X)$ where $\mathrm{Self}(X)$ acts on free semigroup X^* (with empty word 1) by extending every mapping from X to X to an endomorphism of X^*. We will prove that $\mathrm{cf}(S) > \aleph_0$. Assume otherwise. Then there exists a cofinal chain $(S_n)_{n\in\mathbb{N}}$. Since $\{1\} \times \mathrm{Self}(X) \cong \mathrm{Self}(X)$ it follows that $\mathrm{cf}(\{1\} \times \mathrm{Self}(X)) > \aleph_0$. Hence we deduce that there exists $N \in \mathbb{N}$ such that $\{1\} \times$

$\mathrm{Self}(X) \subseteq S_N$. Without loss of generality there exists $(x, 1_X) \in S_N$ for some $x \in X$. If $y \in X \setminus \{x\}$ and σ the transposition that swaps x and y, then

$$(y, 1_X) = (1, \sigma)(x, 1_X)(1, \sigma) \in S_N.$$

Thus $X^* \times \{1_X\} \subseteq S_N$ and so $S \subseteq S_N$, a contradiction.

It remains to prove that S does not satisfy the semigroup Bergman property. The set $U = \{ (x, \tau) \ : \ x \in X \cup \{1\}, \tau \in \mathrm{Self}(X) \}$ generates S and S is not Cayley bounded with respect to U.

Chapter 3

Cayley Automaton Semigroups

In this chapter we characterize when a Cayley automaton semigroup is finite, is free, is a left zero semigroup, is a right zero semigroup, is a group, or is trivial. We also introduce dual Cayley automaton semigroups and discuss when they are finite.

The results of this chapter appeared in [58].

3.1 Introduction and Main Results

In the 1960s, Krohn and Rhodes proposed a construction called the *Cayley machine* of a finite semigroup [6]. The construction is as follows: Let S be a finite semigroup. Consider the right Cayley graph of S with respect to the generating set S. Turn it into a transducer automaton $\mathcal{C}(S)$ by letting the output symbol on the arc leading from s and labeled by t to be st:

$$\mathrm{s} \xrightarrow{\mathrm{t} \mid \mathrm{st}} \mathrm{st}$$

So, the states and letters of $\mathcal{C}(S)$ are elements of S and when the state s reads the letter t, it moves to the state st and outputs the letter st. Hence every state from $\mathcal{C}(S)$ can be viewed as a transformation on the set of all infinite sequences S^∞.

To put our setting formally, let us explain how the automaton $\mathcal{C}(S)$ works. Let $S = \{s_1, \ldots, s_n\}$ be the list of elements of our finite semigroup S. In order to avoid confusion, we will denote the states in $\mathcal{C}(S)$ by an overline: s is a symbol, and $\overline{s}$ is a state. The elements from S^∞ are simply the sequences $\alpha_1\alpha_2\cdots$, where $\alpha_i \in S$ for all $i \geq 1$. Then, for $s \in S$, the state $\overline{s}$ acts on $\alpha_1\alpha_2\cdots$ as follows: $\overline{s}$ acts on α_1, changes it state to $\overline{s\alpha_1}$ and then the new state acts on the sequence $\alpha_2\alpha_3\cdots$:

$$(\alpha_1\alpha_2\cdots)^{\overline{s}} = (s\alpha_1)(\alpha_2\alpha_3\cdots)^{\overline{s\alpha_1}}.$$

(Note that we act by $\overline{s}$ on the *right*.) Now one can recursively define what does it mean for the state $\overline{s}$ to act on $\alpha_1\alpha_2\cdots$, and the result of such an action is a sequence from S^∞. Thus, $\overline{s}$ can be viewed as the corresponding mapping from S^∞ to S^∞. Now, let $\mathbf{C}(S)$ be the semigroup generated by all the mappings from S^∞ to S^∞ corresponding to the states $\overline{s}$ for all $s \in S$. This is what is known as the *automaton semigroup* generated by the automaton $\mathcal{C}(S)$, see [67] for more details. We will name the semigroups $\mathbf{C}(S)$ by *Cayley automaton semigroups*.

Let us explain now a convenient way to realise what are $\mathbf{C}(S)$.

First of all, consider the rooted $|S|$-ary tree. We will call this tree by S-tree. Label the nodes of the first level of tree by $s_1, \ldots, s_n$ (in arbitrary order). The nodes from the second level, which are the children of s_i, are labelled by $s_is_1, \ldots, s_is_n$. Continuing in this manner, we assign to each node of the S-tree a label which is simply a finite sequence of elements from S. We fix these labels once and forever. Then the sequences from S^∞ can be viewed as the corresponding paths in the S-tree which start from the root and follow the edges according to the consecutive symbols from the sequences.

In this way, for every $s \in S$, the mapping from S^∞ to S^∞ associated to the state $\overline{s}$, is in effect a corresponding endomorphism of the S-tree.

The semigroup of endomorphisms of the S-tree is the infinite wreath product of the semigroups $\mathcal{T}_S$ (where $\mathcal{T}_S$ is the semigroup of all mappings from S to S). This enables us to think about $\overline{s}$ in terms of what is known as the *wreath recursion*. So, first of all we view $\overline{s}$ as the corresponding endomorphism of the S-tree. This endomorphism acts on the first level of the S-tree by the function $\lambda_s : S \to S$ defined by $x \mapsto sx$. Let $s_i \in S$. Consider the restriction of the endomorphism $\overline{s}$ to the node s_i. This restriction is an endomorphism of the regular $|S|$-ary rooted tree with the root s_i. The latter $|S|$-ary rooted tree is canonically isomorphic to the S-tree. Thus we may view the restriction of $\overline{s}$ to the rooted tree starting from the node s_i as the corresponding endomorphism of the S-tree. To summarise, $\overline{s}$ may be viewed as the endomorphism of the S-tree constructed as follows: we first put the corresponding endomorphisms to the nodes labelled by s_i for all $i \leq n$ and then 'shuffle' the first level by the mapping λ_s. This means that we may define $\overline{s}$ in a recursive way.

To express in short what we have said in the previous paragraph, we will write the following:

$$\overline{s} = \lambda_s(\overline{ss_1}, \ldots, \overline{ss_n}).$$

Here λ_s stands for the function which corresponds to the action of $\overline{s}$ on the first level of the S-tree, and $\overline{ss_i}$ is the endomorphism of the S-tree,

which corresponds to the restriction of the endomorphism $\overline{s}$ to the rooted tree with the root s_i. Note that, by definition of $\mathcal{C}(S)$, this restriction of $\overline{s}$ indeed corresponds to $\overline{ss_i}$ since upon reading the symbol s_i, the state $\overline{s}$ moves to the state $\overline{ss_i}$.

Furthermore, as we said above, we will deal with *right* actions in this chapter. So, $(x)\lambda_s\lambda_t = (x\lambda_s)\lambda_t = (sx)\lambda_t = tsx$ for all $x \in S$. This means that $\lambda_s\lambda_t = \lambda_{ts}$ for all $s, t \in S$.

Now let us understand how to calculate the product of endomorphisms $\overline{s}$ and $\overline{t}$ for $s, t \in S$. First of all, the composition of functions on the first level goes like this: first we apply λ_s and then apply λ_t, so that the endomorphism $\overline{s} \cdot \overline{t}$ acts on the first level of the S-tree by the function $\lambda_s\lambda_t = \lambda_{ts}$. Next, we need to calculate what is the restriction of the endomorphism $\overline{s} \cdot \overline{t}$ to the node s_i. First we must apply $\overline{ss_i}$ – just the restriction from the first endomorphism (our first endomorphism is $\overline{s}$) and then multiply it by the restriction of $\overline{t}$ to that node, which corresponds to point obtained by mapping s_i by λ_s. Thus this node is ss_i, and the corresponding restriction is associated to $\overline{tss_i}$. Thus, following our above notation, we may write

$$\overline{s} \cdot \overline{t} = \lambda_{ts}(\overline{ss_1} \cdot \overline{tss_1}, \ldots, \overline{ss_n} \cdot \overline{tss_n}).$$

Let $a_1, \ldots, a_k \in S$ and $x \in S$. We will denote by $\tau(\overline{a_1} \cdots \overline{a_k})$ the transformation on the set S, corresponding to the action of $\overline{a_1} \cdots \overline{a_k}$ on the first level of the S-tree. As above, we have that

$$\tau(\overline{a_1} \cdots \overline{a_k}) = \lambda_{a_k \cdots a_1}.$$

The endomorphism, associated to the restriction of $\overline{a_1} \cdots \overline{a_k}$ to the node x will be denoted by $q(\overline{a_1} \cdots \overline{a_k}, x)$. As above, one calculates that

$$q(\overline{a_1} \cdots \overline{a_k}, x) = \overline{a_1 x} \cdot \overline{a_2 a_1 x} \cdots \overline{a_k \cdots a_1 x}.$$

For more details about general automaton semigroups see the work of Alan Cain [11].

Let us now shortly overview what has been known about the Cayley automaton semigroups.

In [35] Grigorchuk and Żuk prove that $\mathbf{C}(\mathbb{Z}_2)$ is a free semigroup of rank 2. Generalizing this result, Silva & Steinberg prove in [80] the following

Theorem 3.1.1. *Let G be a finite non-trivial group. Then $\mathbf{C}(G)$ is a free semigroup of rank $|G|$.*

Under a different perspective, Cayley automaton semigroups appeared in a work by Mintz [64]. One of the main results he proves is

Theorem 3.1.2. *Let S be a finite semigroup. Then $\mathbf{C}(S)$ is finite if and only if S is $\mathcal{H}$-trivial, i.e. that $\mathcal{H}$ is the identity relation.*

In this chapter we present an alternative proof of Theorem 3.1.2, using the machinery of the wreath recursions. There is one more way of proving this theorem, using the action of states of $\mathcal{C}(S)$ on the words from S^∞, see a work of Cain [11]. The proof of Theorem 3.1.2 is contained in Section 3.3.

Making use of Theorem 3.1.2, in Sections 3.4 and 3.5 we will prove the following three propositions:

Proposition 3.1.3. *Let S be a finite semigroup. Then $\mathbf{C}(S)$ is a free semigroup if and only if the minimal ideal K of S consists of a single $\mathcal{R}$-class, in which every $\mathcal{H}$-class is not a singleton, and there exists $k \in K$ such that $st = skt$ for all $s, t \in S$.*

Proposition 3.1.4. *Let S be a finite semigroup. Then $\mathbf{C}(S)$ is a right zero semigroup if and only if $abc = ac$ for all $a, b, c \in S$.*

Proposition 3.1.5. *Let S be a finite semigroup. Then $\mathbf{C}(S)$ is a left zero semigroup if and only if S^2 is the minimal ideal of S and if this ideal forms a right zero semigroup.*

Continuing the study of automaton semigroups, in Section 3.6 we find a characterization of when $\mathbf{C}(S)$ is a group:

Theorem 3.1.6. *For a finite semigroup S, the following statements are equivalent:*

1. *$\mathbf{C}(S)$ is a group.*
2. *$\mathbf{C}(S)$ is trivial.*
3. *S is an inflation of a right zero semigroup by null semigroups.*

Recall that a semigroup S is an inflation of a right zero semigroup T by null semigroups if $T \leq S$ and S can be partitioned into disjoint subsets S_t (for each $t \in T$) such that $t \in S_t$ and $S_u S_t = \{t\}$ for all $t, u \in T$.

After proving this, in Section 3.7 we will discuss these results and their corollaries.

In the final Section 3.8 we introduce the *dual Cayley machine* of a finite semigroup and prove a theorem, analogous to Theorem 3.1.2. In a way, it will show that when turning a Cayley graph of a finite semigroup to an automaton, the most natural construction which appears is the Cayley machine.

Before we start proving our main results we need some preparation.

3.2 Auxiliary Lemmas

Throughout this chapter we will use the following. Let $\alpha, \beta \in \mathbf{C}(S)$. Then $\alpha = \beta$ if and only if $\tau(\alpha) = \tau(\beta)$ and $q(\alpha, x) = q(\beta, x)$ for all $x \in S$. This follows immediately when realizing α and β as endomorphisms of the S-tree.

Lemma 3.2.1. *Let S be a finite semigroup. Then for all $s, t \in S$, $\overline{s} = \overline{t}$ in $\mathbf{C}(S)$ if and only if $\lambda_s = \lambda_t$.*

Proof. Let $s, t \in S$. Then $\overline{s} = \overline{t}$ if and only if $\lambda_s = \lambda_t$ and $\overline{sx} = \overline{tx}$ for all $x \in S$. Furthermore, $\overline{sx} = \overline{tx}$ if and only if $\lambda_{sx} = \lambda_{tx}$ and $\overline{sxy} = \overline{txy}$ for all $y \in S$. Using the above recursive formula for $\overline{s}$, we obtain that $\overline{s} = \overline{t}$ if and only if $\lambda_s = \lambda_t$ and $\lambda_{sx} = \lambda_{tx}$ for all $x \in S$. It remains to notice that $\lambda_s = \lambda_t$ implies $\lambda_{sx} = \lambda_{tx}$ for all $x \in S$. □

Later we will need Cayley automaton semigroups of special types semigroup:

Lemma 3.2.2. *Let L be a finite left zero semigroup. Then $\mathbf{C}(L)$ is a right zero semigroup with $|L|$ elements.*

Proof. Suppose $\mathcal{C}(L)$ is in state $\overline{s}$ and reads symbol t. Then, by the definition of $\mathcal{C}(L)$, it outputs s and moves to the same state $\overline{s}$. Thus $\alpha \cdot \overline{s} = s^\infty$ for all $\alpha \in L^\infty$. Hence for any $s, t \in L$ and $\alpha \in L^\infty$:

$$\alpha \cdot (\overline{s} \cdot \overline{t}) = s^\infty \cdot \overline{t} = t^\infty = \alpha \cdot \overline{t},$$

and so $\overline{s} \cdot \overline{t} = \overline{t}$. It remains to note that, by Lemma 3.2.1, if $s \neq t$, then $\overline{s} \neq \overline{t}$. □

Lemma 3.2.3. *Let S be a finite semigroup and let R be a finite right zero semigroup. Then $\mathbf{C}(S \times R) \cong \mathbf{C}(S)$.*

Proof. Let $s \in S$ and $r, t \in R$. Then it follows from Lemma 3.2.1 that $\overline{(s, r)} = \overline{(s, t)}$ in $\mathbf{C}(S \times R)$. Hence $\mathbf{C}(S \times R)$ coincides with $T = \langle \overline{(s, r_0)} : s \in S \rangle$ for any fixed $r_0 \in R$. It is now easy to check that $\overline{(s, r_0)} \mapsto \overline{s}$ gives rise to an isomorphism from T onto $\mathbf{C}(S)$. □

Corollary 3.2.4. *Let R be a finite right zero semigroup. Then $\mathbf{C}(R)$ is trivial.*

We finish this section with the following three technical lemmas about finite semigroups. The first one follows immediately from [70, Corollary 2.6, p. 446] and [18, Theorem 2.17]:

Lemma 3.2.5. *Let S be a finite semigroup and let $a, b \in S$ belong to the same $\mathcal{D}$-class D of S. Then*

1. *If $ab \in D$ then $ab \in R_a \cap L_b$.*
2. *$ab \in R_a \cap L_b$ if and only if $L_a \cap R_b$ contains an idempotent.*

Lemma 3.2.6. *Let S be a finite $\mathcal{H}$-trivial semigroup. Denote by I all the elements from S which do not belong to any of the maximal $\mathcal{D}$-classes of S. Then*

1. *I is an ideal in S.*
2. *If $I = \varnothing$, then S is a rectangular band.*
3. *If $a_1 \cdots a_k \in S \setminus I$, then all $a_1, \ldots, a_k$ belong to the maximal $\mathcal{D}$-class $D_{a_1 \cdots a_k}$.*
4. *If $x, y \in S$ are such that x and yx do not belong to the same maximal $\mathcal{D}$-class of S, then $yx \in I$. Analogously, if x and xy do not belong to the same maximal $\mathcal{D}$-class of S, then $xy \in I$.*
5. *If $a_1, \ldots, a_m, x \in S$ are such that $a_m \cdots a_1$ and $a_m \cdots a_1 x$ belong to the same maximal $\mathcal{D}$-class, then $a_1 x \mathcal{L} a_2 a_1 x \mathcal{L} \cdots \mathcal{L} a_m \cdots a_1 x$ and $a_1 x \in S \setminus I$.*

Proof. (1). Take arbitrary $i \in I$ and $s \in S$. We will show that $is \in I$. By symmetry it will follow then that $si \in I$ and we will be done. So, assume that $is \notin I$. This means that is lies in some maximal $\mathcal{D}$-class of S. Since $i \geq_{\mathcal{D}} is$, it follows that $i \mathcal{D} is$ and so i lies in a maximal $\mathcal{D}$-class, a contradiction.

(2). Assume that $I = \varnothing$. We will prove that S has only one $\mathcal{D}$-class. Assume the converse, i.e. that one can find two distinct $\mathcal{D}$-classes D_1 and D_2. Since I is empty, both D_1 and D_2 must be maximal. Take $x \in D_1$ and $y \in D_2$. Then $xy \leq_{\mathcal{D}} x$ and $xy \leq_{\mathcal{D}} y$. But $I = \varnothing$ and so every element of S lies in a maximal $\mathcal{D}$-class. In particular, xy lies in some maximal $\mathcal{D}$-class. Thus, by maximality of D_{xy}, actually $xy \mathcal{D} x$ and $xy \mathcal{D} y$. This yields $x \mathcal{D} y$, a contradiction.

Thus, S indeed has only one $\mathcal{D}$-class and so is simple. Since it is $\mathcal{H}$-trivial, from Rees–Suschkewitch Theorem it is now immediate that S is a rectangular band.

(3). Let $a_1 \cdots a_k \in S \setminus I$. Then $D_{a_1 \cdots a_k}$ is a maximal $\mathcal{D}$-class in S. But $D_{a_1 \cdots a_k} \leq D_{a_i}$ for all $i \leq k$. Thus $D_{a_1 \cdots a_k} = D_{a_i}$ for all $i \leq k$. Hence all $a_1, \ldots, a_k$ belong to the maximal $\mathcal{D}$-class $D_{a_1 \cdots a_k}$.

(4). We will prove only the first claim, and we do it by its contrapositive. So, assume that $yx \in S \setminus I$. By (3) it follows that x and y belong to the

same maximal $\mathcal{D}$-class D_{yx}. Hence x and yx belong to the same maximal $\mathcal{D}$-class.

(5). Let $a_m \cdots a_1$ and $a_m \cdots a_1 x$ belong to the same maximal $\mathcal{D}$-class. Then $a_m \cdots a_1 x \in S \setminus I$ and by (4) we have that $a_m \cdots a_1$ and x are from the same maximal $\mathcal{D}$-class. This implies that $a_1, a_2, \ldots, a_m$ and $a_m \cdots a_1, \ldots, a_1$ are all from D_x. Then by Lemma 3.2.5, $a_1 \mathcal{L} a_2 a_1 \mathcal{L} \cdots \mathcal{L} a_m \cdots a_1$. Since $\mathcal{L}$ is a right congruence, we obtain $a_1 x \mathcal{L} a_2 a_1 x \mathcal{L} \cdots \mathcal{L} a_m \cdots a_1 x$. Finally, since $a_m \cdots a_1 x \in S \setminus I$, we have $a_1 x \in S \setminus I$. □

Lemma 3.2.7. *Let S be a finite semigroup in which $\mathcal{H}$ is non-trivial. Then S contains a non-trivial subgroup.*

Proof. Let H be a non-trivial $\mathcal{H}$-class in S. Then the stabiliser $\mathrm{Stab}(H) = \{s \in S : Hs = H\}$ forms a subsemigroup in S. Moreover, there is a congruence ρ on $\mathrm{Stab}(H)$ such that $\mathrm{Stab}(H)/\rho$ is the so-called *Schuetzenberger group* $\Gamma(H)$ of the $\mathcal{H}$-class H, see [18]. Moreover, $|\Gamma(H)| = |H|$, see [18]. So, there exists a homomorphism ϕ from $\mathrm{Stab}(H)$ onto a non-trivial group.

Assume that $\mathrm{Stab}(H)$ does not contain non-trivial subgroups. Let I be the minimal ideal in $\mathrm{Stab}(H)$. Then I is a Rees matrix semigroup over the trivial group, and so I is isomorphic to a rectangular band. Since every element $e \in I$ is an idempotent, we must have that $\phi(e)$ is the identity $1_{\Gamma(H)}$ of $\Gamma(H)$. For every $s \in \mathrm{Stab}(H)$ and $e \in I$ there exists $f \in I$ such that $se = f$ and so

$$1_{\Gamma(H)} = \phi(f) = \phi(s)\phi(e) = \phi(s) \cdot 1_{\Gamma(H)} = \phi(s).$$

Thus $\mathrm{Stab}(H)$ is mapped by ϕ to $\{1_{\Gamma(H)}\}$, a contradiction. Hence $\mathrm{Stab}(H)$ contains non-trivial subgroups and so does S. □

3.3 Proof of Theorem 3.1.2

Proof of Theorem 3.1.2. ($\Rightarrow$). Suppose that $\mathbf{C}(S)$ is finite. Assume with the aim of getting a contradiction that S is not $\mathcal{H}$-trivial. By Lemma 3.2.7, S contains a non-trivial subgroup G.

Now, take $g \in G$. Then $\overline{g}$ is an endomorphism of the S-tree. There is a $|G|$-ary rooted subtree in the S-tree corresponding to the nodes labelled only by the elements from G. The restriction of $\overline{g}$ to this G-subtree coincides with the endomorphism of the G-subtree corresponding to the element $\overline{g}$ from $\mathcal{C}(G)$, the Cayley automaton over the group G. By Theorem 3.1.1, these restrictions for all $g \in G$, generate a free semigroup of rank $|G|$. Therefore, $\langle \overline{g} : g \in G \rangle$ is a free semigroup of rank $|G|$, a contradiction. Thus S is $\mathcal{H}$-trivial.

($\Leftarrow$). We will prove by induction on $|S|$ that if S is $\mathcal{H}$-trivial then $\mathbf{C}(S)$ is finite. The base case $|S| = 1$ is obvious. So, assume that S is a finite $\mathcal{H}$-trivial semigroup and for all $\mathcal{H}$-trivial semigroups T with size $< |S|$ we have that $\mathbf{C}(T)$ is finite.

Let I comprise all the elements from S which do not belong to any of the maximal $\mathcal{D}$-classes of S. By Lemma 3.2.6, I is an ideal. If $I = \varnothing$, then by Lemma 3.2.6, S is a rectangular band, i.e. the direct product of left zero semigroup with right zero semigroup. Then by Lemma 3.2.3, $\mathbf{C}(S)$ is isomorphic to a Cayley automaton semigroup over a finite left zero semigroup. Lemma 3.2.2 tells us then that $\mathbf{C}(S)$ is a finite right zero semigroup. So in the remainder of the proof we may assume that $I \neq \varnothing$. Hence by inductive hypothesis, $\mathbf{C}(I)$ is finite.

For $X \subseteq S$ define $\overline{X} = \{\overline{x} : x \in X\}$.

Let us examine what is the situation we are working with. The following five lemmas will show us how we can reduce the problem of proving that $\mathbf{C}(S)$ is finite to another problem.

Lemma 3.3.1. *$\overline{I}\langle\overline{S}\rangle^1 = \overline{I} \cup \overline{I}\langle\overline{S}\rangle$ is finite.*

Proof. First of all let us prove that $\langle\overline{I}\rangle$ is finite. To do this, it suffices to prove that there are finitely many products $\overline{i} \cdot \overline{i_1} \cdots \overline{i_k} \in \langle\overline{I}\rangle$ for any fixed $i \in I$. We have that $\overline{i} \cdot \overline{i_1} \cdots \overline{i_k}$ and $\overline{i} \cdot \overline{j_1} \cdots \overline{j_n}$ are equal if and only if the restrictions of $\overline{i_1} \cdots \overline{i_k}$ and $\overline{j_1} \cdots \overline{j_n}$ on $S^\infty\overline{i}$ coincide. Notice that $S^\infty\overline{i} \subseteq I^\infty$. Obviously $\overline{i_1} \cdots \overline{i_k}$ and $\overline{j_1} \cdots \overline{j_n}$ act on I^∞ in the same way as the corresponding products from $\mathbf{C}(I)$ do. Hence the set $\{\overline{i_1} \cdots \overline{i_k} \restriction_{S^\infty\overline{i}} : i_1, \ldots, i_k \in I\}$ has at most $|\mathbf{C}(I)|$ elements and so is finite. Thus there are finitely many products $\overline{i} \cdot \overline{i_1} \cdots \overline{i_k} \in \langle\overline{I}\rangle$. Hence $\langle\overline{I}\rangle$ is finite.

Now, take a typical element $p = \overline{i} \cdot \overline{a_1} \cdots \overline{a_k} \in \overline{I}\langle\overline{S}\rangle$. Then for all $x \in S$, we have

$$q(\overline{i} \cdot \overline{a_1} \cdots \overline{a_k}, x) = \overline{ix} \cdot \overline{a_1 ix} \cdots \overline{a_k \cdots a_1 ix} \in \langle\overline{I}\rangle$$

and $\tau(p) = \lambda_{a_k \cdots a_1 i}$ with $a_k \cdots a_1 i \in I$. So, there are at most $|I|$ possible actions of p on the first level of the S-tree and the action of p on any subtree, corresponding to a node from the first level, is by some element from $\langle\overline{I}\rangle$. Hence $|\overline{I}\langle\overline{S}\rangle| \leq |I| \cdot |\langle\overline{I}\rangle|^{|S|}$. The lemma is proved. $\square$

Lemma 3.3.2. *If $\langle\overline{S} \setminus \overline{I}\rangle$ is finite, then $\langle\overline{S}\rangle$ is finite.*

Proof. Follows from $\langle\overline{S}\rangle = \overline{I}\langle\overline{S}\rangle^1 \cup \langle\overline{S} \setminus \overline{I}\rangle \cup \langle\overline{S} \setminus \overline{I}\rangle\overline{I}\langle\overline{S}\rangle^1$ and Lemma 3.3.1. $\square$

Lemma 3.3.3. *If the set $P_0 = \{\overline{a_1 x} \cdot \overline{a_2 a_1 x} \cdots \overline{a_k \cdots a_1 x} : a_1, \ldots, a_k \in S \setminus I,\ x \in S\}$ is finite, then $\langle\overline{S} \setminus \overline{I}\rangle$ is finite.*

Proof. Take a typical product $\overline{a_1}\cdots\overline{a_k} \in \langle \overline{S}\setminus\overline{I}\rangle$ with $a_1,\ldots,a_k \in S\setminus I$. Then

$$q_x = q(\overline{a_1}\cdots\overline{a_k}, x) = \overline{a_1x}\cdot\overline{a_2a_1x}\cdots\overline{a_k\cdots a_1x}$$

for all $x \in S$. Now, all the elements q_x together with $\tau(\overline{a_1}\cdots\overline{a_k})$ define $\overline{a_1}\cdots\overline{a_k}$ uniquely. Hence the claim. □

Lemma 3.3.4. *If the set $P_1 = \{\overline{a_1}\cdots\overline{a_n} : a_1\mathcal{L}a_2\mathcal{L}\cdots\mathcal{L}a_n,\ a_1 \in S\setminus I\}$ is finite, then P_0 is finite.*

Proof. Take an element $p_0 = \overline{a_1x}\cdot\overline{a_2a_1x}\cdots\overline{a_k\cdots a_1x} \in P_0$ with $a_1,\ldots,a_k \in S\setminus I$ and $x \in S$. Let m be the maximal number such that $a_m\cdots a_1x \in S\setminus I$. Then either $m = k$ or $a_{m+1}\cdots a_1x \in I$. Hence $p_0 \in \overline{a_1x}\cdot\overline{a_2a_1x}\cdots\overline{a_m\cdots a_1x}\cdot\left(\overline{I}\langle\overline{S}\rangle^1\right)^1$.

Now, $(a_m\cdots a_1)\cdot x \in S\setminus I$ and so, by Lemma 3.2.6(4), $a_m\cdots a_1$ and $a_m\cdots a_1x$ belong to the same maximal $\mathcal{D}$-class of S. Then, by Lemma 3.2.6(5), $a_1x\mathcal{L}a_2a_1x\mathcal{L}\cdots\mathcal{L}a_m\cdots a_1x$ and $a_1x \in S\setminus I$. Thus $p_0 \in P_1\cdot\left(\overline{I}\langle\overline{S}\rangle^1\right)^1$ and the claim follows. □

Lemma 3.3.5. *If the set*

$$P_2 = \{\overline{a_1}\cdots\overline{a_n} : \{a_1,\ldots,a_n\} \subseteq S\setminus I \text{ is a left zero subsemigroup}\}$$

is finite, then P_1 is finite.

Proof. Let P_2 be finite. Take any $p_1 = \overline{a_1}\cdots\overline{a_k} \in P_1$ with $a_1\mathcal{L}a_2\mathcal{L}\cdots\mathcal{L}a_k$ and $a_1 \in S\setminus I$. For any $x \in S$ we have

$$q(p_1, x) = \overline{a_1x}\cdot\overline{a_2a_1x}\cdots\overline{a_k\cdots a_1x}.$$

As before, it suffices to prove that there are finitely many products $q(p_1, x)$ when p_1 runs through P_1 and x runs through S. As in the proof of Lemma 3.3.4, let $m = m(p_1)$ be the maximal number such that $a_m\cdots a_1x \in S\setminus I$. Then $a_2a_1,\ldots,a_ma_{m-1}$ belong to the same maximal $\mathcal{D}$-class. Then, for all $j \leq m-1$, $a_{j+1}\mathcal{D}a_{j+1}a_j\mathcal{D}a_j$ and so by Lemma 3.2.5 we have that $a_{j+1}a_j \in R_{a_{j+1}}\cap L_{a_j}$ and that $L_{a_{j+1}}\cap R_{a_j}$ contains an idempotent. Recall that $a_j\mathcal{L}a_{j+1}$. Hence $a_j \in L_{a_{j+1}}\cap R_{a_j}$ and since S is $\mathcal{H}$-trivial, we obtain that a_j is an idempotent for all $j < m$. Therefore, since $a_1\mathcal{L}\cdots\mathcal{L}a_m$, it follows that $\{a_1,\ldots,a_{m-1}\}$ forms a left zero subsemigroup in S. Therefore $\overline{a_1}\cdots\overline{a_{m-1}} \in P_2$. Thus there are finitely many products

$$\overline{a_1x}\cdot\overline{a_2a_1x}\cdots\overline{a_{m-1}\cdots a_1x} = q(\overline{a_1}\cdots\overline{a_{m-1}}, x)$$

when p_1 runs through P_1 and x runs through S. Since $a_{m+1}\cdots a_1x \in I$, by Lemma 3.3.1 it follows now that the set $\{q(p_1, x) : p_1 \in P_1,\ x \in S\}$ is finite. Thus P_1 is finite. □

We will prove by induction on k that the subset $Q_k \subseteq P_2$, consisting of those products $\overline{a_1} \cdots \overline{a_n} \in P_2$ such that the left zero subsemigroup $\{a_1, \ldots, a_n\} \subseteq S \setminus I$ contains precisely k distinct idempotents, is finite. This will then prove that P_2 is finite and so the theorem will be established.

Base of induction.

$k = 1$. To prove the base case, it is enough to show that $\overline{a}$ is of finite order for all idempotents $a \in S \setminus I$.

Let a be an arbitrary idempotent from $S \setminus I$. Let E be the set of all idempotents $\mathcal{R}$-equivalent to a and let X_a be the set of all $x \in D_a$ such that ax is an idempotent in D_a. Notice that if $x \in S \setminus X_a$, then $(ax)^2 \in I$; and if $x \in X_a$, then $a\mathcal{R}ax$.

We will prove now that the set $A = \{q(\overline{a}^n, x) : n \geq 1,\ x \in S \setminus X_a\}$ is finite. So, take $x \in S \setminus X_a$ and $n \geq 1$. Then $q_x = q(\overline{a}^n, x) = \overline{ax}^n$. Consider $q_{x,y} = q(q_x, y)$ when $y \in S$:

$$q_{x,y} = \overline{axy} \cdot \overline{axaxy} \cdots \overline{(ax)^n y} \in \overline{I} \cup \overline{S} \cdot \overline{I}\langle \overline{S} \rangle^1,$$

since $(ax)^2 \in I$. Thus the set $\{q(\alpha, y) : \alpha \in A,\ y \in S\}$ is finite and so A is finite.

On the other hand, $q(\overline{a}^n, x) = \overline{ax}^n$ and $ax \in E$, for all $x \in X_a$.

Now, since A is finite there is an infinite increasing sequence $n_1 < n_2 < \cdots$ such that $q(\overline{a}^{n_i}, x) = q(\overline{a}^{n_{i+1}}, x)$ and $\tau(\overline{a}^{n_i}) = \tau(\overline{a}^{n_{i+1}})$ for all $x \in S \setminus X_a$ and for all i.

To summarize: we had an idempotent $a \in S \setminus I$ and arrived at the conclusion of the previous paragraph. The same type conclusion will hold for all elements $e \in E$ (E is the set of all idempotents $\mathcal{R}$-equivalent to a). Hence, taking now subsequences of $n_1 < n_2 < \cdots$ we gradually will arrive at an infinite sequence $k_1 < k_2 < \cdots$ such that $q(\overline{e}^{k_i}, x) = q(\overline{e}^{k_{i+1}}, x)$ and $\tau(\overline{e}^{k_i}) = \tau(\overline{e}^{k_{i+1}})$ for all $x \in S \setminus X_e$, for all $e \in E$ and for all i.

Consider now the wreath recursions for the elements $\overline{e}^{k_1}$ and $\overline{e}^{k_2}$ for any $e \in E$. Their actions on the first level of the S-tree coincide. The restrictions of $\overline{e}^{k_1}$ and $\overline{e}^{k_2}$ to the subtrees with roots labeled by elements from $S \setminus X_e$ are equal. And for any $x \in X_e$, the restrictions of $\overline{e}^{k_1}$ and $\overline{e}^{k_2}$ to the subtrees with roots labeled by an element $x \in X_e$ are $\overline{ex}^{k_1}$ and $\overline{ex}^{k_2}$ where $ex \in E$. Hence, by recursion, $\overline{e}^{k_1} = \overline{e}^{k_2}$ and so $\overline{e}$ is of finite order for all $e \in E$. So, $\overline{a}$ is of finite order. The base case is established.

Induction step.

We will do step $k \mapsto k+1$. Take an arbitrary product $\pi = \overline{a_1} \cdots \overline{a_n} \in Q_{k+1}$. There are precisely $(k+1)$ different $\mathcal{R}$-classes among $R_{a_1}, \ldots, R_{a_n}$. Obviously, it would suffice to prove the step if $a_1, \ldots, a_n$ come from fixed $(k+1)$ $\mathcal{R}$-classes (and for every of these $\mathcal{R}$-classes there is at least one

representative among $a_1, \ldots, a_n$). In particular, in the remainder of the proof all the products from Q_{k+1} will involve these fixed $\mathcal{R}$-classes. The $\mathcal{D}$-class containing these $\mathcal{R}$-classes we will denote by D.

With every such product π we associate the corresponding $\mathcal{L}$-class $L(\pi) = L_{a_1} = \cdots = L_{a_n}$. We have $q_x = q(\pi, x) = \overline{a_1 x} \cdots \overline{a_n x}$ for all $x \in S$.

Make the following observation. Assume that $a_1 x \in S \backslash I$. This happens if and only if $a_1 x \in D$. Then $a_1 x, x \in D$ and so, since $a_1 x \mathcal{L} \cdots \mathcal{L} a_n x$, we obtain that $a_i, x, a_i x \in D$ for all i. Hence $a_i \mathcal{R} a_i x$ for all i.

Furthermore, for every $\mathcal{L}$-class in D there exists x such that $a_1 x$ lies in this $\mathcal{L}$-class. Now we split S into three disjoint sets:

- The set $A(\pi)$ of all x such that $a_1 x \notin D$.
- The set $B(\pi)$ of all x such that $a_1 x \in D$ and there are at most k idempotents among $a_1 x, \ldots, a_n x$.
- The set $C(\pi)$ of all x such that $a_1 x \in D$ and there are precisely $(k+1)$ idempotents among $a_1 x, \ldots, a_n x$.

Notice that $a_1 x \in D$ if and only if $L(\pi) \cap R_x$ is an idempotent. Thus each of $A(\pi), B(\pi), C(\pi)$ depends only on $L(\pi)$ and *not* on a_1.

If $x \in A(\pi)$ then $a_1 x \in I$ and so $q_x \in \overline{I}\langle \overline{S} \rangle^1$.

Let $x \in B(\pi)$. Take $y \in S$. We have $q(q_x, y) = \overline{a_1 x y} \cdots \overline{a_n x a_{n-1} x \cdots a_1 x y}$. Let m be maximum such that $a_i x \cdots a_1 x y \in D$ for all $i \leq m$. Recall that $a_1 x \mathcal{L} \cdots \mathcal{L} a_n x$. So, as in the proof of Lemma 3.3.5, we have that $a_1 x, \ldots, a_{m-1} x$ are idempotents. There are at most k such idempotents and so $a_1 x, \ldots, a_{m-1} x$ split in at most k $\mathcal{R}$-classes. We have $a_i x \cdots a_1 x y = a_i x y \mathcal{R} a_i x$ and so there are at most k different $\mathcal{R}$-classes among $R_{a_1 x y}, \ldots, R_{a_{m-1} x y}$. Therefore there are at most k idempotents among $a_1 x y, \ldots, a_{m-1} x y$ (as they lie in L_{xy} and S is $\mathcal{H}$-trivial). Thus for all $y \in S$, we have $q(q_x, y) \in \overline{I}\langle \overline{S} \rangle^1 \cup Q_k \overline{S} \cdot \overline{I}\langle \overline{S} \rangle^1$. By induction hypothesis this implies that there are only finitely many q_x for every $\pi \in Q_{k+1}$ and $x \in B(\pi)$.

Let, finally, $x \in C(\pi)$. Since $a_1 x, \ldots, a_n x$ lie in exactly $(k+1)$ $\mathcal{R}$-classes, we have that all of $a_1 x, \ldots, a_n x$ are idempotents. In particular $q_x = \overline{a_1 x} \cdots \overline{a_n x} \in Q_{k+1}$ and $a_1 x, \ldots, a_n x$ involve the same (fixed) $\mathcal{R}$-classes as $a_1, \ldots, a_n$. We also mention that if we fix some $\mathcal{L}$-class L in D such that $L = L(\rho)$ for some $\rho \in Q_{k+1}$, then the set of all $q(\pi, x)$, where $\pi \in Q_{k+1}$, $L(\pi) = L$ and $x \in C(\pi)$, exhausts the whole of Q_{k+1}.

Let M be the total (finite) number of elements in $\{q(\pi, x) : x \in A(\pi) \cup B(\pi),\ \pi \in Q_{k+1}\}$. Let also $N = M^{|S|}|S|$ and p be the number of $\mathcal{L}$-classes in D.

Take now any product $\pi = \overline{a_1} \cdots \overline{a_{N^p+1}} \in Q_{k+1}$. We will prove that π equals some element from Q_{k+1} of length less than $N^p + 1$. That will complete the induction step and thus the proof of the theorem.

Let $L_1, \ldots, L_q$ be all $\mathcal{L}$-classes, which in intersection with the fixed $\mathcal{R}$-classes give $(k+1)$ idempotents. Assume without loss of generality that $L(\pi) = L_1$. Note that $\pi = q(\pi, x)$ for some $x \in C(\pi)$.

By Pigeonhole Principle, we have that there exist $1 \leq i_1 < \cdots < i_{N^{p-1}+1} \leq N^p + 1$ such that $\tau(\overline{a_1} \cdots \overline{a_{i_j}}) = \tau(\overline{a_1} \cdots \overline{a_{i_k}})$ and $q(\overline{a_1} \cdots \overline{a_{i_j}}, x) = q(\overline{a_1} \cdots \overline{a_{i_k}}, x)$ for all $x \in A(\pi) \cup B(\pi)$ and $j < k$. Notice now that since $a_1 \mathcal{L} a_{i_1}$, we have $L(\pi) = L(\overline{a_{i_1}} \cdots \overline{a_{i_k}})$. There exists $y \in C(\pi)$ such that $L(q(\pi, y)) = L_2$. Analogously, by Pigeonhole Principle, we have that there is a subsequence $i_1 \leq j_1 < \cdots < j_{N^{p-2}+1} \leq i_{N^{p-1}+1}$ such that $\tau(\overline{a_1 y} \cdots \overline{a_{j_u} y}) = \tau(\overline{a_1 y} \cdots \overline{a_{j_v} y})$ and $q(\overline{a_1 y} \cdots \overline{a_{j_u} y}, x) = q(\overline{a_1 y} \cdots \overline{a_{j_v} y}, x)$ for all $x \in A(q(\pi, y)) \cup B(q(\pi, y))$ and $u < v$. Proceeding in this way in total at most q times we arrive at two indices $u < v$, such that

$$\tau(\overline{a_1 z} \cdots \overline{a_u z}) = \tau(\overline{a_1 z} \cdots \overline{a_v z})$$

and

$$q(\overline{a_1 z} \cdots \overline{a_u z}, x) = q(\overline{a_1 z} \cdots \overline{a_v z}, x)$$

for all $z \in C(\pi)$, $x \in A(q(\pi, z)) \cup B(q(\pi, z))$.

Finally, we remark that if $x \in C(\pi)$ and $y \in C(q(\pi, x))$, then $xy \in C(\pi)$. Thus, from wreath recursions for elements $\overline{a_1 z} \cdots \overline{a_u z}$ and $\overline{a_1 z} \cdots \overline{a_v z}$ for all $z \in C(\pi)$, it now follows that $\overline{a_1} \cdots \overline{a_u} = \overline{a_1} \cdots \overline{a_v}$ and so

$$\pi = \overline{a_1} \cdots \overline{a_u} \cdot \overline{a_{v+1}} \cdots \overline{a_{N^p+1}}$$

is of length strictly less than $N^p + 1$. □

3.4 Proof of Proposition 3.1.3

Proof of Proposition 3.1.3. ($\Rightarrow$). Suppose that $\mathbf{C}(S)$ is free. Let K be the minimal ideal of S. Then K is a Rees matrix semigroup $\mathcal{M}[G; I, J; P]$ for some $J \times I$-matrix P and group G with identity e. By [45, Theorem 3.4.2] we even may assume that $1 \in I$, $1 \in J$ and $p_{j1} = p_{1i} = e$ for all $i \in I$, $j \in J$. Then the element $k = (1, e, 1) \in K$ is clearly an idempotent. We will prove now that $\overline{k} \cdot \overline{s} = \overline{k} \cdot \overline{sk}$. Indeed,

$$q(\overline{k} \cdot \overline{s}, x) = \overline{kx} \cdot \overline{skx} = q(\overline{k} \cdot \overline{sk}, x)$$

holds for every $x \in S$, and $\tau(\overline{k} \cdot \overline{s}) = \lambda_{sk} = \tau(\overline{k} \cdot \overline{sk})$. Hence $\overline{k} \cdot \overline{s} = \overline{k} \cdot \overline{sk}$ and so, since a free semigroup is cancellative, we obtain $\overline{s} = \overline{sk}$. Then $\lambda_s = \lambda_{sk}$ and, in particular, $st = skt$ for all $s, t \in S$.

Fix some $i \in I$. For every $x \in S$ there exist $i_x \in I$, $j_x \in J$ and $g_x \in G$ such that $x(1,e,1) = (i_x, g_x, j_x)$. Then $(i_x, g_x, j_x) = (i_x, g_x, j_x)(1,e,1) = (i_x, g_x, 1)$ and so $x(1,e,1) = (i_x, g_x, 1)$. Hence, since $\overline{s} = \overline{s(1,e,1)}$ for all $s \in S$, we have

$$\overline{(i,g,1)x} = \overline{(i,g,1)x(1,e,1)} = \overline{(i,g,1)(i_x,g_x,1)} = \overline{(i,gg_x,1)}$$

for all $g \in G$ and $x \in S$. Now, for all $g, g' \in G$ and $x \in S$ we have that

$$q(\overline{(i,g,1)} \cdot \overline{(1,g',1)}, x) = \overline{(i,g,1)x} \cdot \overline{(1,g'g,1)x} = \overline{(i,gg_x,1)} \cdot \overline{(1,g'gg_x,1)}$$

is a product from $\overline{(i,G,1)} \cdot \overline{(1,G,1)}$. But

$$\lambda(\overline{(i_1,g,1)} \cdot \overline{(1,g',1)}) = \lambda_{(1,g'g,1)} = \lambda(\overline{(i_2,g,1)} \cdot \overline{(1,g',1)})$$

for all $i_1, i_2 \in I$. Hence, by wreath recursion, we obtain that $\overline{(i_1,g,1)} \cdot \overline{(1,g',1)} = \overline{(i_2,g,1)} \cdot \overline{(1,g',1)}$ for all $g, g' \in G$ and $i_1, i_2 \in I$. Then $\overline{(i_1,e,1)} = \overline{(i_2,e,1)}$ and so $\lambda_{(i_1,e,1)} = \lambda_{(i_2,e,1)}$ for all $i_1, i_2 \in I$. Thus I is a singleton and so K contains only one $\mathcal{R}$-class.

Finally, since $\lambda_s = \lambda_{sk}$ for all $s \in S$, we have that $S^2 \subseteq K$. Hence the only non-singleton $\mathcal{H}$-classes in S must be those lying in K. If K contains singleton $\mathcal{H}$-classes, then S is $\mathcal{H}$-trivial and so, by Theorem 3.1.2, $\mathbf{C}(S)$ is finite, a contradiction. Thus all $\mathcal{H}$-classes in K are non-singleton.

($\Leftarrow$). Since K contains only one $\mathcal{R}$-class, we have that $K = G \times R$ where G is a group with identity e and R is a right zero semigroup. By assumption G is non-trivial. Let $k = (g,r) \in K$ be as in the hypothesis. Then $\lambda_s = \lambda_{sk} = \lambda_{s(g,r)}$ for all $s \in S$.

Take any $s \in S$. Then $s(g,r) = (h,r')$ for some $h \in G$ and $r' \in R$. Since $(g,r)(e,r) = (g,r)$, we have $(h,r') = (h,r')(e,r) = (h,r)$. That is, $\lambda_s = \lambda_{s(g,r)} = \lambda_{(h,r)}$. Hence, by Lemma 3.2.1, $\overline{s} = \overline{(h,r)}$ and so $\overline{S} = \overline{H_{(e,r)}}$. Note that $H_{(e,r)} \cong G$ and so $H_{(e,r)}$ is a non-trivial subgroup. As in the proof of Theorem 3.1.2, we have that $\overline{H_{(e,r)}}$ is a free system. Hence $\mathbf{C}(S) = \langle \overline{H_{(e,r)}} \rangle$ is free of rank $|G|$. $\square$

3.5 Proofs of Propositions 3.1.4 and 3.1.5

Proof of Proposition 3.1.4. ($\Rightarrow$). Suppose that $\mathbf{C}(S)$ is a right zero semigroup. Let $a, b \in S$. Then $\overline{b} \cdot \overline{a} = \overline{a}$. In particular, $\lambda_{ab} = \lambda_a$. This implies that $abc = ac$ for all $a, b, c \in S$.

($\Leftarrow$). Suppose that $abc = ac$ for all $a, b, c \in S$. Then $\lambda_{ab} = \lambda_a$ for all $a, b \in S$. Now, $\overline{b} \cdot \overline{a} = \overline{a}$ if and only if $\lambda_{ab} = \lambda_a$ and $\overline{bx} \cdot \overline{abx} = \overline{ax}$ for all $x \in S$. By hypothesis, the latter is equivalent to $\overline{bx} \cdot \overline{ax} = \overline{ax}$. By recursive

arguments we now obtain that $\overline{b} \cdot \overline{a} = \overline{a}$ for all $a, b \in S$. Thus $\mathbf{C}(S)$ is a right zero semigroup. $\square$

Proof of Proposition 3.1.5. $(\Rightarrow)$. Suppose that $\mathbf{C}(S)$ is a left zero semigroup. Since this left zero semigroup is finitely generated, it is finite. So, by Theorem 3.1.2, S is $\mathcal{H}$-trivial. Let I be the minimal ideal in S. Then $\langle \overline{I} \rangle \subseteq \mathbf{C}(S)$ can be homomorphically mapped onto $\mathbf{C}(I)$. Since I is simple and finite, it is a Rees matrix semigroup. Since S is $\mathcal{H}$-trivial, $I = X \times Y$ for some left zero semigroup X and a right zero semigroup Y. By Lemmas 3.2.2 and 3.2.3, $\mathbf{C}(I)$ is a right zero semigroup on $|X|$ points. A homomorphic image of the left zero semigroup $\langle \overline{I} \rangle$ must be a left zero semigroup. Hence $|X| = 1$ and so I is a right zero semigroup.

Let $s \in S$ and $i \in I$. Then, since $\mathbf{C}(S)$ is a left zero semigroup, $\overline{s} \cdot \overline{i} = \overline{s}$; consequently $\lambda_s = \lambda_{is}$. Hence $sS = isS \subseteq I$ for all $s \in S$ and so $S^2 \subseteq I$. Thus $I = S^2$.

$(\Leftarrow)$. Suppose that the minimal ideal I of S coincides with S^2 and that I is a right zero semigroup.

Take an arbitrary $s \in S$ and fix $i \in I$. Then for every $x \in S$ we have that $sx \in I$ and so $isx = sx$. This implies that $\lambda_s = \lambda_{is}$. By Lemma 3.2.1, we have that $\overline{s} = \overline{is}$. Therefore $\overline{S} = \overline{I}$ and in particular $\mathbf{C}(S) = \langle \overline{I} \rangle$. So it suffices to prove that $\overline{i} \cdot \overline{j} = \overline{i}$ for all $i, j \in I$. Note that if $\alpha \in S^\infty$, then $\alpha \cdot \overline{i} \in I^\infty$. Since I is a right zero semigroup, $\overline{j}$ acts identically on I^∞. Hence $\alpha \cdot (\overline{i} \cdot \overline{j}) = \alpha \cdot \overline{i}$ for all $\alpha \in S^\infty$ and so $\overline{i} \cdot \overline{j} = \overline{i}$, as required. $\square$

3.6 Proof of Theorem 3.1.6

Proof of Theorem 3.1.6. The proof follows via the chain of implications $(1) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1)$.

$(2) \Rightarrow (1)$ is clear.

$(3) \Rightarrow (2)$. Let S be an inflation of a right zero semigroup T. Then for all $s, t, x \in S$, we have $sx = tx$. Hence $\lambda_s = \lambda_t$ and so, by Lemma 3.2.1, $\overline{s} = \overline{t}$ for all $s, t \in S$. It remains to prove that for any fixed $s \in S$, the element $\overline{s}$ is an idempotent. We have $\overline{s} = \lambda_s(\overline{s}, \ldots, \overline{s})$ and $\overline{s}^2 = \lambda_{s^2}(\overline{s}^2, \ldots, \overline{s}^2)$. Thus it suffices to prove that $\lambda_{s^2} = \lambda_s$. This holds since $s^2 x = sx$ for all $x \in S$.

$(1) \Rightarrow (3)$. We will prove by induction on $|S|$ that if $\mathbf{C}(S)$ is a group, then S is an inflation of a right zero semigroup by null semigroups. The base case $|S| = 1$ is trivial. So suppose the implication holds for all semigroups of cardinality $< |S|$ and $\mathbf{C}(S)$ is a group.

Let $\mathcal{T}_S$ be the transformation semigroup on S. The subsemigroup $\langle \lambda_s : s \in S \rangle$ in $\mathcal{T}_S$ is a homomorphic image of the group $\mathbf{C}(S)$ and so is a group.

This implies that the images and kernels of the mappings λ_s must coincide. These conditions can be translated as

- $sS = tS$ for all $s, t \in S$ and
- $sx = sy$ if and only if $tx = ty$, for all $s, t, x, y \in S$.

Notice that the condition that $sS = tS$ for all $s, t \in S$ is equivalent to $sS = S^2$ for all $s \in S$. The rest of the proof depends on whether $S^2 = S$ or not.

Case 1: $S^2 = S$**.**

Then, by the observations above, $sS = S^2 = S$ for all $s \in S$. So each $s \in S$, acting via left-multiplication, permutes S. Then for any $s \in S$, some power of s is a left identity e for S. Then for all $s, x, y \in S$, the condition $sx = sy$ implies $x = ex = ey = y$. Hence S is left cancellative. The condition that $sS = S$ for all $s \in S$ implies that S is right simple.

Therefore S is a right group and so $S = G \times R$ for some group G and a right zero semigroup R, see [18, Theorem 1.27]. By Lemma 3.2.3, we have $\mathbf{C}(G \times R) = \mathbf{C}(G)$. Hence by Theorem 3.1.1, G must trivial. Then $S \cong R$ is a right zero semigroup and so (3) holds.

Case 2: $S^2 \neq S$**.**

The condition of the case means that S contains indecomposable elements.

Recall that the kernels of all the mappings λ_s coincide. Partition S into these kernel classes $A_1, \ldots, A_k$ and notice that, for every $s \in S$, the equality $sx = sy$ holds if and only if x and y come from the same class. Furthermore, since the mappings λ_s generate a subgroup in $\mathcal{T}_S$, it follows that every kernel class A_i contains an image point, which must of course be an element of S^2 (the image of every λ_s is S^2).

The remainder of the proof we will work out in two subcases:

Subcase a: for all $a \in S \setminus S^2$ **there exists** $x \in S \setminus \{a\}$ **with** $x(S \setminus \{a\}) \neq (S \setminus \{a\})(S \setminus \{a\})$**.**

Consider an arbitrary $a \in S \setminus S^2$ and find the corresponding $x \in S \setminus \{a\}$. That $x(S \setminus \{a\}) \neq (S \setminus \{a\})(S \setminus \{a\})$ means that there exists an element $uv \notin x(S \setminus \{a\})$ where $u, v \in S \setminus \{a\}$. Since $uS = S^2 = xS$, there exists some $b \in S$ with $uv = xb$. Obviously then $b = a$. Hence $xa \notin x(S \setminus \{a\})$. That is, $xa \neq xy$ for all $y \in S \setminus \{a\}$. This is equivalent to that $sa \neq sy$ for all $s \in S$ and $y \in S \setminus \{a\}$. The kernel class A that contains a is not a singleton, for it

must contain an element from S^2 and a itself is indecomposable. Take an arbitrary $c \in A \setminus \{a\}$. Then $sa = sc$ for any $s \in S$, a contradiction.

Subcase b: There exists $a \in S \setminus S^2$ such that for all $x \in S \setminus \{a\}$ there holds $x(S \setminus \{a\}) = (S \setminus \{a\})(S \setminus \{a\})$.

Fix such an a. Obviously $T = S \setminus \{a\}$ is a subsemigroup of S.

We will show now that $\mathbf{C}(T)$ is a homomorphic image of $\mathbf{C}(S)$ and thus that $\mathbf{C}(T)$ is a group. Let I be the minimal ideal in S. Then I is simple and so, being finite, is completely simple. Hence I is a Rees matrix semigroup. Take now an arbitrary $i \in I$. Since I is a Rees matrix semigroup, there exists $e \in I$ such that $ei = i$. Then $\tau(\bar{i} \cdot \overline{a}) = \lambda_{ai} = \lambda_{aei} = \tau(\bar{i} \cdot \overline{ae})$ and

$$q(\bar{i} \cdot \overline{a}, x) = \overline{ix} \cdot \overline{aix} = \overline{ix} \cdot \overline{aeix} = q(\bar{i} \cdot \overline{ae}, x)$$

for all $x \in S$. Thus $\bar{i} \cdot \overline{a} = \bar{i} \cdot \overline{ae}$ in $\mathbf{C}(S)$. Since $\mathbf{C}(S)$ is a group, we derive now that $\overline{a} = \overline{ae}$. Since $e \in I$, the element ae must lie in $I \subseteq T$. Hence $\overline{S} = \overline{T}$ in $\mathbf{C}(S)$. Restricting the action of the states from $\mathcal{C}(S)$ to T^* yields the automaton $\mathcal{C}(T)$. Therefore $\mathbf{C}(T)$ is a homomorphic image of $\mathbf{C}(S)$, and as so is a group.

So, by the induction hypothesis, T is an inflation of a right zero semigroup by null semigroups. Suppose without loss of generality that $a \in A_k$. Then $A_1, \ldots, A_{k-1}, A_k \setminus \{a\}$ are the corresponding null semigroups from T. For each i, let $e_i \in A_i$ be the right zero in A_i. Then $S^2 = \{e_1, \ldots, e_k\}$. In particular, $e_k \neq a$ since a is indecomposable. Take now $a_i \in A_i$ and $a_j \in A_j$. Recall that $sx = sy$ as soon as x and y are from the same kernel class.

1. If $a_i \neq a$ and $a_j \neq a$, then $a_i a_j = e_i e_j = e_j$.
2. If $a_i \neq a$ and $a_j = a$, then $a_i a_j = a_i a = a_i e_k = e_k$.
3. Let $a_i = a$ and $a_j \neq a$. Let $aa_j = e_m$ for some m. Then $e_m = e_m^2 = e_m a a_j$. Since $e_m a \in T$, it follows that $e_m a a_j = e_j$ and so $e_m = e_m a a_j = e_j$. Hence $a_i a_j = e_j$.
4. If $a_i = a_j = a$, then $a_i a_j = a^2 = a e_k = e_k$.

Thus S is an inflation of a right zero semigroup $\{e_1, \ldots, e_k\}$ and the induction step is established. □

3.7 Further Discussion

The following proposition is an important consequence of Theorem 3.1.2.

Proposition 3.7.1. *Any infinite Cayley automaton semigroup contains a free semigroup of rank* 2.

Proof. Suppose $\mathbf{C}(S)$ is infinite. Then S is not $\mathcal{H}$-trivial. So S contains a non-trivial subgroup $G \leq S$. Then $\langle \overline{G} \rangle$ is a free semigroup of rank $|G|$. $\square$

Corollary 3.7.2. *The free product of two trivial semigroups* $\mathrm{Sg}\langle e, f \mid e^2 = e,\ f^2 = f \rangle$ *and free commutative semigroups of rank* > 1 *are all automaton semigroups, but neither of them is a Cayley automaton semigroup.*

Proof. That $\mathrm{Sg}\langle e, f \mid e^2 = e,\ f^2 = f \rangle$ and free commutative semigroups of rank > 1 are automaton semigroups can be found in [11]. That neither of these semigroups is a Cayley automaton semigroup follows immediately from Proposition 3.7.1. $\square$

Remark 3.7.3. The characterization of those finite semigroups S such that $\mathbf{C}(S)$ is a right zero semigroup, is 'close' to the characterization of rectangular bands: the latter are precisely those semigroups S such that all the elements from S are idempotents and $abc = ac$ for all $a, b, c \in S$, [45, Theorem 1.1.3].

In the following example we show that it is possible for a Cayley automaton semigroup to be a *non-trivial* left zero semigroup:

Example 3.7.4. Define a finite semigroup S on four points i, j, k, f with the following multiplication table:

	i	j	k	f
i	i	j	k	i
j	i	j	k	i
k	i	j	k	j
f	i	j	k	i

Then $\mathbf{C}(S)$ is a left zero semigroup on 2 points.

Proof. One checks that the multiplication table indeed gives a semigroup. By Lemma 3.2.1, $\overline{i} = \overline{j} = \overline{f}$. Hence, by Proposition 3.1.5, $\mathbf{C}(S)$ is a left zero semigroup generated by $\overline{j}$ and $\overline{k}$. It remains to notice that $\overline{j} \neq \overline{k}$. It follows from Lemma 3.2.1 and $f\lambda_j = jf = i \neq j = kf = f\lambda_k$. $\square$

In Theorem 3.1.6 we proved that no Cayley automaton semigroup can be a non-trivial group. In addition, it is proved in [64] that if S is a finite $\mathcal{H}$-trivial semigroup, then $\mathbf{C}(S)$ is a (finite) $\mathcal{H}$-trivial semigroup. In fact, the author believes that every Cayley automaton semigroup is $\mathcal{H}$-trivial and poses the following problem:

Question 1. Are all Cayley automaton semigroups $\mathcal{H}$-trivial?

3.8 Dual Cayley Automaton Semigroups

Let S be a finite semigroup. Define the *dual Cayley machine* $\mathcal{C}^*(S)$ to be the automaton, obtained from the right Cayley graph of S with respect to the generating set S by specifying the output symbol on the arc, going from s and labeled by x, to be xs. In other words, the states and the letters of $\mathcal{C}^*(S)$ are the elements of S and when $\mathcal{C}^*(S)$ is in the state s and reads the letter x, it moves to the state sx and outputs the letter xs.

The automaton semigroup generated by $\mathcal{C}^*(S)$ we will denote by $\mathbf{C}^*(S)$. The main goal of this section is

Theorem 3.8.1. *Let S be a finite semigroup. Then $\mathbf{C}^*(S)$ is finite if and only if S is $\mathcal{H}$-trivial and does not contain non-trivial right zero subsemigroups.*

In comparison to Theorem 3.1.2 there appears an additional condition to $\mathcal{H}$-triviality. Probably this means that, at least as regards automaton semigroups, the most natural way to obtain a transducer from the Cayley graph of a semigroup, is to construct $\mathcal{C}(S)$. The remainder of the section is devoted to the proof of Theorem 3.8.1. The proof will resemble that of Theorem 3.1.2, but is somewhat easier: there will be no need to deal with 'long' words and trying to reduce their lengths. Before we start the proof, first make some preparation.

In order to distinguish the states and letters in $\mathcal{C}^*(S)$, we will write $\underline{s}$ to denote the state corresponding to $s \in S$. If $S = \{s_1, \ldots, s_n\}$, then the wreath recursion for $\underline{s}$ looks like

$$\underline{s} = \rho_s(\underline{ss_1}, \ldots, \underline{ss_n}),$$

where $\rho_s : S \to S$ is given by $x \mapsto xs$.

If $x \in S$ and $\alpha \in \mathbf{C}^*(S)$, then by $q(\alpha, x)$ we will denote the state, to which α moves after reading $x \in S$. The transition function of α on S we will denote by $\tau(\alpha)$. So, $\tau(\alpha) : S \to S$ and for all $x \in S$, $x\tau(\alpha)$ is the symbol which outputs $\mathcal{C}^*(S)$, reading x in the state α. By definition, for all $a_1, \ldots, a_k, x \in S$, we have

$$q(\underline{a_1} \cdots \underline{a_k}, x) = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}}.$$

Also the corresponding transition function $\tau(\underline{a_1} \cdots \underline{a_k})$ is $\rho_{a_1} \cdots \rho_{a_k} = \rho_{a_1 \cdots a_k}$.

Lemma 3.8.2. *Let L be a finite left zero semigroup and S be a finite semigroup. Then $\mathbf{C}^*(S \times L) = \mathbf{C}^*(S)$.*

The proof of Lemma 3.8.2 is similar to that of Lemma 3.2.3. However, the analogue of Lemma 3.2.2 does not hold for the 'dual' case:

Lemma 3.8.3 ([11, Proposition 7]). *Let R be a finite right zero semigroup with $|R| > 1$. Then $\mathbf{C}^*(R)$ is a free semigroup of rank $|R|$.*

Lemma 3.8.4. *Let G be a non-trivial finite group. Then $\mathbf{C}^*(G)$ is infinite.*

Proof. Take any non-identity element $a \in G$. Then $H = \langle a \rangle$ is a non-trivial commutative group. Obviously the restriction of the action of the state $\underline{h}$, $h \in H$, to H^∞, is the same as the action of $\underline{h}$ in $\mathbf{C}^*(H)$. Notice that $\mathcal{C}(H) = \mathcal{C}^*(H)$ and so, by Theorem 3.1.1, $\underline{H}$ is a free system. Thus $\mathbf{C}^*(G)$ is infinite. □

Proof of Theorem 3.8.1. First notice that the condition that S does not contain non-trivial right zero subsemigroups is equivalent to the condition that there are no two distinct idempotents $e, f \in S$ such that $e\mathcal{R}f$.

($\Rightarrow$). Suppose that $\mathbf{C}^*(S)$ is finite. In the same way as in the proof of Theorem 3.1.2, one can show that S is $\mathcal{H}$-trivial. It remains to prove that there are no distinct idempotents $e, f \in S$ such that $e\mathcal{R}f$. So, suppose the converse: that there exist two idempotents $e \neq f$ with $e\mathcal{R}f$. Then $\{e, f\}$ is a 2-element right zero semigroup. Restricting the action of $\underline{e}$ and $\underline{f}$ to $\{e, f\}^\infty$ yields the automaton $\mathcal{C}^*(\{e, f\})$. By Lemma 3.8.3, it follows now that $\langle \underline{e}, \underline{f} \rangle$ is a free semigroup of rank 2, a contradiction.

($\Leftarrow$). We will prove by induction on $|S|$ that if S is $\mathcal{H}$-trivial and every its $\mathcal{R}$-class contains at most one idempotent, then $\mathbf{C}^*(S)$ is finite. The base case $|S| = 1$ is obvious. So, assume that S is a finite $\mathcal{H}$-trivial semigroup with no non-trivial zero subsemigroups and that the hypothesis holds for all such semigroups of size $< |S|$.

As in the proof of Theorem 3.1.2, let I be the set of all elements which do not lie in any maximal $\mathcal{D}$-class of S. By Lemma 3.2.6, I is an ideal. If $I = \varnothing$ then S is a rectangular band, and by assumption is thus a left zero subsemigroup. Then by Lemma 3.8.2, $\mathbf{C}^*(S)$ is trivial and so finite. So in the remainder of the proof we may assume that $I \neq \varnothing$. Analogously as we did in Lemma 3.3.1, one can prove that $\underline{I}\langle \underline{S} \rangle^1 = \underline{I} \cup \underline{I}\langle \underline{S} \rangle$ is finite. Since

$$\langle \underline{S} \rangle = \underline{I}\langle \underline{S} \rangle^1 \cup \langle \underline{S} \setminus \underline{I} \rangle \cup \langle \underline{S} \setminus \underline{I} \rangle \underline{I}\langle \underline{S} \rangle^1$$

we are left to prove that $\langle \underline{S} \setminus \underline{I} \rangle$ is finite. It follows from the following series of lemmas.

Lemma 3.8.5. *If the set $P_0 = \{\underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}} : a_1, \ldots, a_k \in S \setminus I,\ x \in S\}$ is finite, then $\langle \underline{S} \setminus \underline{I} \rangle$ is finite.*

Proof. Take a typical product $\underline{a_1} \cdots \underline{a_k} \in \langle \underline{S} \setminus \underline{I} \rangle$ with $a_1, \ldots, a_k \in S \setminus I$. Then

$$q_x = q(\underline{a_1} \cdots \underline{a_k}, x) = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}}.$$

for all $x \in S$. All the elements q_x together with $\tau(\underline{a_1} \cdots \underline{a_k})$ define $\underline{a_1} \cdots \underline{a_k}$ uniquely. This proves the claim. $\square$

Lemma 3.8.6. *If the set*

$$P_1 = \{\underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}} \mid a_i x a_1 \cdots a_{i-1} \in S \setminus I \text{ for all } i \leq k\}$$

is finite, then P_0 is finite.

Proof. Take a typical product $p_0 = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}} \in P_0$ with $a_1, \ldots, a_k \in S \setminus I$ and $x \in S$. Let m be the maximal number such that $a_m x a_1 \cdots a_{m-1} \in S \setminus I$. Then $p_0 \in P_1 \cdot (\underline{I}\langle \underline{S} \rangle^1)^1$ and hence the claim. $\square$

Lemma 3.8.7. *If the set*

$$P_2 = \{\underline{a_1} \cdots \underline{a_k} \mid a_1, \ldots, a_k \text{ are } \mathcal{L} - \text{equivalent idempotents from } S \setminus I\}$$

is finite, then P_1 is finite.

Proof. Take a typical product $p_1 = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}} \in P_1$. Since $a_k x a_1 \cdots a_{k-1} \in S \setminus I$, by Lemma 3.2.6(3) we have that all $a_1, \ldots, a_k, x$ lie in the same maximal $\mathcal{D}$-class D. Moreover, $a_1 x, \ldots, a_k x \in D$. Hence by Lemma 3.2.5, we have that each $\mathcal{H}$-class $L_{a_1} \cap R_x, \ldots, L_{a_k} \cap R_x$ contains an idempotent. Then, since every two $\mathcal{R}$-equivalent idempotents coincide, $a_1 \mathcal{L} \cdots \mathcal{L} a_k$. Now, for all $i \leq k-1$, we have $a_i a_{i+1} \in D$ and so $L_{a_i} \cap R_{a_{i+1}}$ contains an idempotent. Having that $a_i \mathcal{L} a_{i+1}$ and by $\mathcal{H}$-triviality, we deduce that a_{i+1} is an idempotent. Then $a_1 = a_1 a_2 = \cdots = a_1 \cdots a_{k-1}$. Hence

$$p_1 = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1 \cdots a_{k-1}} = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1}.$$

Finally, $a_1 x \in D$ and so $x a_1$, being the unique element of $L_{a_1} \cap R_x$, by Lemma 3.2.5 is an idempotent. Then for all $2 \leq i \leq k$, $a_i \mathcal{L} a_1 \mathcal{L} x a_1$, and since a_i is an idempotent, we obtain that $a_i x a_1 = a_i$. Therefore $p_1 = \underline{a_1 x} \cdot \underline{a_2} \cdots \underline{a_k}$. Thus $a_2, \ldots, a_k$ are $\mathcal{L}$-equivalent idempotents, so $p_1 \in \underline{S} \cdot P_2$ and we are done. $\square$

Lemma 3.8.8. *P_2 is finite.*

Proof. Take a typical product $\underline{a_1} \cdots \underline{a_k} \in P_2$. Then $q_x = q(\underline{a_1} \cdots \underline{a_k}, x) = \underline{a_1 x} \cdot \underline{a_2 x a_1} \cdots \underline{a_k x a_1}$ for all $x \in S$. Consider now the following three cases:

Case 1: $(a_1 x, a_1) \notin \mathcal{D}$.

Then, by Lemma 3.2.6(4), $a_1 x \in I$ and so there are at most $k_1 = |\underline{I}\langle \underline{S} \rangle^1|$ many such q_x-s.

Case 2: $a_1x\mathcal{D}a_1$ **but** $(a_1x, a_1) \notin \mathcal{L}$**.**

Let $y \in S$ be arbitrary. Then

$$q_{x,y} = q(q_x, y) = \underline{a_1xy} \cdot \underline{a_2xa_1ya_1x} \cdot \underline{a_3xa_1ya_1xa_2xa_1} \cdots .$$

We will prove that if $k > 2$, then $a_3xa_1ya_1xa_2xa_1 \in I$. Suppose the contrary. Then $a_3xa_1ya_1xa_2xa_1\mathcal{D}a_1$ and so a_1x, a_2, a_1xa_2 all lie in the same $\mathcal{D}$-class D_{a_1}. Then by Lemma 3.2.5, we obtain that $L_{a_1x} \cap R_{a_2} = \{e\}$ contains an idempotent. But $a_1\mathcal{L}a_2$ and $(a_1x, a_1) \notin \mathcal{L}$, so that a_2 and e are $\mathcal{R}$-equivalent distinct idempotents, a contradiction.

Therefore $q_{x,y} \in \underline{S} \cup \underline{S}^2 \cup (\underline{S}^2 \cdot \underline{I}\langle\underline{S}\rangle^1)$. In turn, it implies that there at most k_2 elements q_x, where k_2 is a finite number which depends only on S.

Case 3: $a_1x\mathcal{L}a_1$**.**

Then $a_1x \in D_{a_1}$ and so $x\mathcal{L}a_1$. Now, by Lemma 3.2.5 we have that $L_{a_1} \cap R_x$ is an idempotent. Hence x is an idempotent. Therefore $a_1x = a_1$, $a_2xa_1 = a_2, \ldots, a_kxa_1 = a_k$. Thus $q_x = \underline{a_1} \cdots \underline{a_k}$.

So, from Case 3 it follows that $\underline{a_1} \cdots \underline{a_k}$ is uniquely determined by $\tau(\underline{a_1} \cdots \underline{a_k})$ and q_x-s with $x \in S$ such that $(a_1x, a_1) \notin \mathcal{L}$. Thus from Cases 1 and 2 we have

$$|P_2| \leq |S| \cdot (k_1 + k_2)^{|S|}.$$

□

This completes the proof of the theorem. □

Chapter 4

Ideals, Finiteness Conditions and Green Index for Subsemigroups

In the present chapter we investigate a number of finiteness conditions related to ideals: stability, $\mathcal{J} = \mathcal{D}$, having finitely many ideals, $\min_R$, $\min_J$ and π-regularity.

The results of this chapter were obtained in collaboration with Robert Gray, James Mitchell and Nik Ruškuc and are taken from the work [32].

4.1 Introduction

In this chapter we direct our attention to some finiteness conditions that are peculiar to semigroups (in the sense that they are trivial for all groups), mostly related to ideals. More precisely, letting T be a subsemigroup of finite Green index in a semigroup S, for each of the following properties $\mathcal{P}$, we are going to prove that T satisfies $\mathcal{P}$ if and only if S satisfies $\mathcal{P}$:

- stability (Theorem 4.2.1);
- finitely many ideals (Theorem 4.4.1);
- $\min_R$ (Theorem 4.5.1);
- $\min_J$ (Theorem 4.5.3);
- π-regularity (Theorem 4.6.2).

Perhaps surprisingly, the finiteness condition $\mathcal{J} = \mathcal{D}$ behaves somewhat differently: it is preserved by supersemigroups of finite Green index (Theorem 4.3.1), and is *not* preserved even by subsemigroups of finite Rees index (Example 4.3.6). However, under certain regularity conditions, one can reverse Theorem 4.3.1; see Theorems 4.3.7 and 4.3.8.

4.2 Stability

Theorem 4.2.1. *Let S be a semigroup and let T be a subsemigroup of S with finite Green index. Then T is (right, left or two-sided) stable if and only if S is (right, left, or two-sided respectively) stable.*

We will need the following lemma:

Lemma 4.2.2. *Let S be a semigroup, let T be a right stable subsemigroup of S with finite Green index, and let $a, x \in S$ such that $(ax^i, ax^j) \notin \mathcal{R}^T$ for all $i \neq j$. Then there exists $N \in \mathbb{N}$ such that $x^i \in T$, $ax^i \in T$ and $(ax^i, ax^{2i}) \notin \mathcal{J}^T$ for all $i \geq N$.*

Proof. Since $(ax^i, ax^j) \notin \mathcal{R}^T$ for all $i \neq j$, it follows that $(ax^i, ax^j) \notin \mathcal{H}^T$ for all $i \neq j$. There are only finitely many $\mathcal{H}^T$-classes in $S \setminus T$, this implies that there exists $N \in \mathbb{N}$ such that $ax^i \in T$ for all $i \geq N$. Likewise, if $(x^i, x^j) \in \mathcal{H}^T$, then $(x^i, x^j) \in \mathcal{R}^T$ and so, since $\mathcal{R}^T$ is a left congruence, $(ax^i, ax^j) \in \mathcal{R}^T$. Therefore without loss of generality we may assume that $x^i \in T$ for all $i \geq N$.

Hence the right ideal ax^iT^1 of T properly contains the right ideal $ax^{2i}T^1$ for all $i \geq N$. It follows that the $\mathcal{R}$-class of ax^i in T is not a minimal $\mathcal{R}$-class in the $\mathcal{J}$-class of ax^{2i} in T. So, by Proposition 1.4.1(iv), ax^i and ax^{2i} lie in separate $\mathcal{J}$-classes of T. That is, $(ax^i, ax^{2i}) \notin \mathcal{J}^T$ for all $i \geq N$. □

Proof of Theorem 4.2.1. Clearly it is sufficient to prove the assertion for right stability.

($\Rightarrow$) It suffices, by Lemma 1.4.2, to prove that if $R_a^S \leq R_{ba}^S$, then $R_a^S = R_{ba}^S$ for all $a, b \in S$. Let $a, b \in S$ be arbitrary and let $x \in S$ be such that $a = bax$. Then for all $i \geq 1$ we have

$$a = bax = b^i ax^i.$$

We start by proving that there exist $i, j \in \mathbb{N}$ such that $i < j$ and $(ax^i, ax^j) \in \mathcal{R}^T$. Seeking a contradiction assume the contrary, that is, $(ax^i, ax^j) \notin \mathcal{R}^T$ for all $i \neq j$. It follows from Lemma 4.2.2 that there exists $N \in \mathbb{N}$ such that $(ax^i, ax^{2i}) \notin \mathcal{J}^T$ and $x^i \in T$ for all $i \geq N$. Now, if $i \geq N$, then

$$ax^i = b^i \cdot ax^{2i} \cdot 1 \ \ \& \ \ ax^{2i} = 1 \cdot ax^i \cdot x^i.$$

As $(ax^i, ax^{2i}) \notin \mathcal{J}^T$, we deduce that $b^i \in S \setminus T$ for all $i \geq N$. Since T has finite Green index, there exist $m, n \in \mathbb{N}$ such that $m - n, n \geq N$ and $(b^m, b^n) \in \mathcal{H}^T$. Thus $(b^m, b^n) \in \mathcal{L}^T$ and so there exists $t \in T^1$ such that $b^m = tb^n$. Hence

$$a = b^m ax^m = tb^n ax^m = t \cdot ax^{m-n} \cdot 1 \ \ \& \ \ ax^{m-n} = 1 \cdot a \cdot x^{m-n}$$

and so $(a, ax^{m-n}) \in \mathcal{J}^T$. Similarly,

$$a = t^2 \cdot ax^{2(m-n)} \cdot 1 \ \ \& \ \ ax^{2(m-n)} = 1 \cdot a \cdot x^{2(m-n)}$$

implies that $(a, ax^{2(m-n)}) \in \mathcal{J}^T$. Therefore $(ax^{m-n}, ax^{2(m-n)}) \in \mathcal{J}^T$, a contradiction as $m - n \geq N$.

So, we have shown that there exist $i < j$ such that $(ax^i, ax^j) \in \mathcal{R}^T$. In particular, there exists $u \in T^1$ such that $ax^i = ax^j u$. It follows that

$$ba = b^{i+1}ax^i = b^{i+1}ax^j u = ax^{j-i-1}u.$$

Thus from the assumption that $R_a^S \leq R_{ba}^S$ we obtain $(ba, a) \in \mathcal{R}^S$. That is, $R_{ba}^S = R_a^S$, as required.

($\Leftarrow$) As in the direct implication it suffices to prove that $R_a^T \leq R_{ba}^T$ implies $R_a^T = R_{ba}^T$ for all $a, b \in T$. Let $a, b \in T$ be arbitrary and let $x \in T$ such that $a = bax = b^k ax^k$. Since $R_a^S \leq R_{ba}^S$ and S is right stable, it follows that $R_a^S = R_{ba}^S$. Hence there exists $y \in S^1$ such that $ba = ay$ (and so, of course, $b^k a = ay^k$ for all $k \geq 1$). Now,

$$ba = b^{k+1}ax^k = ay^{k+1}x^k. \tag{4.1}$$

If $y^{k+1}x^k \in T$ for some $k \geq 1$, then $ba \in aT$ by (4.1). Then $R_a^T = R_{ba}^T$ and the proof is concluded.

On the other hand if $y^{k+1}x^k \in S \setminus T$ for all $k \geq 1$, then $y^k \in S \setminus T$ for all $k \geq 2$ (as $x \in T$). Then there exists $m \geq 2$ and $n \geq 1$ such that $(y^{m+n}, y^m) \in \mathcal{H}^T$ and, in particular, $(y^{m+n}, y^m) \in \mathcal{L}^T$. Hence there exists $t \in T^1$ such that $y^{m+n} = ty^m$. Then for all $k \geq 1$ we have that

$$t^k y^m x^{m+kn-1} = y^{m+kn}x^{m+kn-1} \in S \setminus T. \tag{4.2}$$

It follows that $y^m x^{m+kn-1} \in S \setminus T$ for all $k \geq 1$ (as $t \in T^1$). Hence there exist $u, v \in \mathbb{N}$ such that $v > u + 1$ and $(y^m x^{m+un-1}, y^m x^{m+vn-1}) \in \mathcal{H}^T$. In particular, $(y^m x^{m+un-1}, y^m x^{m+vn-1}) \in \mathcal{R}^T$ and so there exists $t_0 \in T^1$ where

$$y^m x^{m+un-1} = y^m x^{m+vn-1} t_0. \tag{4.3}$$

To conclude,

$$\begin{aligned}
ba &= ay^{m+un}x^{m+un-1} && \text{by (4.1)} \\
&= at^u y^m x^{m+un-1} && \text{by (4.2)} \\
&= at^u y^m x^{m+vn-1} t_0 && \text{by (4.3)} \\
&= at^u y^m x^{m+un-1} \cdot x^{(v-u)n} t_0 \\
&= ba \cdot x^{(v-u)n} t_0 \\
&= bax \cdot x^{(v-u)n-1} t_0 \\
&= ax^{(v-u)n-1} t_0 \in aT.
\end{aligned}$$

Thus $R_a^T = R_{ba}^T$, as required. $\square$

4.3 $\mathcal{J} = \mathcal{D}$

Theorem 4.3.1. *Let S be a semigroup, and let T be a subsemigroup of S with finite Green index. If $\mathcal{J} = \mathcal{D}$ in T, then $\mathcal{J} = \mathcal{D}$ in S.*

In order to prove Theorem 4.3.1 we need some preparation. Let S be a semigroup and T be a subsemigroup of S with finite Green index such that $\mathcal{J} = \mathcal{D}$ in T. Note that $\mathcal{J}^S = \mathcal{D}^S$ if and only if $\mathcal{J}^{S^1} = \mathcal{D}^{S^1}$. Hence we assume without of loss of generality that S has an identity 1 and that $1 \in T$ throughout this section. Let $a, b \in S$ such that $(a, b) \in \mathcal{J}^S$. Then define

$$Q_{a,b} = \{\, (x_1, x_2, y_1, y_2) \in S \times S \times S \times S \;:\; a = x_1 b y_1 \text{ and } b = x_2 a y_2 \,\}.$$

Note that if $(x_1, x_2, y_1, y_2) \in Q_{a,b}$ and $k > 0$, then

$$\begin{gathered}(x_1(x_2x_1)^k, x_2, y_1(y_2y_1)^k, y_2) \in Q_{a,b} \;\;\&\\ (x_1, x_2(x_1x_2)^k, y_1, y_2(y_1y_2)^k) \in Q_{a,b}.\end{gathered} \tag{4.4}$$

Lemma 4.3.2. *Let $a, b \in S$ such that $(a, b) \in \mathcal{J}^S$ and let $(x_1, x_2, y_1, y_2) \in Q_{a,b}$. Then*

(i) *if $\{k \in \mathbb{N} : x_1(x_2x_1)^k \in S \setminus T$ or $x_2(x_1x_2)^k \in S \setminus T\}$ is infinite, then $(b, x_1b) \in \mathcal{L}^S$ and $(a, x_2a) \in \mathcal{L}^S$;*

(ii) *if $\{k \in \mathbb{N} : y_1(y_2y_1)^k \in S \setminus T$ or $y_2(y_1y_2)^k \in S \setminus T\}$ is infinite, then $(b, by_1) \in \mathcal{R}^S$ and $(a, ay_2) \in \mathcal{R}^S$.*

Proof. **(i)** Assume that $x_1(x_2x_1)^k \in S \setminus T$ for infinitely many $k > 0$. Then there exist $k, r > 0$ such that $(x_1(x_2x_1)^k, x_1(x_2x_1)^{k+r}) \in \mathcal{H}^T$. In particular, $(x_1(x_2x_1)^k, x_1(x_2x_1)^{k+r}) \in \mathcal{L}^T$ and so there exists $t \in T$ such that $x_1(x_2x_1)^k = tx_1(x_2x_1)^{k+r}$. Hence

$$b = (x_2x_1)^{k+1}b(y_1y_2)^{k+1} = x_2tx_1(x_2x_1)^{k+r}b(y_1y_2)^{k+1} = x_2tx_1(x_2x_1)^{r-1}b$$

and so $(b, x_1b) \in \mathcal{L}^S$.

Also

$$a = (x_1x_2)^{k+1}a(y_2y_1)^{k+1} = tx_1(x_2x_1)^{k+r}x_2a(y_2y_1)^{k+1} = t(x_1x_2)^r a$$

and so $(a, x_2a) \in \mathcal{L}^S$.

The result follows by symmetry in the case that $x_2(x_1x_2)^k \in S \setminus T$ for infinitely many $k \in \mathbb{N}$.

(ii) The proof in this case is dual to that of the first case. □

Lemma 4.3.3. *Let $a, b \in S$ such that $(a, b) \in \mathcal{J}^S$. If there exists $(x_1, x_2, y_1, y_2) \in Q_{a,b}$ with $x_1, x_2, y_1, y_2 \in T$, then $(a, b) \in \mathcal{D}^S$.*

Proof. It suffices to consider the case when $a, b \in T$ and the case when $a, b \in S \setminus T$. (The case that $a \in T$ and $b \in S \setminus T$, say, cannot occur as $b = x_2 a y_2$ and $x_2, y_2 \in T$.)

In the first case, when $a, b \in T$, we have that $(a, b) \in \mathcal{J}^T$ and so $(a, b) \in \mathcal{D}^T$ by assumption. Thus $(a, b) \in \mathcal{D}^S$, as required.

In the second case, when $a, b \in S \setminus T$, we will prove that $(b, x_1 b) \in \mathcal{L}^S$ and $(x_1 b, a) \in \mathcal{R}^S$. Since $b = (x_2 x_1)^k b (y_1 y_2)^k$, we have that $(x_2 x_1)^k b \in S \setminus T$ for all $k \geq 1$. Hence there exist $m, n \geq 1$ and $t \in T$ with $(x_2 x_1)^m b = t(x_2 x_1)^{m+n} b$ (again since T has finite Green index). Then

$$b = (x_2 x_1)^m b (y_1 y_2)^m = t(x_2 x_1)^{m+n} b (y_1 y_2)^m = t(x_2 x_1)^n b$$

and so $(b, x_1 b) \in \mathcal{L}^S$.

Analogously, $(b, b y_1) \in \mathcal{R}^S$ and since $\mathcal{R}^S$ is a left congruence, $(a, x_1 b) = (x_1 b y_1, x_1 b) \in \mathcal{R}^S$. Moreover, as we have shown, $(x_1 b, b) \in \mathcal{L}^S$ and the proof is complete. □

Lemma 4.3.4. *Let $a, b \in S$ such that $(a, b) \in \mathcal{J}^S$. If $(x_1, 1, y_1, y_2) \in Q_{a,b}$ with $y_1, y_2 \in T$, then $(a, b) \in \mathcal{D}^S$.*

Proof. As $(x_1, 1, y_1, y_2) \in Q_{a,b}$, we have that $a = x_1 b y_1$ and $b = a y_2$. Hence $a = x_1^k b y_1 (y_2 y_1)^{k-1}$ for all $k \geq 1$. It follows that $(x_1^k, 1, y_1 (y_2 y_1)^{k-1}, y_2) \in Q_{a,b}$. Hence if there exists $k \in \mathbb{N}$ such that $x_1^k \in T$, then $(a, b) \in \mathcal{D}^S$ by Lemma 4.3.3.

Thus we may assume that $x_1^k \in S \setminus T$ for all $k \geq 1$. This implies that there exist $m, n \geq 1$ such that $x_1^{m+n} = t x_1^m$ for some $t \in T$ (again since T has finite Green index in S). Hence

$$a = x_1^{m+n} b (y_1 y_2)^{m+n-1} y_1 = t x_1^m b (y_1 y_2)^{m+n-1} y_1 = t \cdot b \cdot (y_1 y_2)^{n-1} y_1.$$

It follows that the quadruple $(t, 1, (y_1 y_2)^{n-1} y_1, y_2)$ lies in $Q_{a,b}$ and all its entries are in T and the result follows by Lemma 4.3.3. □

The following lemma provides the crucial step in the proof of Theorem 4.3.1.

Lemma 4.3.5. *Let $a, b \in S$ such that $(a, b) \in \mathcal{J}^S$. If $(x_1, x_2, y_1, y_2) \in Q_{a,b}$ with $y_1, y_2 \in T$, then $(a, b) \in \mathcal{D}^S$.*

Proof. There are two cases to consider: either

1. there exists $N \in \mathbb{N}$ such that $x_1(x_2x_1)^k, x_2(x_1x_2)^k \in T$ for all $k \geq N$; or
2. $x_1(x_2x_1)^k$ or $x_2(x_1x_2)^k \in S \setminus T$ for infinitely many k.

In Case (1), the quadruple

$$(x_1(x_2x_1)^N, x_2(x_1x_2)^N, y_1(y_2y_1)^N, y_2(y_1y_2)^N)$$

lies in $Q_{a,b}$ and all of its entries are in T. Hence the result follows by Lemma 4.3.3.

To prove the lemma in Case (2), note that $x_2a = x_2x_1 \cdot b \cdot y_1$ and $b = 1 \cdot x_2a \cdot y_2$. This implies that $(x_2a, b) \in \mathcal{J}^S$ and $(x_2x_1, 1, y_1, y_2) \in Q_{x_2a,b}$. So, by Lemma 4.3.4, $(x_2a, b) \in \mathcal{D}^S$. By the assumption of Case (2) it follows from Lemma 4.3.2(i) that $(x_2a, a) \in \mathcal{L}^S$. Therefore $(a, b) \in \mathcal{D}^S$. □

We can now use Lemmas 4.3.2 and 4.3.5 to prove Theorem 4.3.1.

Proof of Theorem 4.3.1. Let $a, b \in S$ such that $(a, b) \in \mathcal{J}^S$. Then by Lemma 4.3.5, if there exists $(x_1, x_2, y_1, y_2) \in Q_{a,b}$ with either $x_1, x_2 \in T$ or $y_1, y_2 \in T$, then the proof is concluded.

If neither of these conditions hold, then for all $(x_1, x_2, y_1, y_2) \in Q_{a,b}$ and for all $k \in \mathbb{N}$ we have $x_1(x_2x_1)^k$ or $x_2(x_1x_2)^k \in S \setminus T$ and $y_1(y_2y_1)^k$ or $y_2(y_1y_2)^k \in S \setminus T$ (from (4.4)). Therefore by Lemma 4.3.2, $(b, x_1b) \in \mathcal{L}^S$ and $(b, by_1) \in \mathcal{R}^S$. Thus $(a, by_1) = (x_1b \cdot y_1, by_1) \in \mathcal{L}^S$ and so $(a, b) \in \mathcal{D}^S$. □

The property $\mathcal{J} = \mathcal{D}$ is not inherited the other way round, from S to T, even for the finite Rees index, as the following example shows.

Example 4.3.6. We are going to define a semigroup S by means of a (fairly large) presentation. The generators are

$$A = \{a, b, c, d, x\},$$

and the main relations are

$$bxa = ac,\ acd = a,\ dc = cd,\ x^3 = x,\ x^2a = a. \tag{4.5}$$

There is also a number of zero relations, making the 'unnecessary' products of generators equal to zero:

$$\begin{aligned}
&aa = ab = ax = 0\\
&ba = bb = bc = bd = 0\\
&ca = cb = cx = 0\\
&da = db = dx = 0\\
&xc = xd = 0,\\
&bx^2b = 0.
\end{aligned}$$

As a consequence of these relations

$$ac^{k+1}d = acdc^k = ac^k$$

for all $k \geq 0$. A routine check confirms that the presentation together with the relations $ac^{k+1}d = ac^k$, viewed as the correspondent rewriting system is confluent. It is easy to see that this rewriting system is also terminating: it is length reducing, except for the relation $dc = cd$, which pushes ds systematically to the right. Therefore, a set of normal forms for non-zero elements is provided by all the words from A^+ which do not contain the left hand side of a relation as a subword; they are:

$$\begin{aligned}
&x,\ x^2\\
&ac^i,\ ad^j,\ xac^i,\ xad^j,\ c^id^j\ (i,j \geq 0),\\
&x^j(bx)^ib^kx^l\ (i \geq 0,\ j = 0,1,2,\ k = 0,1,\ l = 0,1,2).
\end{aligned}$$

The non-singleton Green's classes in S are:

$$\begin{aligned}
&L_x = R_x = D_x = J_x = \{x, x^2\},\\
&L_{ac^i} = \{ac^i, xac^i\},\ L_{ad^i} = \{ad^j, xad^j\},\\
&R_a = \{ac^i, ad^i\ :\ i \geq 0\}, R_{xa} = \{xac^i, xad^i\ :\ i \geq 0\},\\
&L_{xac^i} = \{xac^i, x^2ac^i\},\ L_{xad^i} = \{xad^i, x^2ad^i\},\\
&J_a = \{ac^i, ad^i, xac^i, xad^i\ :\ i \geq 0\},\\
&L_{x(bx)^ib^kx^l} = \{x(bx)^ib^kx^l, x^2(bx)^ib^kx^l\},\\
&R_{x^j(bx)^ib^kx} = \{x^j(bx)^ib^kx, x^j(bx)^ib^kx^2\}.
\end{aligned}$$

Therefore $\mathcal{J}^S = \mathcal{D}^S$.

Let now $T = S \setminus \{x\}$. The only words of S that are equal to x are x^{2i+1}, where $i \geq 0$. Such a word cannot be expressed as a product of two elements of T. Hence T is a subsemigroup of S. Now note that

$$a = b \cdot xa \cdot d,\ xa = xbx \cdot a \cdot d;$$

hence $(a, xa) \in \mathcal{J}^T$. We claim that $(a, xa) \notin \mathcal{D}^T$. Viewed in S we have

$$R_a = \{ac^i, ad^i\ :\ i \geq 0\}.$$

However, unlike the situation in S, the $\mathcal{L}$-class of xa in T is trivial. Indeed, the only elements of T we can premultiply xa with and not obtain 0 are of the form x^2 and $x^j(bx)^ix^l$ with $i > 0$ and $l \in \{0, 2\}$. After rewriting $x^j(bx)^ib^kx^l \cdot xa$ we can obtain only the words ac^i and xac^i. Thus, by premultiplying xa by elements of T, except x^2, we never get back to xa, and so L_{xa} is trivial in T. Therefore $L_{xa} \cap R_a = \varnothing$ in T, and hence $(a, xa) \notin \mathcal{D}^T$.

What is really curious is that under certain regularity assumptions, the property $\mathcal{J} = \mathcal{D}$ *is* inherited the other way as well. Below are two sample results. We have not been able to obtain a single satisfactory general result.

Theorem 4.3.7. *Let T be a subsemigroup in a semigroup S with finite Green index. Let also T be regular. Then $\mathcal{J} = \mathcal{D}$ in S implies $\mathcal{J} = \mathcal{D}$ in T.*

Theorem 4.3.8. *Let T be a subsemigroup in a semigroup S with finite Rees index. Let also S be regular. Then $\mathcal{J} = \mathcal{D}$ in S implies $\mathcal{J} = \mathcal{D}$ in T.*

In order to prove them we need the following technical lemma:

Lemma 4.3.9. *Let S be a semigroup, and let T be a subsemigroup of finite Green index in S. Let also $a, b \in T$ be such that $a\mathcal{D}^S ab$. Then there exists $c \in T$ such that $a\mathcal{L}^S c\mathcal{R}^S ab$ and $c\mathcal{J}^T a$.*

Proof. Since $a\mathcal{D}^S ab$, there exists $c \in S$ such that $a\mathcal{L}^S c\mathcal{R}^S ab$. It means that there exist $x_1, x_2, y_1, y_2 \in S^1$ with

$$\begin{aligned} a &= x_1 c & \qquad ab &= cx_2 \\ c &= y_1 a & \qquad c &= aby_2. \end{aligned}$$

Then $a = x_1 \cdot a \cdot by_2$ and $c = x_1 \cdot c \cdot by_2$.

The considerations are split into two cases.

Case 1: *there are infinitely many $k \geq 1$ with $(by_2)^k \in S \setminus T$.* Then there exist $k, n \geq 1$ such that $(by_2)^k \mathcal{H}^T (by_2)^{k+n}$. In particular there exists $t \in T^1$ such that $(by_2)^{k+n} t = (by_2)^k$. Then

$$a = x_1^k a (by_2)^k = x_1^k a (by_2)^{k+n} t = a(by_2)^n t = c \cdot (by_2)^{n-1} t.$$

Having that $c = a \cdot by_2$, we obtain $a\mathcal{R}^S c$. Then $a\mathcal{R}^S ab$ and so $a\mathcal{L}^S a\mathcal{R}^S ab$, as required since $a\mathcal{J}^T a$ trivially.

Case 2: *there exists $k_0 \geq 1$ such that $(by_2)^k \in T$ for all $k \geq k_0$.* We prove first that $c \in T$. Suppose the converse: $c \in S \setminus T$. Recall that $c = x_1^k c \cdot (by_2)^k$ and $c \in S \setminus T$. Hence $x_1^k c \in S \setminus T$ for all $k \geq k_0$. Then there exist $k, n \geq k_0$ such that $x_1^k c \mathcal{H}^T x_1^{k+n} c$. In particular, $t x_1^k c = x_1^{k+n} c$ for some $t \in T^1$. Then

$$c = x_1^{k+n} c (by_2)^{k+n} = t x_1^k c (by_2)^{k+n} = t x_1 \cdot c \cdot (by_2)^{n+1} = t \cdot a \cdot (by_2)^n.$$

Since $n \geq k_0$, we obtain $c \in T$, a contradiction. Hence $c \in T$. It remains to prove that $c\mathcal{J}^T a$.

Now, we have $c = x_1^k \cdot a \cdot (by_2)^{k+1}$ for all $k \geq k_0$. If there are infinitely many k such that $x_1^k \in S \backslash T$, then there exist $k, n \geq k_0$ such that $x_1^{k+n} = t \cdot x_1^k$ for some $t \in T$. Then

$$c = x_1^{k+n} \cdot a \cdot (by_2)^{k+n+1} = tx_1^k \cdot a \cdot (by_2)^{k+n+1} = t \cdot a \cdot (by_2)^{n+1}$$

and so $c \in TaT$. On the other hand, if $x_1^k \in T$ for all $k \geq N_0$ for some $N_0 \geq k_0$, then $c = x_1^{N_0} \cdot a \cdot (by_2)^{N_0+1}$ and so $c \in TaT$.

Having $a = x_1^{k+1} \cdot c \cdot (by_2)^k$ for all $k \geq k_0$, by analogous reasoning as in the previous paragraph we deduce that $a \in TcT$. Thus $c\mathcal{J}^T a$, as required. □

Proof of Theorem 4.3.7. Take two $\mathcal{J}^T$-equivalent elements t_1 and t_2 from T. Then there exist elements $\alpha_1, \alpha_2, \beta_1, \beta_2 \in T^1$ with $t_1 = \alpha_1 t_2 \beta_1$ and $t_2 = \alpha_2 t_1 \beta_2$. Then $t_1 \mathcal{J}^T t_1 \beta_2 \mathcal{J}^T t_2$ and $t_2 = \alpha_2 \cdot t_1 \beta_2$. Hence, to prove the theorem, it suffices to establish that, for every two elements $a, b \in T$, if $a\mathcal{J}^T ab$ then $a\mathcal{D}^T ab$, and that if $a\mathcal{J}^T ba$ then $a\mathcal{D}^T ba$. We will prove only the first assertion.

So suppose that $a, b \in T$ are such that $a\mathcal{J}^T ab$. Then $a\mathcal{J}^S ab$ and so $a\mathcal{D}^S ab$. By Lemma 4.3.9 we have that $a\mathcal{L}^S c\mathcal{R}^S ab$ for some $c \in T$. Recall that if P is a regular subsemigroup of a semigroup Q and $x, y \in P$ are $\mathcal{R}$-equivalent (resp. $\mathcal{L}$-equivalent) in Q, then x and y are $\mathcal{R}$-equivalent (resp. $\mathcal{L}$-equivalent) in P. Now, since T is regular, we have $a\mathcal{L}^T c$ and $c\mathcal{R}^T ab$. Thus $a\mathcal{D}^T ab$ and we are done. □

Before proving Theorem 4.3.8 we need another technical result:

Lemma 4.3.10. *Let T be a semigroup and $x, y, \alpha, \beta, \gamma, \delta \in T$ such that $x = \alpha y \beta$ and $y = \gamma x \delta$. Furthermore, assume that there exists $n \in \mathbb{N}$ such that $y = y(\beta\delta)^n$. Then x and y are $\mathcal{D}$-related in T.*

Proof. First notice that $y\mathcal{R}y\beta$. Now,

$$y = (\gamma\alpha)^n \cdot y \cdot (\beta\delta)^n = (\gamma\alpha)^n y.$$

Hence $y\beta = (\gamma\alpha)^{n-1}\gamma \cdot \alpha y\beta = (\gamma\alpha)^{n-1}\gamma \cdot x$. Having $x = \alpha \cdot y\beta$ we now obtain $y\beta\mathcal{L}x$. Thus $x\mathcal{D}y$. □

Proof of Theorem 4.3.8. As in the proof of Theorem 4.3.7, it suffices to prove that if $a\mathcal{J}^T ab$ then $a\mathcal{D}^T ab$ for all $a, b \in T$. So, let $a\mathcal{J}^T ab$ for some $a, b \in T$. Then $a\mathcal{D}^S ab$. By Lemma 4.3.9 we have that there exists $c \in J_a^T = J_{ab}^T$ such that $a\mathcal{L}^S c\mathcal{R}^S ab$.

Therefore, in order to prove the theorem, it is enough to prove that if $x, y \in T$ are such that $x\mathcal{R}^S y$ [$x\mathcal{L}^S y$] and $x\mathcal{J}^T y$, then $x\mathcal{D}^T y$. We will do this only for the $\mathcal{R}$-case.

So, let $x, y \in T$ be such that $x\mathcal{J}^T y$ and $x\mathcal{R}^S y$. We need to prove that $x\mathcal{D}^T y$. There exist $x', y' \in S$ such that $x = xx'x$ and $y = yy'y$. There also exist $\alpha, \beta, \gamma, \delta \in T$ such that $x = \alpha y \beta$ and $y = \gamma x \delta$. We have four possible cases.

Case 1: *$x \in yT$ and $y \in xT$.* Then immediately $x\mathcal{R}^T y$, as required.

Case 2: *$x = yt$ and $y = xf$ for some $t \in T$ and $f \in S \setminus T$.* In this case we have to distinguish three subcases:

Subcase 2a: *$x' \in T$ and $y' \in T$.* Then $x\mathcal{R}^T xx'$ and $y\mathcal{R}^T yy'$. In addition, $xx'\mathcal{R}^S x\mathcal{R}^S y\mathcal{R}^S yy'$. Hence $xx' = yy' \cdot xx'$ and $yy' = xx' \cdot yy'$. Therefore $xx'\mathcal{R}^T yy'$ and so $x\mathcal{R}^T y$.

Subcase 2b: *$x' \in S \setminus T$ and $y' \in T$.* Then $y\mathcal{R}^T yy'$. Moreover,

$$x = yy' \cdot yt \tag{4.6}$$
$$yy' = x \cdot fy'. \tag{4.7}$$

If $fy' \in T$ then $x\mathcal{R}^T yy'$ and so $x\mathcal{R}^T y$. So, let $fy' \in S \setminus T$. Recall that $x\mathcal{R}^S yy'$ and $x\mathcal{J}^T yy'$. Since it suffices to prove that $x\mathcal{D}^T yy'$, in view of (4.6), without loss of generality we may assume that $y^2 = y$ and put $y' = y$. Now, $y = x \cdot fy$. If $fy \in T$ then $x\mathcal{R}^T y$, as required. Hence we may assume that $fy \in S \setminus T$. Then $f(\gamma\alpha)^k \cdot y(\beta\delta)^k \in S \setminus T$ for all $k \geq 1$ and so $f(\gamma\alpha)^k \in S \setminus T$ for all $k \geq 1$. This implies that $f(\gamma\alpha)^k = f(\gamma\alpha)^{k+n}$ for some $k, n \geq 1$. Then

$$fy = f \cdot (\gamma\alpha)^{k+n} y(\beta\delta)^{k+n} = f(\gamma\alpha)^k y(\beta\delta)^{k+n} = fy(\beta\delta)^n.$$

Hence $y = x \cdot fy = xfy(\beta\delta)^n = y(\beta\delta)^n$ and so by Lemma 4.3.10, $x\mathcal{D}^T y$, as required.

Subcase 2c: *$y' \in S \setminus T$.* Then $y = x \cdot fy'y$. If $fy'y \in T$ then $x\mathcal{R}^T y$. Hence we may assume that $fy'y \in S \setminus T$. Then $fy'(\gamma\alpha)^k \cdot y(\beta\gamma)^k \in S \setminus T$ for all $k \geq 1$. Thus $fy'(\gamma\alpha)^k \in S \setminus T$ for all $k \geq 1$. Then there exist $k, n \geq 1$ such that $fy'(\gamma\alpha)^k = fy'(\gamma\alpha)^{k+n}$. Hence

$$fy'(\gamma\alpha)^k = fy'(\gamma\alpha)^{k+nr}$$

for all $r \geq 1$. Since $y = xf$, we have $yy'(\gamma\alpha)^k = yy'(\gamma\alpha)^{k+nr}$ for all $r \geq 1$.

Now,

$$\begin{aligned} y &= yy'y \\ &= yy'(\gamma\alpha)^k y(\beta\delta)^k \\ &= yy'(\gamma\alpha)^{k+nr} y(\beta\delta)^k \\ &= yy'(\gamma\alpha)^{nr} y \end{aligned}$$

for all $r \geq 1$. Hence we may assume that $y'(\gamma\alpha)^{nr} \in S \setminus T$ for all $r \geq 1$ (otherwise we can move to **Subcase 2b** and obtain that $x\mathcal{D}^T y$). So, there exist $r_1 < r_2$ with $r_2 - r_1 > 1$ such that $y'(\gamma\alpha)^{nr_1} = y'(\gamma\alpha)^{nr_2}$. Then

$$\begin{aligned} y'y(\beta\delta)^n &= y'(\gamma\alpha)^{nr_1} \cdot y(\beta\delta)^{n(r_1+1)} \\ &= y'(\gamma\alpha)^{nr_2} \cdot y(\beta\delta)^{n(r_1+1)} \\ &= y'(\gamma\alpha)^{n(r_2-r_1-1)} y. \end{aligned}$$

This yields

$$y = y \cdot y'(\gamma\alpha)^{n(r_2-r_1-1)} y = yy'y \cdot (\beta\delta)^n = y(\beta\delta)^n$$

and so $x\mathcal{D}^T y$ by Lemma 4.3.10.

Case 3: *$x = yf$ and $y = xt$ for some $t \in T$ and $f \in S \setminus T$.* This case is dual to Case 2.

Case 4: *$x = yf_1$ and $y = xf_2$ for some $f_1, f_2 \in S \setminus T$.* Once again we will distinguish three subcases:

Subcase 4a: *$x' \in T$ and $y' \in T$.* Then immediately $x\mathcal{R}^T y$.

Subcase 4b: *$x' \in S \setminus T$ and $y' \in T$.* Note first that

$$\begin{aligned} x &= yy' \cdot yf_1 \\ yy' &= x \cdot f_2 y'. \end{aligned}$$

If any of yf_1 and f_2y' is in T then we move to Cases 1–3 and derive that $x\mathcal{D}^T yy'$. Since $y\mathcal{R}^T yy'$, then $x\mathcal{D}^T y$ and we are done. Hence without loss of generality we may assume that $y^2 = y$ and $y' = y$. Then $y = x \cdot f_2 y$. If $f_2 y \in T$ then we move to **Case 3** and the proof is complete. So we may assume that $f_2 y \in S \setminus T$. Then, as before, $f_2(\gamma\alpha)^k \in S \setminus T$ for all $k \geq 1$. Then $f_2(\gamma\alpha)^{k+n} = f_2(\gamma\alpha)^k$ for some $k, n \geq 1$. This implies $f_2 y(\beta\delta)^n = f_2 y$ and so

$$y = xf_2 y = xf_2 y(\beta\delta)^n = y(\beta\delta)^n.$$

Then by Lemma 4.3.10, $x\mathcal{D}^T y$.

Subcase 4c: $y' \in S \setminus T$. Then in the same way as in Subcase 2c we can show that we either can move to **Subcase 4b** or move to **Case 3**. In any of cases we have $x\mathcal{D}^T y$. □

The only case we have not covered leads to the following problem:

Question 2. Let T be a subsemigroup in a semigroup S with finite Green index. Let also S be regular and $\mathcal{J} = \mathcal{D}$ in S. Is it true then that $\mathcal{J} = \mathcal{D}$ in T?

4.4 Finitely Many Ideals

In [33] it was proved that if T is a subsemigroup of finite Green index in a semigroup S, then T has finitely many right (left) ideals if and only S has finitely many right (resp. left) ideals. We prove here the same theorem for the case of two-sided ideals:

Theorem 4.4.1. *Let S be a semigroup and let T be a subsemigroup of S with finite Green index. Then T has finitely many ideals if and only if S has finitely many ideals.*

Proof. ($\Rightarrow$) Suppose that T has finitely many ideals, or, equivalently, finitely many $\mathcal{J}$-classes. Let J be an arbitrary $\mathcal{J}$-class of S. Then $J \cap T$ is a union of $\mathcal{J}$-classes of T, while $J \cap (S \setminus T)$ is a union of relative $\mathcal{R}^T$-classes. It follows that S has finitely many $\mathcal{J}$-classes.

($\Leftarrow$) Let now S have finitely many ideals, and suppose that T has infinitely many ideals. Then there exists a $\mathcal{J}$-class J of S which contains infinitely many $\mathcal{J}$-classes of T. In particular, it either contains an infinite chain

$$J_{u_1} > J_{u_2} > \dots$$

or an infinite chain

$$J_{u_1} < J_{u_2} < \dots$$

or an infinite antichain

$$J_{u_1}, J_{u_2}, \dots$$

of $\mathcal{J}$-classes of T. In any case, for any number $M \geq 1$, it is possible to find elements $u_1, \dots, u_M$ in J such that

$$J_{u_i} \not\leq J_{u_j} \ (1 \leq i < j \leq M) \tag{4.8}$$

in T. Take so far M to be some unspecified number, we will discuss later what we should take for M.

Since u_i and u_j are $\mathcal{J}$-related in S for all $1 \leq i < j \leq M$, we can write

$$u_i = \alpha_i u_{i+1} \beta_i \ (i = 1, 2, \ldots, M-1;\ \alpha_i, \beta_i \in S). \tag{4.9}$$

Define

$$\alpha_{i,j} = \alpha_i \alpha_{i+1} \ldots \alpha_{j-1},\ \beta_{i,j} = \beta_{j-1} \ldots \beta_{i+1} \beta_i \tag{4.10}$$

for all $1 \leq i < j \leq M$. These elements satisfy

$$u_i = \alpha_{i,j} u_j \beta_{i,j} \ (1 \leq i < j \leq M). \tag{4.11}$$

From (4.11) and (4.8) it follows that for all $1 \leq i < j \leq M$ at least one of $\alpha_{i,j}, \beta_{i,j}$ is not in T. By Ramsey's Theorem, for any a priori prescribed $M_1 \geq 1$, there exists M such that there exists an subset $I \subseteq \{1, \ldots, M\}$ of size M_1 such that either $\alpha_{i,j} \in S \setminus T$ for all $i, j \in I$, $i < j$, or else $\beta_{i,j} \in S \setminus T$ for all $i, j \in I$, $i < j$. Without loss of generality assume the first of these possibilities occurs. By discarding all the values of i, j not belonging to I, and then renumbering, we see that without loss of generality we may assume

$$\alpha_{i,j} \in S \setminus T \ (1 \leq i < j \leq M_1). \tag{4.12}$$

M_1 is again unspecified, but shortly it will be clear what should we take for M_1.

A similar application of Ramsey's Theorem shows that for any a priori prescribed number $M_2 \geq 1$ there exists $M_1 \geq 1$ such that we can find a set $P \subseteq \{1, \ldots, M_1\}$ of size M_2 such that

$$\beta_{i,j} \in T \ (i < j,\ i, j \in P), \text{or}$$
$$\beta_{i,j} \in S \setminus T \ (i < j,\ i, j \in P).$$

It will be clear shortly what one needs to take for M_2. Again, without loss of generality we may assume that one of the two following cases concerning $\beta_{i,j}$ occurs:

$$\beta_{i,j} \in T \ (1 \leq i < j \leq M_2), \text{or} \tag{4.13}$$
$$\beta_{i,j} \in S \setminus T \ (1 \leq i < j \leq M_2). \tag{4.14}$$

Let us examine each of them in turn.

Suppose first that (4.13) holds. Then we can find large enough $N \in \mathbb{N}$ and $M_2 \geq N$ so as to guarantee, by the Pigeonhole Principle, that there exist i, j $(1 \leq i < j \leq N)$ such that

$$(\alpha_{i,N}, \alpha_{j,N}) \in \mathcal{H}^T \tag{4.15}$$

and write

$$\alpha_{i,N} = a\alpha_{j,N} \ (a \in T). \tag{4.16}$$

Now we have

$$\begin{array}{rcll} u_i & = & \alpha_{i,N} u_N \beta_{i,N} & \text{(by (4.11))} \\ & = & a\alpha_{j,N} u_N \beta_{i,N} & \text{(by (4.16))} \\ & = & a\alpha_{j,N} u_N \beta_{N-1} \dots \beta_j \beta_{j-1} \dots \beta_i & \text{(by (4.10))} \\ & = & a\alpha_{j,N} u_N \beta_{j,N} \beta_{j-1} \dots \beta_i & \text{(by (4.10))} \\ & = & a u_j \beta_{j-1} \dots \beta_i & \text{(by (4.11))} \end{array}$$

This, together with (4.13), contradicts (4.8).

Consider now the situation where (4.14) holds, and let $N \in \mathbb{N}$ and $M_2 \geq N$ be large enough to guarantee the existence of i, j $(1 \leq i < j \leq N)$ such that

$$(\alpha_{i,N}, \alpha_{j,N}), (\beta_{i,N}, \beta_{j,N}) \in \mathcal{H}^T, \tag{4.17}$$

and write

$$\alpha_{i,N} = a\alpha_{j,N}, \ \beta_{i,N} = \beta_{j,N} b \ (a, b \in T). \tag{4.18}$$

Now we have

$$\begin{array}{rcll} u_i & = & \alpha_{i,N} u_N \beta_{i,N} & \text{(by (4.11))} \\ & = & a\alpha_{j,N} u_N \beta_{j,N} b & \text{(by (4.18))} \\ & = & a u_j b & \text{(by (4.11))}, \end{array}$$

again contradicting (4.8). This completes the proof of the theorem. □

4.5 Minimal Conditions for Ideals

Theorem 4.5.1. *Let S be a semigroup and let T be a subsemigroup of S with finite Green index. Then T has $\min_R$ if and only if S has $\min_R$.*

Proof. Obviously without loss of generality we may assume that S has an identity 1 and $1 \in T$.

($\Rightarrow$) Let T have $\min_R$. Assume that S does not have $\min_R$. Then there exists an infinite chain $R^S_{x_1} > R^S_{x_2} > R^S_{x_3} > \cdots$ where $x_i \in S$.

If there are infinitely many elements from $S \setminus T$ among $x_1, x_2, \ldots$, then there exist $i < j$ such that $x_i \mathcal{H}^T x_j$. Then $x_i \mathcal{R}^T x_j$ and so $x_i \mathcal{R}^S x_j$, a contradiction. Hence there are only finitely many i such that $x_i \in S \setminus T$, and without loss of generality we may assume that $x_i \in T$ for all $i \geq 1$. Now, for every $n \geq 1$ there exists $p_n \in S$ such that $x_n p_n = x_{n+1}$. Then $x_1 \cdot p_1 \cdots p_i = x_{i+1}$ for all $i \geq 1$. If $p_1 \cdots p_i \in S \setminus T$ for all $i \geq 1$, then there would exist $i < j$ such that $p_1 \cdots p_i \mathcal{R}^T p_1 \cdots p_j$ and so $x_{i+1} = x_1 p_1 \cdots p_i \mathcal{R}^S x_1 p_1 \cdots p_j = x_{j+1}$, a contradiction. Hence there exists i_1 such that $p_1 \cdots p_{i_1} \in T$. Then $R^T_{x_1} \geq R^T_{x_{i_1+1}}$.

Analogously, there exists $i_2 > i_1$ such that $R^T_{x_{i_1+1}} \geq R^T_{x_{i_2+1}}$. Proceeding in this way, there exists an infinite sequence $i_1 < i_2 < \cdots$ such that $R^T_{x_1} \geq R^T_{x_{i_1+1}} \geq R^T_{x_{i_2+1}} \geq R^T_{x_{i_3+1}} \geq \cdots$. Since every x_i lies in T and T has $\min_R$, we obtain that $R^T_{x_{i_k+1}} = R^T_{x_{i_n+1}}$ for some $k < n$. Then $R^S_{x_{i_k+1}} = R^S_{x_{i_n+1}}$, a contradiction.

($\Leftarrow$) Let S have $\min_R$. Assume that T does not have $\min_R$. Then there exists an infinite chain $R^T_{x_1} > R^T_{x_2} > R^T_{x_3} > \cdots$ where $x_i \in T$. Since $R^S_{x_1} \geq R^S_{x_2} \geq R^S_{x_3} \geq \cdots$, we may assume without loss of generality that $R^S_{x_n} = R^S_{x_{n+1}}$ for all $n \geq 1$. Then for every $n \geq 1$ there exists $q_n \in S$ with $x_{n+1}q_n = x_n$. Now,

$$x_1 = x_2 q_1 = \cdots = x_{n+1} q_n \cdots q_1$$

for all $n \geq 1$. Hence $q_n \cdots q_1 \in S \setminus T$ for all $n \geq 1$. Then there exist numbers $i < j < N$ such that $q_N \cdots q_i \mathcal{H}^T q_N \cdots q_j$. In particular, there exists $t \in T$ with $q_N \cdots q_i = q_N \cdots q_j \cdot t$. Then

$$x_i = x_{N+1} q_N \cdots q_i = x_{N+1} q_N \cdots q_j t = x_j t,$$

a contradiction. $\square$

Now we will prove an analogue of Theorem 4.5.1 for $\min_J$. For this we will require the following lemma.

Lemma 4.5.2. *Let T be a subsemigroup of finite Green index in a semigroup S. Let also $J^S_{x_1} > J^S_{x_2} > J^S_{x_3} > \cdots$ be an infinite chain where $x_i \in T$ for all $i \geq 1$. Then there is a sequence $n_1 < n_2 < n_3 < \cdots$ such that $J^T_{x_{n_1}} \geq J^T_{x_{n_2}} \geq J^T_{x_{n_3}} \geq \cdots$.*

Proof. For each $n \geq 1$ there exist $p_n, q_n \in S$ such that $x_{n+1} = p_n x_n q_n$. Define $p_{i,j} = p_{j-1} \cdots p_i$ and $q_{i,j} = q_i \cdots q_{j-1}$ for all $1 \leq i < j$. Then $x_j = p_{i,j} x_i q_{i,j}$ for all $1 \leq i < j$. We will say that an element $s \in S$ is of the first type if $s \in T$, and is of the second type if $s \in S \setminus T$. By Ramsey's Theorem there exists an infinite subset $I \subseteq \mathbb{N}$ such that all the elements $p_{i,j}$ with $i < j$ and $i, j \in I$ are of the same type, and all the elements $q_{i,j}$ with $i < j$ and $i, j \in I$ are of the same type. By renumbering, without loss of generality we may assume that $I = \mathbb{N}$. If all $p_{i,j}$ and $q_{i,j}$ are of the first type, then $J^T_{x_1} \geq J^T_{x_2} \geq J^T_{x_3} \geq \cdots$ and we are done. Hence either all $p_{i,j}$ are of the second type, or all $q_{i,j}$ are of the second type. Without loss of generality we may assume the former case, i.e. $p_{i,j} \in S \setminus T$ for all $1 \leq i < j$. Now we consider two possible cases:

Case 1: *$q_{i,j} \in T$ for all $1 \leq i < j$.* By Ramsey's Theorem there exists an infinite subset $J \subseteq \mathbb{N}$ such that all the $p_{i,j}$ with $i < j$ and $i, j \in J$ lie in the same $\mathcal{H}^T$-class. Up to renumbering, we may assume that $J = \mathbb{N}$. Then, in

particular, $p_{n+1}p_n\mathcal{H}^T p_n$ for all $n \geq 1$. Hence there exists $t_{n+1} \in T$ such that $p_{n+1}p_n = t_{n+1}p_n$. Then

$$x_{n+2} = p_{n+1}p_n x_n q_n q_{n+1} = t_{n+1}p_n x_n q_n q_{n+1} = t_{n+1}x_{n+1}q_{n+1} \in Tx_{n+1}T$$

for all $n \geq 1$. Therefore $J^T_{x_2} \geq J^T_{x_3} \geq J^T_{x_4} \geq \cdots$.

Case 2: $q_{i,j} \in S \setminus T$ *for all* $1 \leq i < j$. By the Pigeonhole Principle there exist numbers $N < i < j$ such that $p_{N,i}\mathcal{H}^T p_{N,j}$ and $q_{N,i}\mathcal{H}^T q_{N,j}$. Then there exist $t_1, t_2 \in T$ such that $p_{N,i} = t_1 p_{N,j}$ and $q_{N,i} = q_{N,j}t_2$. Then

$$x_i = p_{N,i}x_N q_{N,i} = t_1 p_{N,j}x_N q_{N,j}t_2 = t_1 x_j t_2,$$

and so $J^S_{x_i} = J^S_{x_j}$, a contradiction. □

Theorem 4.5.3. *Let S be a semigroup and let T be a subsemigroup of S with finite Green index. Then T has $\min_J$ if and only if S has $\min_J$.*

Proof. Without loss we may assume that S has an identity 1 and that $1 \in T$.

($\Rightarrow$) Let T have $\min_J$. Assume that S does not have $\min_J$. Then there exists an infinite chain $J^S_{x_1} > J^S_{x_2} > J^S_{x_3} > \cdots$ where $x_i \in S$. As in the proof of Theorem 4.5.1 we may assume that $x_i \in T$ for all $i \geq 1$. By Lemma 4.5.2 there exists a sequence $n_1 < n_2 < n_3 < \cdots$ such that $J^T_{x_{n_1}} \geq J^T_{x_{n_2}} \geq J^T_{x_{n_3}} \geq \cdots$. Therefore $J^T_{x_k} = J^T_{x_n}$ for some $k < n$. Then $J^S_{x_k} = J^S_{x_n}$, a contradiction.

($\Leftarrow$) Let S have $\min_J$. Assume that T does not have $\min_J$. Then there exists an infinite chain $J^T_{x_1} > J^T_{x_2} > J^T_{x_3} > \cdots$ where $x_i \in T$. As in the proof of Theorem 4.5.1 we may assume that $J^S_{x_n} = J^S_{x_{n+1}}$ for all $n \geq 1$. Then for each $n \geq 1$ there exists $p_n, q_n \in S$ such that $x_n = p_n x_{n+1} q_n$. Define $p_{i,j} = p_i \cdots p_{j-1}$ and $q_{i,j} = q_{j-1} \cdots q_i$ for all $1 \leq i < j$. Then $x_i = p_{i,j}x_j q_{i,j}$ for all $1 \leq i < j$. It follows that for every $i < j$, either $p_{i,j} \in S \setminus T$, or $q_{i,j} \in S \setminus T$. By Ramsey's Theorem and up to renumbering, we may assume that $p_{i,j} \in S \setminus T$ for all $i < j$. Furthermore, we may even assume that all of $p_{i,j}$ lie in the same $\mathcal{H}^T$-class.

Take arbitrary $i < j$. Then $p_{i,j}p_j = p_{i,j+1}\mathcal{H}^T p_{j,j+1} = p_j$ and so there exists $t \in T$ such that $p_{i,j}p_j = tp_j$. Then $x_i = p_{i,j}p_j x_{j+1}q_j q_{i,j} = tp_j x_{j+1}q_j q_{i,j} = tx_j q_{i,j}$ and so $q_{i,j} \in S \setminus T$.

Now, by the Pigeonhole Principle there exist numbers $i < j < N$ such that $p_{i,N}\mathcal{H}^T p_{j,N}$ and $q_{i,N}\mathcal{H}^T q_{j,N}$. Therefore there exist $t_1, t_2 \in T$ such that $p_{i,N} = t_1 p_{j,N}$ and $q_{i,N} = q_{j,N}t_2$. Then

$$x_i = p_{i,N}x_N q_{i,N} = t_1 p_{j,N}x_N q_{j,N}t_2 = t_1 x_j t_2,$$

a contradiction. This proves the theorem. □

Proposition 4.5.4. *Let T be a subsemigroup of finite Green index in a semigroup S. If T has a minimal ideal, then S has a minimal ideal.*

Proof. Let I be a minimal ideal in T and assume that S does not have a minimal ideal. Take any $x \in I$. Then there exists an infinite chain $J_x^S > J_{x_1}^S > J_{x_2}^S > \cdots$ where $x_i \in S$. As in the proof of Theorem 4.5.3 we may assume that $x_i \in T$ for all T. Now, $J_{x_1}^T \geq J_x^T$ and so $J_{x_1}^S = J_x^S$, a contradiction. □

4.6 π-regularity

We close the chapter by discussing one more important finiteness condition, this time not related to ideals.

Definition 4.6.1. A semigroup S is π-regular if for every $s \in S$ there exists $n \in \mathbb{N}$ such that s^n is a regular element of S.

π-regular semigroups are important as they generalise the regular semigroups, and cover a big class of non-regular semigroups with behaviour similar to that of the regular semigroups.

Theorem 4.6.2. *Let S be a semigroup and let T be a subsemigroup with finite Green index. Then S is π-regular if and only if T is π-regular.*

Proof. Suppose that T is π-regular and let $s \in S$ be arbitrary. If $s^m \in T$ for some $m \in \mathbb{N}$ then since T is π-regular, $(s^m)^n = s^{mn}$ is regular in T (and hence also in S) for some $n \in \mathbb{N}$. Otherwise $s^m \notin T$ for all m and since T has finite Green index in S there exist $n, r \in \mathbb{N}$ with $s^{n+r}\mathcal{H}^T s^n$. Then as in the proof of [33, Theorem 18] choosing $z \in \mathbb{N}$ with $0 \leq z \leq r-1$ and $n + z \equiv 0 \pmod{r}$ we have $(s^{n+z})^2 \mathcal{H}^T s^{n+z}$. In particular s^{n+z} is a regular element of S.

For the converse, suppose that S is π-regular and let $t \in T$. Since S is π-regular there exists an infinite subset $I \subseteq \mathbb{N}$ such that t^i is regular in S for all $i \in I$. For each $i \in I$ let s_i be an inverse of t^i in S, so

$$t^i s_i t^i = t^i \quad \& \quad s_i t^i s_i = s_i. \tag{4.19}$$

If $s_i \in T$ for some $i \in I$ then t^i is regular in T and we are done, so suppose otherwise. For all $i \in I$, set $f_i = t^i s_i$ noting that by (4.19), f_i is an idempotent satisfying $f_i \mathcal{R}^S t^i$ and $f_i \mathcal{L}^S s_i$. Since $s_i \in S \setminus T$ for all $i \in I$, and T has finite Green index in S, it follows that there is an infinite subset $J \subseteq I$ such that for all $i, j \in J$ we have $s_i \mathcal{H}^T s_j$. Let $i, j \in J$ be arbitrary, with $i < j$ say. Then

$$f_i \mathcal{L}^S s_i \mathcal{L}^S s_j \mathcal{L}^S f_j$$

and therefore $f_i f_j = f_i$. Since $\mathcal{R}^S$ is a left congruence $t^j \mathcal{R}^S f_j$ implies $f_i t^j \mathcal{R}^S f_i f_j$ and hence

$$t^j = t^i t^{j-i} = t^i s_i t^i t^{j-i} = (t^i s_i) t^j = f_i t^j \mathcal{R}^S f_i f_j = f_i \mathcal{R}^S t^i.$$

By a dual argument $t^j \mathcal{L}^S t^i$ and hence $t^j \mathcal{H}^S t^i$.

Since $i, j \in J$ were arbitrary it follows that $t^k \mathcal{H}^S t^l$ for all $k, l \in J$. By [33, Proposition 10] each $\mathcal{H}^S$-class of S is a union of finitely many $\mathcal{H}^T$-classes. Since J is infinite it follows that there exist $p, q \in J$ with $t^p \mathcal{H}^T t^q$. Now as in the proof of the converse above we can find a number $y \in \mathbb{N}$ with $(t^y)^2 \mathcal{H}^T t^y$, and we conclude that t^y is a regular element of T. $\square$

In view of Theorem 4.6.2 and our previous discussion of the finiteness condition $\mathcal{J} = \mathcal{D}$, the following problem is of great interest:

Question 3. Let T be a subsemigroup in a semigroup S with finite Green index. Let also T or S be π-regular, and $\mathcal{J} = \mathcal{D}$ in S. Is it true then that $\mathcal{J} = \mathcal{D}$ in T?

Chapter 5

Hopficity and Rees Index for Semigroups

In this chapter we prove the following: If a finitely generated semigroup S has a hopfian subsemigroup T of finite Rees index then S is hopfian too. This no longer holds if S is not finitely generated. There exists a finitely generated hopfian semigroup S with a non-hopfian subsemigroup T such that $S \setminus T$ has size 1.

The results of this chapter were obtained in collaboration with Nik Ruškuc and are taken from [60].

5.1 Introduction and the Statement of Main Result

An algebraic structure A is said to be *hopfian* if no proper quotient of A is isomorphic to A, or, equivalently, if every surjective endomorphism of A is an automorphism. Hopficity is clearly a finiteness condition (i.e. all finite algebraic structures are hopfian), and so the question arises of its preservation under substructures that are in some sense 'large', or extensions that are in some sense 'small'.

The property was introduced by Hopf [44] who asked if every finitely generated group was hopfian. The group defined by $\mathrm{Gp}\langle a, b : a^{-1}b^2a = b^3\rangle$ is an easy (but not the first) counter-example; see [7]. In the same paper the authors show that the group $\mathrm{Gp}\langle a, b : a^{-1}b^{12}a = b^{18}\rangle$ is hopfian, but contains a normal non-hopfian subgroup of index 6. In particular, hopficity is not preserved by subgroups of finite index, even in the finitely generated case. By way of contrast, Hirshon [41] proved that if H is a hopfian subgroup of finite index in a finitely generated group G, then G is hopfian as well. To the best of our knowledge, it is still open if the same statement holds without finite generation assumption.

The purpose of this chapter is to demonstrate that the situation in semigroups with respect to finite Rees index is analogous to the above de-

scribed situation for groups with respect to the group-theoretic index.

Here we prove that, provided the semigroup is finitely generated, hopficity is preserved by finite Rees index extensions:

Theorem 5.1.1. *Let S be a finitely generated semigroup, and let T be a subsemigroup with $S \setminus T$ finite. If T is hopfian then S is hopfian as well.*

Accompanying Theorem 5.1.1 are two examples, establishing the following:

- if finite generation assumption is removed, Theorem 5.1.1 no longer holds; and
- hopficity is not inherited by finite Rees index subsemigroups, even in the finitely generated case.

Theorem 5.1.1 is proved in Section 5.4, although the brunt of the work is in proving a result concerning finite Rees index and endomorphisms in Section 5.3. The accompanying examples are exhibited before and after the proof, in Sections 5.2 and 5.5 respectively. The final section contains some further commentary and open problems.

5.2 An Introductory Example

The purpose of this section is to show that, without adding the finite generation assumption, hopficity is not preserved by either finite Rees index extensions or subsemigroups.

We begin by defining a family of isomorphic semigroups $T_i = \langle b_i : b_i^2 = b_i^4 \rangle$, $i \in \mathbb{N}$. Form their union $T = \bigcup_{i \in \mathbb{N}} T_i$, and extend the multiplication defined on each T_i to a multiplication on the whole of T by letting $xy = yx = y$ for any $x \in T_i$, $y \in T_j$, $i < j$. It is easy to see that this turns T into a semigroup.

Further, let F be the semigroup $\langle a : a^5 = a^2 \rangle$, let $S = T \cup F$, and extend the multiplication on T and F to a multiplication on the whole of S by $xy = yx = y$ for $x \in F$, $y \in T$. Again, this turns S into a semigroup. Finally, let S^1 be the semigroup S with an identity adjoined to it. Clearly we have $T \leq T^1 \leq S^1$, a sequence of finite Rees index extensions.

Proposition 5.2.1. *The semigroups S^1 and T are hopfian, while the semigroup T^1 is not. Hence, hopficity is preserved by neither finite Rees index extensions nor subsemigroups*

Proof. *T is hopfian.* Let $\phi : T \to T$ be a surjective endomorphism. Since b_1 is the only indecomposable element of T (in the sense that it cannot be written as a product of any two elements of T), we must have $b_1\phi^{-1} = \{b_1\}$. In particular $\phi\restriction_{T_1}$ is the identity mapping. The set of elements on which b_1 acts trivially (meaning $b_1x = xb_1 = x$) is precisely $T \setminus T_1$, so ϕ maps this set onto itself. But clearly $T \setminus T_1$ is a subsemigroup isomorphic to T, and an inductive argument shows that ϕ is in fact the identity mapping. Thus T indeed is hopfian.

T^1 is not hopfian. A routine verification shows that the mapping $b_1 \mapsto 1$, $b_{n+1} \mapsto b_n$ ($n \in \mathbb{N}$) extends to a surjective, non-injective endomorphism of T^1.

S^1 is hopfian. Let $\phi : S^1 \to S^1$ be a surjective endomorphism. Clearly, $1\phi = 1$. Note that a is the only element $x \in S^1$ such that $\langle x \rangle$ is not a group and $x^5 = x^2$. It follows that $a\phi^{-1} = \{a\}$.

Now, assume that for some $i \geq 1$, $b_i\phi \notin T$. Notice that $b_i\phi = (ab_i)\phi = a\phi \cdot (b_i)\phi = a \cdot (b_i)\phi$. Hence $b_i\phi \neq 1$ and in fact $b_i\phi \in F$, i.e. $b_i\phi = a^k$ for some k. Then $a^k = b_i\phi = a \cdot (b_i)\phi = a^{k+1}$, which cannot hold in F. Thus $b_i\phi \in T$ for all $i \geq 1$.

Hence ϕ maps $\langle b_1, b_2, \dots \rangle = T$ onto itself. We have already proved that T is hopfian, and so it follows that ϕ is a bijection, and so S^1 is hopfian, as required. □

5.3 Finite Rees Index and Endomorphisms

The following result will be of crucial importance in the proof of Theorem 5.1.1.

Theorem 5.3.1. *For every endomorphism ϕ of a finitely generated semigroup S and every proper subsemigroup T of finite Rees index we have $T\phi \neq S$.*

Proof. Suppose to the contrary that $T\phi = S$. Let $F = S \setminus T$, a finite set.

Claim 5.3.2. *There exists $N \geq 1$ such that for every $f \in F$ at least one of the following holds: $f\phi^{tN} \in T$ for all $t \geq 1$, or $f\phi^N = f\phi^{2N}$.*

Proof. Consider the following two sets:

$$F_\infty = \{f \in F : f\phi^k \in F \text{ for infinitely many } k \geq 1\},$$
$$F_0 = \{f \in F : f\phi^k \in F \text{ for only finitely many } k \geq 1\},$$

which clearly partition F. The following assertions follow easily from finiteness of F: First of all, for every $f \in F_\infty$ its orbit $O(f) = \{f\phi^k : k \geq 0\}$

is finite. Then $O(F_\infty) = \bigcup_{f \in F_\infty} O(f)$ is finite too, and so there exists $p \geq 1$ such that $\phi^p \restriction_{O(F_\infty)}$ is an idempotent. Finally, there exists $q \geq 1$ such that $F_0\phi^k \subseteq T$ for all $k \geq q$. Any number N which is greater than q and is a multiple of p will satisfy the conditions of the claim. $\square$

Let us denote the mapping ϕ^N by π. From the assumption that $T\phi = S$ it follows that $T\pi = S$ as well. For every $k \geq 0$ let

$$A_k = F\pi^{-k}, \tag{5.1}$$

and let

$$B = T \setminus \bigcup_{k \geq 0} A_k = \{t \in T : t\pi^k \in T \text{ for all } k \geq 0\}. \tag{5.2}$$

From (5.2) and $T\pi = S$ it is immediately clear that B is a subsemigroup of T (or possibly empty) and that $B\pi = B$. Furthermore, from Claim 5.3.2 and the definition of π it follows that for every $f \in F$ we have:

$$f\pi \in B \text{ or } f\pi^2 = f\pi \in F. \tag{5.3}$$

From (5.1), (5.2), (5.3) it follows that

$$A_k\pi^l \subseteq B \cup F \ (l \geq k \geq 0). \tag{5.4}$$

We now start using finite generation of S. We remark that by [75, Theorem 1.1] this is equivalent to T being finitely generated.

Claim 5.3.3. *There exists a finite set $Y \subseteq B$ such that the set $Y \cup F$ generates S.*

Proof. Let X be any finite generating set for T. Since X is finite there must exist $k \geq 0$ such that $X \subseteq B \cup A_1 \cup \cdots \cup A_k$. Note that $X \cup F$ generates S. Since π is onto, the set $(X \cup F)\pi^k$ also generates S. But, using (5.4), we have $(X \cup F)\pi^k \subseteq B \cup F$. $\square$

Let $U = \{f \in F : f\pi = f\}$; clearly $U = F \cap F\pi$ by (5.3). Note that

$$(Y \cup F)\pi = Y\pi \cup (T \cap F\pi) \cup (F \cap F\pi) = Z \cup U,$$

where $Z = Y\pi \cup (T \cap F\pi) \subseteq B$. So we have:

Claim 5.3.4. *There exists a finite set $Z \subseteq B$ such that $Z \cup U$ generates S.*

Now let $V = T \cap (U^2 \cup U^3)$.

Claim 5.3.5. *We have $F \cap \langle U \rangle = U$ and $T \cap \langle U \rangle = \langle V \rangle \subseteq B$.*

Proof. For the first assertion, let $f \in F \cap \langle U \rangle$, and write $f = u_1 \cdots u_k$ for some $u_1, \ldots, u_k \in U$. Then

$$f\pi = (u_1\pi) \cdots (u_k\pi) = u_1 \cdots u_k = f$$

and so $f \in U$. Therefore $F \cap \langle U \rangle \subseteq U$, and the converse inclusion is obvious.

For the second assertion, we shall show that if $t \in T \cap \langle U \rangle$, then $t \in \langle V \rangle$ by induction on the length k of an expression $t = u_1 u_2 \cdots u_k$ with $u_1, u_2, \ldots, u_k \in U$. So, let us have a decomposition $t = u_1 \cdots u_k$ with $u_1, \ldots, u_k \in U$. Obviously, $k \geq 2$. The base of induction $k = 2$ and $k = 3$ is immediate: we have $t \in V$ by the definition of V. Suppose now $k \geq 4$ and assume that the induction hypothesis holds for all numbers $< k$. If any of $u_1 u_2$ and $u_3 \cdots u_k$ belongs to F, then it belongs to $F \cap \langle U \rangle = U$ and so we may apply induction hypothesis. Hence we may assume that both $u_1 u_2$ and $u_3 \cdots u_k$ belong to T. Then $u_1 u_2 \in V$ and, by induction, $u_3 \cdots u_k \in \langle V \rangle$, so that $t \in \langle V \rangle$ as well, as required. □

In what follows, as a technical convenience, we will take 1 to denote an identity element adjoined to S, for any set $X \subseteq S$ write $X^1 = X \cup \{1\}$, and adopt the convention that $1\pi = 1$.

Claim 5.3.6. *Let $n \geq 0$ be arbitrary. Every element $s \in S$ can be represented in the form*

$$u_1 w_1 u_2 w_2 \cdots u_k w_k u_{k+1}, \tag{5.5}$$

where $k \geq 0$, $u_1, u_{k+1} \in U^1$, $u_i \in U$ for $i = 2, \ldots, k$, and $w_i \in \langle Z\pi^n \cup V \rangle$ for $i = 1, \ldots, k$.

Proof. First of all note that since $Z \cup U$ is a generating set for S and $U\pi = U$, we have that $Z\pi^n \cup U = (Z \cup U)\pi^n$ is a generating set for S, since π is surjective. By Claim 5.3.5 a product of generators from U of length greater than 1 can be replaced either by a single element from U, or by a product of elements from V. □

Claim 5.3.7. *For any $u_1, u_2 \in U^1$ and $w \in Z \cup V$ there exists $n \geq 1$ such that $u_1(w\pi^k)u_2 \in U \cup B$ for all $k \geq n$.*

Proof. From $F\pi \cap F = U$ and $F\pi \cap T \subseteq B$ it follows that $F\pi \subseteq U \cup B$. Combining this with (5.4), we see that for every $s \in S$ there exists $n \geq 1$ such that $s\pi^k \in B \cup F$ for all $k \geq n$. Applying this to $s = u_1 w u_2$, and remembering that $u\pi^k = u$ for all $u \in U^1$, yields the result. □

Note that since $V \subseteq \langle U \rangle$, every element of V is fixed by π. The sets U^1, Z and V are all finite, and so Claim 5.3.7 implies that there exists $M \geq 1$ such that

$$T \cap \{u_1 w u_2 : u_1, u_2 \in U^1,\ w \in Z\pi^M \cup V\} \subseteq B \tag{5.6}$$

$$F \cap \{u_1 w u_2 : u_1, u_2 \in U^1,\ w \in Z\pi^M \cup V\} \subseteq U. \tag{5.7}$$

Let us now consider an arbitrary element $t \in T$. Write t in the form (5.5) with $w_i \in \langle Z\pi^M \cup V \rangle$. Furthermore, choose this decomposition so that the length of the corresponding product of generators $U \cup V \cup Z\pi^M$ is as short as possible. Consider now an arbitrary w_i, $i = 1, \ldots, k-1$. Suppose that its shortest expression as a product of generators from $Z\pi^M \cup V$ starts with $a \in Z\pi^M \cup V$, and write $w_i = aw_i'$. From (5.6), (5.7) it follows that $u_i a \in U \cup B$. But we cannot have $u_i a \in U$, as that would allow us to shorten the expression for t. Hence $u_i a \in B$, and since $w_i' \in \langle Z\pi^M \cup V \rangle^1 \subseteq B^1$, it follows that $u_i w_i \in B$ for all $i = 1, \ldots, k-1$. A similar argument shows that $u_k w_k u_{k+1} \in B$; one just needs to consider both the first and the last factors of w_k. This implies that $t \in B$, and hence $T = B$. But then $S = T\pi = B\pi = B = T$, a contradiction as T is a proper subsemigroup of S. This completes the proof of Theorem 5.3.1. □

5.4 The Proof of Theorem 5.1.1

Let S be a finitely generated semigroup, and let T be a hopfian subsemigroup of finite index. Suppose $\phi : S \to S$ is a surjective endomorphism of S.

Let $F = S \setminus T$. Since ϕ is onto, for every $k \geq 0$ we must have $T\phi^k \supseteq S \setminus F\phi^k$, and so $T\phi^k$ is a subsemigroup of finite Rees index in S; moreover this index is no more than $|F\phi^k| \leq |F|$. By [76, Corollary 4.5], a finitely generated semigroup has only finitely many subsemigroups of any given finite Rees index. Therefore there exist $k, r \geq 1$ such that $T\phi^k = T\phi^{k+r}$, and hence $T\psi = T\psi^2$, where $\psi = \phi^{(k+1)r}$.

From $T\psi^2 = T\psi$ it follows that $(T \cup T\psi)\psi = T\psi$. Since ψ is onto, we must have

$$(S \setminus (T \cup T\psi))\psi \supseteq S \setminus (T \cup T\psi)\psi = S \setminus T\psi.$$

Now we have

$$|S \setminus T\psi| \geq |S \setminus (T \cup T\psi)| \geq |(S \setminus (T \cup T\psi))\psi| \geq |S \setminus T\psi|,$$

and hence $S \setminus T\psi = S \setminus (T \cup T\psi)$, which in turn implies $T \subseteq T\psi$.

Thus ψ is a surjective endomorphism of $T\psi$, and T is a subsemigroup of finite index mapping onto the whole of $T\psi$. By Theorem 5.3.1, T cannot be a proper subsemigroup, and hence $T = T\psi$. Thus $\psi\restriction_T$ is a surjective endomorphism of T, and, since T is hopfian, $\psi\restriction_T$ is actually an automorphism. Since ψ is a surjection on S and $T\psi = T$, it follows that $F \subseteq F\psi$. So $\psi\restriction_F$ is surjective. Since F is a finite set, $\psi\restriction_F$ is therefore a bijection. Thus ψ as a whole is bijective, and hence so is ϕ since $\psi = \phi^{(k+1)r}$. Theorem 5.1.1 has been proved.

5.5 A Concluding Example

The purpose of this section is to exhibit an example which demonstrates that hopficity is not inherited by passing to finite Rees index subsemigroups, not even in the finitely generated case. This is accomplished in Theorem 5.5.7 at the end of the section.

The construction relies on the notion of S-acts (or actions). All actions will be on the right, and to distinguish them from the semigroup operations we will denote the result of the action of a semigroup element $s \in S$ on an element $x \in X$ by $x \cdot s$. An S-act X can, of course, be viewed as an algebraic structure in its own right, with every $s \in S$ inducing a unary operation $x \mapsto x \cdot s$ on X. Therefore the standard algebraic notions – substructures, homomorphisms, generation, hopficity – are all meaningful in this context. For a systematic introduction into the semigroup actions see for instance [45, Section 8.1].

Our first result is well known, but since we have not been able to locate an explicit example in the literature, we give one here for completeness.

Lemma 5.5.1. *The free semigroup of rank* 3 *admits a cyclic non-hopfian act.*

Proof. Let $F = \langle a, b, c : \varnothing \rangle$ be the free semigroup of rank 3. Consider the action of generators a, b, c on the set

$$X = \{x_i, y_i : i \in \mathbb{Z}\} \cup \{z_i : i \in \mathbb{N}\} \cup \{0\}$$

given by

$$\begin{aligned}
&x_i \cdot a = x_{i+1},\\
&x_i \cdot b = x_{i-1},\\
&x_i \cdot c = y_i,\\
&y_i \cdot a = y_i \cdot b = 0,\\
&y_i \cdot c = \begin{cases} y_i & \text{if } i \leq 0,\\ z_i & \text{if } i > 0,\end{cases}\\
&z_i \cdot a = z_i \cdot b = 0,\\
&z_i \cdot c = z_i,\\
&0 \cdot a = 0 \cdot b = 0 \cdot c = 0.
\end{aligned}$$

This action is shown in Figure 5.1. Since F is free on a, b, c, this action extends to a unique action of F on X. Clearly, this action is generated by x_0 (or, indeed, any x_i).

Let $\psi : X \to X$ be defined by

$$\begin{aligned}
&x_i\psi = x_{i-1},\\
&y_i\psi = y_{i-1},\\
&z_1\psi = y_0,\\
&z_i\psi = z_{i-1}\ (i > 1),\\
&0\psi = 0.
\end{aligned}$$

Effectively, ψ moves all of x_i, y_i, z_i one to the left, except for z_1 which it maps to y_0, the same as y_1. It is a routine matter to verify that ψ is a surjective, non-injective endomorphism of X. □

Lemma 5.5.2. *Let F be a free semigroup, and let X be a cyclic F-act. Then there exists an F-act Y such that the following hold:*

1. *X is a subact of Y;*
2. *$|Y \setminus X| = 1$;*
3. *Y is hopfian.*

Proof. Suppose that $F = \langle A \mid \rangle$, and suppose X is generated by x_0, i.e. $x_0 \cdot F^1 = X$. Let $Y = X \cup \{y_0\}$, where $y_0 \notin X$. Extend the action of F on X to an action on Y by setting

$$y_0 \cdot a = x_0\ (a \in A).$$

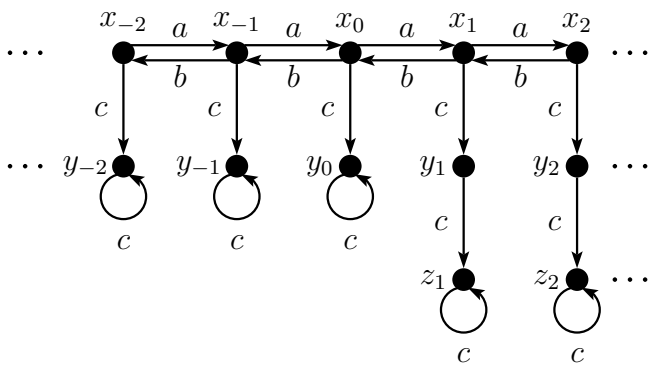

Figure 5.1: A non-hopfian action of F on X. The arrows not shown all point to 0.

Assertions 1 and 2 are clear. To verify that Y is hopfian, let $\psi : Y \to Y$ be any surjective endomorphism. Since $Y \cdot F = X$ (i.e. y_0 is the only element of Y which has no arrows coming into it) it follows that $x\psi \neq y_0$ for all $x \in X$. This, combined with ψ being onto, implies $y_0\psi = y_0$. Since the F-act Y is generated by y_0, it readily follows that ψ must be the identity mapping, and so Y is indeed hopfian. $\square$

We now introduce a semigroup construction that we then use to build our desired example. The ingredients for the construction are a semigroup S and an S-act X (with $S \cap X = \varnothing$). The new semigroup, which we denote by $S[X]$, has the carrier set $S \cup X$; the multiplication in S remains the same, while for $s \in S$, $x, y \in X$ we define

$$sx = x, \; xs = x \cdot s, \; xy = y.$$

It is a routine matter to check that $S[X]$ is indeed a semigroup.

Lemma 5.5.3. *Let S be a semigroup, let X, Y be two S-acts, and let $\psi : X \to Y$ be a homomorphism of S-acts. Define a mapping $\phi : S[X] \to S[Y]$ by $\phi = 1_S \cup \psi$, where 1_S is the identity mapping on S. Then ϕ is a (semigroup) homomorphism. Moreover, ϕ is surjective (respectively injective, bijective) if and only if ψ is surjective (resp. injective, surjective).*

Proof. For $s, t \in S$ and $x, y \in X$ we have

$$\begin{aligned}
&(st)\phi = st = (s\phi)(t\phi),\\
&(sx)\phi = x\phi = x\psi = s(x\psi) = (s\phi)(x\phi),\\
&(xs)\phi = (x \cdot s)\phi = (x \cdot s)\psi = (x\psi) \cdot s = (x\phi)s = (x\phi)(s\phi),\\
&(xy)\phi = y\phi = y\psi = (x\psi)(y\psi) = (x\phi)(y\phi).
\end{aligned}$$

The final three assertions are obvious. □

Lemma 5.5.4. *Let $F = \langle A | \rangle$ be a free semigroup of finite rank, let X be an F-act, and suppose that $\phi : F[X] \to F[X]$ is a surjective endomorphism. Then:*

1. *$\phi\restriction_F$ is an automorphism of F.*
2. *$X\phi = X$.*

Proof. 1 All elements of X are idempotents, while F has no idempotents; hence $X\phi \subseteq X$. Since ϕ is onto it follows that $F \subseteq F\phi$. Now let

$$A_F = \{a \in A : a\phi \in F\},$$
$$A_X = \{a \in A : a\phi \in X\}.$$

Since X is an ideal of $F[X]$, it follows that $(F^1 A_X F^1)\phi \subseteq X$. Again, since ϕ is onto we must have $\langle A_F \rangle \phi = F$. But $\langle A_F \rangle$ is a free subsemigroup of F of rank $|A_F|$. Since A is finite it follows that $A_F = A$ and $A_X = \varnothing$. Hence $\phi\restriction_F$ is a surjective endomorphism of F, and indeed an automorphism since F is hopfian.

2 We have already proved $X\phi \subseteq X$. The assertion now follows from $F\phi = F$ and ϕ being surjective. □

Lemma 5.5.5. *Let F be a free semigroup of finite rank, and let X be an F-act. Suppose $\phi : F[X] \to F[X]$ is a surjective endomorphism with $\phi\restriction_F = 1_F$. Then $\phi\restriction_X$ is a surjective endomorphism of the F-act X.*

Proof. By Lemma 5.5.4 2 we have that $\phi\restriction_X$ maps X onto itself. Furthermore, for $x \in X$ and $s \in F$, we have

$$(x \cdot s)\phi\restriction_X = (xs)\phi = (x\phi)(s\phi) = (x\phi)s = (x\phi\restriction_X) \cdot s,$$

i.e. $\phi\restriction_X$ is an F-act endomorphism. □

Lemma 5.5.6. *Let F be a free semigroup of finite rank, and let X be an F-act. The semigroup $F[X]$ is hopfian if and only if X is a hopfian F-act.*

Proof. ($\Rightarrow$) Suppose $F[X]$ is hopfian, and let $\psi : X \to X$ be a surjective endomorphism of F-acts. Using Lemma 5.5.3, there is a surjective endomorphism $\phi : F[X] \to F[X]$ such that $\phi\restriction_X = \psi$. Since $F[X]$ is hopfian, ϕ is injective, and hence ψ is injective as well.

($\Leftarrow$) Suppose X is a hopfian F-act, and let $\phi : F[X] \to F[X]$ be a surjective endomorphism. By Lemma 5.5.4, the mapping $\phi\restriction_F$ is an automorphism of F. Since the automorphism group of F is isomorphic to the finite

symmetric group S_r (where r is the rank of F), there exists $n \in \mathbb{N}$ such that $(\phi\restriction_F)^n = 1_F$. By Lemma 5.5.5, applied to the mapping ϕ^n, we have that $(\phi\restriction_X)^n$ is a surjective endomorphism of the F-act X. But X is hopfian, and hence $(\phi\restriction_X)^n$ is injective. It follows that $\phi\restriction_X$, and indeed ϕ itself, are injective, and so $F[X]$ is hopfian. □

Theorem 5.5.7. *There exists a finitely generated hopfian semigroup S which contains a non-hopfian subsemigroup T with $|S \setminus T| = 1$.*

Proof. Let $F = \langle a, b, c \mid \rangle$ be the free semigroup of rank 3, and let X be a cyclic, non-hopfian F-act, guaranteed by Lemma 5.5.1. Extend X to a cyclic hopfian F-act Y with $|Y \setminus X| = 1$, as in Lemma 5.5.2. Let $S = F[Y]$, $T = F[X]$. Clearly, $T \leq S$ and $|S \setminus T| = 1$. By Lemma 5.5.6 we have that S is hopfian, while T is not. Finally, S is finitely generated: indeed $S = \langle a, b, c, y_0 \rangle$, where y_0 is any generator of the F-act Y. □

5.6 Concluding Remarks

If we perform the construction as described in the proof of Theorem 5.5.7, starting from the act exhibited in Lemma 5.5.1 it is relatively easy to see that the resulting semigroups S and T are not finitely presented. The following two examples show that there exists a hopfian semigroup, admitting a finite complete rewriting system, with a non-hopfian subsemigroup of finite Rees index:

Example 5.6.1. The one-relation semigroup $T = \mathrm{Sg}\langle a, b : abab^2ab = b\rangle$ is non-hopfian. To verify this, first note that

$$abab^3 = abab^2 \cdot abab^2ab = abab^2ab \cdot ab^2ab = bab^2ab.$$

It easy to check that the rewriting system $\{abab^2ab \to b, abab^3 \to bab^2ab\}$ is confluent and noetherian and so defines T. Notice that

$$\begin{aligned} a \cdot bab \cdot a \cdot (bab)^2 \cdot a \cdot bab &= abab \cdot abab^2ab \cdot abab \\ &\to abab^2ab \cdot ab \\ &\to bab. \end{aligned}$$

This means that the assignment $a \mapsto a$, $b \mapsto bab$ lifts to an endomorphism ϕ of S. Since $a \cdot bab \cdot bab = b$, the endomorphism is onto. Under ϕ we obviously have $ab^2 \mapsto b$ and so $ab^2a^2b^2 = ab^2 \cdot a \cdot ab^2 \mapsto bab$. But, by our rewriting system, $ab^2a^2b^2 \neq b$ and so ϕ is not bijective.

Example 5.6.2. The semigroup

$$S = \mathrm{Sg}\langle a, b, f : abab^2ab = b,\ fa = ba,\ af = ab,\ fb = bf = f^2 = b^2\rangle$$

is obviously a finite Rees extension of T from the previous example. We will show that S hopfian. Indeed, let ψ be an onto endomorphism of S. Since a and f are the only indecomposables in S, we must have that $\{a, f\}\psi = \{a, f\}$. Let $\vartheta = \psi^2$. Then ϑ is an onto endomorphism of S and $a\vartheta = a$ and $f\vartheta = f$. If $b\vartheta = f$, then $f = afaf^2af = b$, a contradiction. Hence $b\vartheta = w \in T$. Then

$$ab = af = a\vartheta \cdot f\vartheta = (af)\vartheta = (ab)\vartheta = aw.$$

But T is left-cancellative by Adjan's Theorem, and so $w = b$. Thus ϑ is the identity mapping and so ψ is bijective.

Since finite Green index generalises both finite Rees index and finite group index, the only unknown to us question about preservation of hopficity under finite Green index is

Question 4. Is it true that if a finitely generated semigroup S has a hopfian subsemigroup T of finite Green index then S itself must be hopfian?

If the answer is positive, the proof of this fact would most likely incorporate elements of both Hirshon's original argument, and our considerations in Sections 5.3, 5.4.

We close the chapter with the following two open problems:

Question 5. Is hopficity decidable for one relation semigroups (or one relator groups)?

This problem appears to be quite difficult at present. In fact, even the seemingly easier related question of deciding residual finiteness is still open:

Question 6. Is residual finiteness decidable for one relation semigroups (or one relator groups)?

The reader should recall a classical theorem of Malcev [56] (see also [52, Theorem IV.4.10]) that a finitely generated residually finite group (or semigroup) is hopfian, and consult [50] and [77] for some relevant information.

Chapter 6

Word-Hyperbolic Semigroups

In this chapter we prove that any monoid presented by a confluent context-free monadic rewriting system is word-hyperbolic. This result is then applied to answer a question asked by Duncan & Gilman by exhibiting an example of a word-hyperbolic monoid that does not admit a word-hyperbolic structure with uniqueness. The example we provide does not admit a regular language of normal forms with uniqueness.

The results of this chapter were obtained in collaboration with Alan Cain and are taken from [16].

6.1 Introduction

Hyperbolic groups — groups whose Cayley graphs are hyperbolic metric spaces — have grown into one of the most fruitful areas of group theory since the publication of Gromov's seminal paper [37]. The concept of hyperbolicity generalises to semigroups and monoids in more than one way. First, one can consider semigroups and monoids whose Cayley graphs are hyperbolic [12]. Second, one can use Gilman's characterisation of hyperbolic groups using context-free languages [31]. This characterisation says that a group G is hyperbolic if and only if there is a regular language L over some finite generating set for G which represents all the elements of G and such that the language

$$M(L) = \left\{u\#_1 v\#_2 w^{\mathrm{rev}} : u, v, w \in L \wedge uv =_G w\right\}$$

(where w^{rev} denotes the reverse of w) is context-free. The pair $(L, M(L))$ is called a *word-hyperbolic structure*. Duncan & Gilman [24] pointed out that this characterisation generalises naturally to semigroups and monoids. The geometric generalisation gives rise to the notion of *hyperbolic* semigroup; the linguistic one to the notion of *word-hyperbolic* semigroups. While

the two notions are equivalent for groups [24, Corollary 4.3], they are not equivalent for general semigroups. This chapter is concerned with *word-hyperbolic* semigroups:

Definition 6.1.1. A *word-hyperbolic structure* for a semigroup S is a pair $(L, M(L))$, where L is a regular language over a finite generating set A for S such that L maps onto S, and where

$$M(L) = \{u\#_1 v\#_2 w^{\mathrm{rev}} : u, v, w \in L \wedge uv =_S w\}$$

is context-free. The pair $(L, M(L)$ is a *word-hyperbolic structure with uniqueness* if L maps bijectively onto S; that is, if every element of S has a unique representative in L. A semigroup is *word-hyperbolic* if it admits a word-hyperbolic structure.

Duncan & Gilman [24, Question 2] asked whether every word-hyperbolic monoid admits a word-hyperbolic structure with uniqueness. The main goal of this chapter is to give a negative answer to this question; see Example 6.3.2. En route, however, a result of independent interest is proven: any monoid presented by a confluent context-free monadic rewriting system is word-hyperbolic – Theorem 6.2.1.

Before we start proving our main results, let us show that every hyperbolic *group* admits a word-hyperbolic structure with uniqueness: If $(L, M(L))$ is a word-hyperbolic structure for a group G, then the fellow-traveller property is satisfied [24, Theorem 4.2] and so L forms part of an automatic structure for G [25, Theorem 2.3.5]. Therefore there exists an automatic structure with uniqueness for G, where the language of representatives L' is a subset of L [25, Theorem 2.5.1]. Hence $(L', M(L) \cap L'\#_1 L'\#_2 (L')^{\mathrm{rev}})$ is a word-hyperbolic structure with uniqueness for G.

6.2 Monoids Presented by Confluent Context-Free Monadic Rewriting Systems

Recall that a special or monadic rewriting system (A, R) is *context-free* if, for each $a \in A \cup \{1\}$ (where 1 stands for the empty word), the set of all left-hand sides of rules in R with right-hand side a is a context-free language.

Theorem 6.2.1. *Let (A, R) be a confluent context-free monadic rewriting system. Then $(A^*, M(A^*))$ is a word-hyperbolic structure for $\mathrm{Mon}\langle A : R\rangle$.*

Proof. Let $M = \mathrm{Mon}\langle A : R\rangle$ and define

$$K = \{u\#_2 v^{\mathrm{rev}} : u, v \in A^*, u =_M v\}.$$

Let $\phi : (A \cup \{\#_1, \#_2\})^* \to (A \cup \{\#_2\})^*$ be the homomorphism extending

$$\#_1 \mapsto 1, \quad \#_2 \mapsto \#_2, \quad a \mapsto a \text{ for all } a \in A.$$

Then $M(A^*) = K\phi^{-1} \cap A^*\#_1A^*\#_2A^*$. Since the class of context-free languages is closed under taking inverse homomorphisms, to prove that $M(A^*)$ is context-free it suffices to prove that K is context-free.

For each $a \in A \cup \{1\}$, let $\$_a$ and $\tilde{\$}_a$ be new symbols. Let

$$\$_{A\cup\{1\}} = \{\$_a : a \in A \cup \{1\}\} \qquad \$_A = \{\$_a : a \in A\},$$
$$\tilde{\$}_{A\cup\{1\}} = \{\tilde{\$}_a : a \in A \cup \{1\}\} \qquad \tilde{\$}_A = \{\tilde{\$}_a : a \in A\},$$

and for any word $w = w_1 \cdots w_n$ with $w_i \in A$, let $\$_w$ and $\tilde{\$}_w$ be abbreviations for $\$_{w_1} \cdots \$_{w_n}$ and $\tilde{\$}_{w_1} \cdots \tilde{\$}_{w_n}$ respectively.

For each $a \in A \cup \{1\}$, let $\Gamma_a = (N_a, A, P_a, O_a)$ be a context-free grammar such that $L(\Gamma_a)$ is the set of left-hand sides of rewriting rules in R whose right-hand side is a. Since R is length-reducing, no $L(\Gamma_a)$ contains 1. Therefore assume without loss of generality that no Γ_a contains a production whose right-hand side is 1 [43, Theorem 4.3].

Modify each Γ_a by replacing each appearance of a terminal letter $b \in A$ in a production by $\$_b$; the grammar $\Gamma'_a = (N'_a, \$_{A\cup\{1\}}, P'_a, O'_a)$ thus formed has the property that $w \in L(\Gamma_a)$ if and only if $\$_w \in L(\Gamma'_a)$. Modify each Γ_a by reversing the right-hand side of every production in P_a and by replacing each appearance of a terminal letter $b \in A$ in a production by $\tilde{\$}_b$; the grammar $\Gamma''_a = (N''_a, \$_{A\cup\{1\}}, P''_a, O''_a)$ thus produced has the property that $w \in L(\Gamma_a)$ if and only if $\tilde{\$}_{w^{\mathrm{rev}}} \in L(\Gamma''_a)$.

The language

$$\{\$_p\#_2\tilde{\$}_{p^{\mathrm{rev}}} : p \in A^*\}$$

is clearly context-free. (Notice that $\$_p$ can either be an abbreviation for a non-empty word $\$_{p_1} \cdots \$_{p_k}$ or the single letter $\$_1$, and similarly for $\tilde{\$}_{p^{\mathrm{rev}}}$.) Let $\Delta = (N_\Delta, \$_{A\cup\{1\}} \cup \tilde{\$}_{A\cup\{1\}} \cup \{\#_2\}, P_\Delta, O_\Delta)$ be a context-free grammar defining this language. Assume without loss of generality that the various non-terminal alphabets N'_a, N''_a and N_Δ are pairwise disjoint.

Define a new context-free grammar $\Theta = (N_\Theta, A \cup \{\#_2\}, P_\Theta, O_\Delta)$ by letting

$$N_\Theta = N_\Delta \cup \$_{A\cup\{1\}} \cup \tilde{\$}_{A\cup\{1\}} \cup \bigcup_{a\in A\cup\{1\}} (N'_a \cup N''_a),$$

and

$$P_\Theta = P_\Delta \cup \Big[\bigcup_{a \in A \cup \{1\}} (P'_a \cup P''_a) \Big]$$

$$\cup \big\{ \$_a \to \$_a \$_1, \$_a \to \$_1 \$_a, \tilde{\$}_a \to \tilde{\$}_a \tilde{\$}_1, \tilde{\$}_a \to \tilde{\$}_1 \tilde{\$}_a : a \in A \cup \{1\} \big\} \tag{6.1}$$

$$\cup \big\{ \$_a \to O'_a, \tilde{\$}_a \to O''_a : a \in A \cup \{1\} \big\} \tag{6.2}$$

$$\cup \big\{ \$_a \to a, \tilde{\$}_a \to a : a \in A \cup \{1\} \big\}. \tag{6.3}$$

Notice that elements of $\$_{A \cup \{1\}}$ now play the rôle of non-terminals, while in the various grammars Γ'_a and Γ''_a, they were terminals. Notice further that the start symbol of Θ is O_Δ.

The aim is now to show that $L(\Theta) = K$.

Lemma 6.2.2. *If $w \in L(\Theta)$, then $w = u\#_2 v^{\mathrm{rev}}$ for some $u, v \in A^*$, and there exists some $p \in A^*$ such that $\$_p \Rightarrow_\Theta^* u$ and $\tilde{\$}_{p^{\mathrm{rev}}} \Rightarrow_\Theta^* v^{\mathrm{rev}}$.*

Proof. Let $w \in L(\Theta)$. Then $O_\Delta \Rightarrow_\Theta^* w$, and the first production applied is from P_Δ. Since no production in $P_\Theta - P_\Delta$ introduces a non-terminal symbol from N_Δ, assume that all productions from P_Δ in the derivation of w are carried out first, before any productions from $P_\Theta - P_\Delta$. This shows that there is some word $q \in L(\Delta)$ such that $O_\Delta \Rightarrow_\Theta^* q \Rightarrow_\Theta^* w$. By the definition of Δ, it follows that $q = \$_p \#_2 \tilde{\$}_{p^{\mathrm{rev}}}$ with

$$O_\Delta \Rightarrow_\Theta^* \$_p \#_2 \tilde{\$}_{p^{\mathrm{rev}}} \Rightarrow_\Theta^* w.$$

Since symbols from $\$_{A \cup \{1\}} \cup \tilde{\$}_{A \cup \{1\}}$ can ultimately only derive symbols from A (and not the symbol $\#_2$), it follows that there exist $u, v \in A^*$ with $\$_p \Rightarrow_\Theta^* u$ and $\tilde{\$}_{p^{\mathrm{rev}}} \Rightarrow_\Theta^* v^{\mathrm{rev}}$ such that $w = u\#_2 v^{\mathrm{rev}}$. □

Lemma 6.2.3. *Let $w, u \in A^*$. If $w \to_R^* u$, then $\$_u \Rightarrow_\Theta^* \$_w$.*

Proof. Suppose

$$w = w_0 \to_R w_1 \to_R w_2 \to_R \ldots \to_R w_n = u$$

is a sequence of rewriting of minimal length from w to u.

Proceed by induction on n. If $n = 0$, it follows that $w = u$ and there is nothing to prove. So suppose $n > 0$ and that the result holds for all shorter such minimal-length rewriting sequences. Then $w_0 \to_R w_1$, and so $w_0 = x\ell y$ and $w_1 = xay$ for some $x, y \in A^*$, $a \in A \cup \{1\}$, and $(\ell, a) \in R$. So

$\ell \in L(\Gamma_a)$. Hence, first applying a production of type (6.2), the construction of Γ'_a and the inclusion of all its productions in Θ shows that

$$\$_a \Rightarrow_\Theta O'_a \Rightarrow^*_\Theta \$_\ell. \tag{6.4}$$

By the induction hypotheses, $\$_u \Rightarrow^*_\Theta \$_{w_1}$. Now consider the cases $a \in A$ and $a = 1$ separately:

1. $a \in A$. Then $\$_{w_1} = \$_x\$_a\$_y$ and so

$$\begin{aligned}
\$_u &\Rightarrow^*_\Theta \$_{w_1} && \text{(by the induction hypothesis)}\\
&= \$_x\$_a\$_y\\
&\Rightarrow^*_\Theta \$_x\$_\ell\$_y && \text{(by (6.4))}\\
&= \$_{w_0}\\
&= \$_w.
\end{aligned}$$

2. $a = 1$. Then $\$_{w_1} = \$_x\$_y$ and so by (6.4),

$$\begin{aligned}
\$_u &\Rightarrow^*_\Theta \$_{w_1} && \text{(by the induction hypothesis)}\\
&= \$_x\$_y\\
&\Rightarrow_\Theta \$_x\$_a\$_y && \text{(by (6.1))}\\
&\Rightarrow^*_\Theta \$_x\$_\ell\$_y && \text{(by (6.4))}\\
&= \$_{w_0}\\
&= \$_w.
\end{aligned}$$

This completes the proof. □

Lemma 6.2.4. *Let $u, w \in A^*$. If $\$_u \Rightarrow^*_\Theta \$_w$, then $w \to^*_R u$.*

Proof. The strategy is to proceed by induction on the number n of productions of type (6.1) or (6.2) in the minimal-length derivation of $\$_w$ from $\$_u$.

Suppose such a minimal length derivation involves a production $\$_1 \to 1$ (of type (6.3)). If this symbol $\$_1$ is introduced by a production of type (6.1), then the derivation would not be of minimal length. So this symbol $\$_1$ must be present in $\$_u$, which, by the definition of the abbreviation $\$_u$ requires $u = 1$. But this would mean that the derivation produced 1, which contradicts the hypothesis of the lemma. So the derivation does not involve productions $\$_1 \to 1$.

The only productions where symbols from $\$_{A\cup\{1\}}$ appear on the left-hand side are of types (6.1), (6.2), and (6.3). Since there are no productions $\$_1 \to 1$, any production of type (6.3) would produce a terminal symbol,

which is impossible. So the first production applied in the derivation sequence must be of type (6.1) or (6.2).

Recall that n is the number of productions of type (6.1) or (6.2) in the minimal-length derivation of $\$_w$ from $\$_u$.

Suppose first that $n = 0$. Then, since the first production cannot be of type (6.3) or from $P_\Delta \cup \left[\bigcup_{a \in A \cup \{1\}} (P'_a \cup P''_a)\right]$, there is no possible first production and thus $\$_w = \$_u$, which entails $w = u$ and so there is nothing to prove.

Suppose now that $n > 0$ and that the result holds for all shorter such minimal-length derivations. Consider cases separately depending on the whether the first production applied in the derivation is of type (6.1) or (6.2).:

1. Type (6.1). So $\$_u = \$_x\$_y \Rightarrow_\Theta \$_x\$_1\$_y$ for some $x, y \in A^*$ with $xy = u$. The symbol $\$_1$ thus produced does not derive 1 since no production $\$_1 \to 1$ is involved. So $\$_x \Rightarrow^*_\Theta \$_{w'}$, $\$_1 \Rightarrow^*_\Theta \$_{w''}$, $\$_y \Rightarrow^*_\Theta \$_{w'''}$, where $w = w'w''w'''$, $w', w''' \in A^*$ and $w'' \in A^+$ and all three of these derivations involve fewer than n productions of type (6.1) or (6.2). By the induction hypothesis, $w' \to^*_R x$, $w'' \to^*_R 1$, and $w''' \to^*_R y$, and thus $w = w'w''w''' \to^*_R xy = u$.

2. Type (6.2). So $\$_u = \$_x\$_a\$_y \Rightarrow_\Theta \$_x O'_a \$_y$ for some $x, y \in A^*$ with $xay = u$. Now, O'_a is the start symbol of Γ'_a, and $L(\Gamma'_a)$ consists of words of the form $\$_\ell$ where $\ell \to_R a$. Thus

$$\$_u \Rightarrow_\Theta \$_x O'_a \$_y \Rightarrow^*_\Theta \$_x\$_\ell\$_y \Rightarrow^*_\Theta \$_w.$$

Thus $\$_x \Rightarrow^*_\Theta \$_{w'}$, $\$_\ell \Rightarrow^*_\Theta \$_{w''}$, and $\$_y \Rightarrow^*_\Theta \$_{w'''}$, where $w', w'', w''' \in A^*$ are such that $w = w'w''w'''$, and each of these derivation sequences involve fewer than n productions of type (6.1) or (6.2). Hence by the induction hypothesis, $w' \to^*_R x$, $w'' \to^*_R \ell$, and $w''' \to^*_R y$. Therefore

$$w = w'w''w''' \to^*_R x\ell y \to_R xay = u.$$

This completes the proof. □

Lemma 6.2.5. *For any $u, w \in A^*$, $w \to^*_R u$ if and only if $\$_u \Rightarrow^*_\Theta w$.*

Proof. Suppose $w \to^*_R u$. Then $\$_u \Rightarrow^*_\Theta \$_w$ by Lemma 6.2.3. By $|w|$ applications of productions of type (6.3), $\$_w \Rightarrow^*_\Theta w$. So $\$_u \Rightarrow^*_\Theta w$.

Suppose that $\$_u \Rightarrow^*_\Theta w$. Only productions of type (6.3) have terminals on the right-hand side. So $\$_u \Rightarrow^*_\Theta \$_w \Rightarrow^*_\Theta w$. So by Lemma 6.2.4, $w \to^*_R u$. □

Reasoning symmetric to the proofs of Lemmas 6.2.3, 6.2.4, and 6.2.5 establishes the following result:

Lemma 6.2.6. *For any $u, w \in A^*$, $w \to_R^* u$ if and only if $\tilde{\$}_{u^{\mathrm{rev}}} \Rightarrow_\Theta^* w^{\mathrm{rev}}$.*

Suppose $u\#_2 v^{\mathrm{rev}} \in K$. Then $u, v \in A^*$ and $u =_M v$. Therefore there is a normal form word p with $u \to_R^* p$ and $v \to_R^* p$. So by Lemmas 6.2.5 and 6.2.6, $\$_p \Rightarrow_\Theta^* u$ and $\tilde{\$}_{p^{\mathrm{rev}}} \Rightarrow_\Theta^* v^{\mathrm{rev}}$. Since every production in P_Δ is included in P_Θ, it follows that

$$O_\Delta \Rightarrow_\Theta^* \$_p\#_2\tilde{\$}_{p^{\mathrm{rev}}},$$

whence $O_\Delta \Rightarrow_\Theta^* u\#_2 v^{\mathrm{rev}}$ and so $u\#_2 v^{\mathrm{rev}} \in L(\Theta)$.

Conversely, suppose $w \in L(\Theta)$. By Lemma 6.2.2, there are words $u, v, p \in A^*$ with $w = u\#_2 v^{\mathrm{rev}}$, $\$_p \Rightarrow_\Theta^* u$, and $\tilde{\$}_{p^{\mathrm{rev}}} \Rightarrow_\Theta^* v^{\mathrm{rev}}$. (Notice that p need not be in normal form.) By Lemmas 6.2.5 and 6.2.6, it follows that $u \to_R^* p$ and $v \to_R^* p$. So $u =_M v$ and thus $w = u\#_2 v^{\mathrm{rev}} \in K$.

Hence $L(\Theta) = K$. Thus K and so $M(A^*)$ are context-free. Therefore $(A^*, M(A^*))$ is a word-hyperbolic structure for the monoid M. □

6.3 Word-Hyperbolic Structures with Uniqueness

This section exhibits an example of a word-hyperbolic monoid that does not admit a word-hyperbolic structure with uniqueness.

The following preliminary result, showing that admitting a word-hyperbolic structure with uniqueness is not dependent on the choice of generating set, is needed. The proof is similar to that of the independence of word-hyperbolicity from the choice of generating set [24, Theorem 3.4], but the detail and exposition are different to make clear that uniqueness is preserved. Additionally, the result here also shows that whether one deals with monoid or semigroup generating sets is not a concern.

Proposition 6.3.1. *Let M be a monoid that admits a word-hyperbolic structure with uniqueness over either a semigroup or monoid generating set, and let A be a finite alphabet representing a semigroup or monoid generating set for M. Then there is a language $L \subseteq A^*$ such that $(L, M(L))$ is a word-hyperbolic structure with uniqueness for M.*

Proof. Assume that S admits a word-hyperbolic structure with uniqueness $(K, M(K))$ where K is a regular language over a finite alphabet B. For each $b \in B$, let $u_b \in A^*$ be such that $u_b =_M b$. (If A represents a semigroup generating set, ensure that u_b lies in A^+; this restriction is important only if b is actually the identity.) Let $\mathcal{P} \subseteq B^* \times A^*$ be the rational relation

$$\mathcal{P} = \big(\{(b, u_b) : b \in B\}\big)^*,$$

i.e. the relation consisting of the pairs $(b_1 \cdots b_k, u_{b_1} \cdots u_{b_k})$ for $k \geq 1$ and $b_1, \ldots, b_k \in B$. Notice that if $(v, w) \in \mathcal{P}$, then $v =_M w$.

Let

$$L = K \circ \mathcal{P} = \big\{w \in A^* : (\exists v \in K)((v, w) \in \mathcal{P})\big\};$$

observe that L is a regular language. Notice that, by the definition of $\mathcal{P}$, for each word v in K there is exactly one word $w \in L$ with $(v, w) \in \mathcal{P}$. Since for each $x \in M$ there is exactly one word v in K with $v =_M x$, it follows that there is exactly one word $w \in L$ with $w =_M x$. That is, the language L maps bijectively onto M.

Let Q be the rational relation

$$\mathcal{P}(\#_1, \#_1)\mathcal{P}(\#_2, \#_2)\mathcal{P}^{\mathrm{rev}}.$$

Then $M(L) = M(K) \circ Q$ and so $M(L)$ is a context-free language.

Thus $(L, M(L))$ is a word-hyperbolic structure for S in every case except when S is a monoid, A is a semigroup generating set, and the representative in K of the identity is 1. In this case, let $L_1 = (L - \{1\}) \cup \{e\}$, where $e \in A^+$ represents the identity. Then L_1 is contained in A^+ and maps bijectively onto S. The language $M(L_1)$ is context-free. Indeed, let $e = a_1 \cdots a_p$ where $a_1, \ldots, a_p \in A$. Let $x_1, \ldots, x_p$ be letters not from A and define $\phi : A \cup \{x_1, \ldots, x_p\} \to A$ by $a \mapsto a$ and $x_i \mapsto a_i$ for all $i \leq p$ and $a \in A$. Then ϕ gives rise to a homomorphism from $(A \cup \{x_1, \ldots, x_p\})^*$ to A^* which we will also denote by ϕ. Then the language

$$L_2 = \big[(A + x_1 \cdots x_p)^* \#_1 (A + x_1 \cdots x_p)^* \#_2 (A + x_1 \cdots x_p)^*\big] \cap \phi^{-1}(M(L)),$$

being an intersection of a regular language with a context-free one, is context-free itself. It is easy to see that

$$M(L_1) = \phi(L_2) \cap A^+ \#_1 A^+ \#_2 A^+,$$

and thus $M(L_1)$ is an intersection of a context-free language with a regular language, and thus $M(L_1)$ is indeed context-free. □

Example 6.3.2. Let $A = \{a, b, c, d\}$, $R = \{ab^n c^n d \to 1 : n \geq 1\}$, and $M = \mathrm{Mon}\langle A : R\rangle$. Then M is word-hyperbolic but does not admit a regular language of unique representatives and thus, in particular, does not admit a word-hyperbolic structure with uniqueness.

Proof. Let G be the language of left-hand sides of rewriting rules in R. The language G is context-free, and so (A, R) is a context-free special rewriting system. Two left-hand sides of rewriting rules in R only overlap if they

are exactly equal, and so (A, R) is confluent. Hence, by Theorem 6.2.1, $(A^*, M(A^*))$ is a word-hyperbolic structure for the monoid M. So M is word-hyperbolic. Identify M with the language of normal form words of (A, R).

Suppose for *reductio ad absurdum* that M admits a word-hyperbolic structure with uniqueness. Then, by Proposition 6.3.1, there is a regular language L over A such that $(L, M(L))$ is a word-hyperbolic structure with uniqueness for M. In particular, every element of M has a unique representative in L. Let $\mathcal{A}$ be a finite state automaton recognizing L and let n be the number of states in $\mathcal{A}$.

Now, if $w \in L$ represents $u \in M$, then $w \to_R^* u$: the word u can be obtained from w by replacing subwords lying in G by the empty word, which effectively means deleting subwords that lie in G. Consider this process in reverse: the word w can be obtained from u by inserting words from G.

If a word from G is inserted between two letters of u, call it a *depth*-1 inserted word. If a word from G is inserted between two letters of a depth-k inserted word, it is called a depth-$(k+1)$ inserted word. A word inserted immediately before the first letter or immediately after the last letter of a depth-k inserted word also counts as a depth-k inserted word. See the following example, where for clarity symbols from u are denoted by x:

$$x\,\underbrace{ab\,\overbrace{abbccd}^{\text{depth 2}}\,bccd}_{\text{depth 1}}\,\overbrace{abbccd}^{\text{depth 1}}\,xx\,\overbrace{abbbcccd}^{\text{depth 1}}\,xx.$$

Then it is possible to obtain w from u by performing all depth-1 insertions first, then all depth-2 insertions, and so on until w is reached.

Suppose that, in order to obtain w from u, a word $ab^\alpha c^\alpha d \in G$ is inserted for some $\alpha > n$. Let $w = w'aw''dw'''$, where these distinguished letters a and d are the first and last letters of this inserted word. Notice that $w'' \to_R^* b^\alpha c^\alpha$, since

$$w = w'aw''dw'' \to_R^* w'ab^\alpha c^\alpha dw''' \to_R w'w''' \to_R^* u.$$

(Of course, w'' may or may not contain inserted words of greater depth.) Since α exceeds n, the automaton $\mathcal{A}$ enters the same state immediately after reading two different symbols b of this inserted word, say after reading $w'apb$ and $w'apbqb$. Similarly it enters the same state immediately after reading two different symbols c of this inserted word, say after reading $w'apbqbrc$ and $w'apbqbrcsc$. Therefore by the pumping lemma, w factors as

$w'apbqbrcsctdw'''$ such that

$$w'apb(qb)^i rc(sc)^j tdw''' \in L$$

for all $i, j \in \mathbb{N} \cup \{0\}$, where the subwords p and q consist of letters b (letters of this inserted word) and possibly also inserted words of greater depth, the subwords s and t consist of letters c (letters of this inserted word) and possibly also inserted words of greater depth, and the subword r consists of some letters b followed by some letters c (letters of this inserted word) and possibly also inserted words of greater depth. Thus

$$p \to_R^* b^{\beta_1}, \qquad q \to_R^* b^{\beta_2}, \qquad r \to_R^* b^{\beta_3} c^{\gamma_3}, \qquad s \to_R^* c^{\gamma_2}, \qquad t \to_R^* c^{\gamma_1},$$

where $\beta_1 + \beta_2 + \beta_3 + 2 = \gamma_1 + \gamma_2 + \gamma_3 + 2 = \alpha$. It follows that

$$\begin{aligned} & w'apb(qb)^i rc(sc)^j tdw''' \\ \to_R^* \; & w'ab^{\beta_1} b(b^{\beta_2} b)^i b^{\beta_3} c^{\gamma_3} c(c^{\gamma_2} c)^j c^{\gamma_1} dw''' \\ = \; & w'ab^{\alpha+(\beta_2+1)(i-1)} c^{\alpha+(\gamma_2+1)(j-1)} dw'''. \end{aligned}$$

Set $i = \gamma_2 + 2$ and $j = \beta_2 + 2$ to see that

$$w'apb(qb)^{\gamma_2+2} rc(sc)^{\beta_2+2} tdw''' \in L$$

and

$$\begin{aligned} & w'apb(qb)^{\gamma_2+2} rc(sc)^{\beta_2+2} tdw''' \\ \to_R^* \; & w'ab^{\alpha+(\beta_2+1)(\gamma_2+1)} c^{\alpha+(\gamma_2+1)(\beta_2+1)} dw''' \\ \to_R^* \; & w'w'' \qquad (\text{since } ab^{\alpha+(\beta_2+1)(\gamma_2+1)} c^{\alpha+(\gamma_2+1)(\beta_2+1)} d \in G) \\ \to_R^* \; & u. \end{aligned}$$

So there are two distinct words w and $w'apb(qb)^{\gamma_2+2} rc(sc)^{\beta_2+2} tdw''$ in L representing the same element u of M. This is a contradiction and so shows the falsity of the supposition that the insertion of a word $ab^\alpha c^\alpha d$ with $\alpha > n$ is used in obtaining the representative in L from a normal form word in M.

Let $G' = \{ab^\alpha c^\alpha d : \alpha \leq n\}$. Then obtaining a word $w \in L$ representing $u \in M$ requires inserting only words from $G' \subset G$.

Now suppose that an insertion of depth greater than n^2 is required to obtain w from u. Then w factorizes as $w'apaqdrdw''$, where the first distinguished letter a and second distinguished letter d are the first and last letters of some inserted word of depth k, and the second distinguished letter a and first distinguished letter d are from some inserted word of depth

$\ell > k$, and where the automaton $\mathcal{A}$ enters the same state after reading the two distinguished letters a and enters the same state after reading the two distinguished letters d. (Such a factorization must exist because there are only n^2 possible pairs of states, and there are inserted words of depth exceeding n^2.) Notice that $aqd \to_R^* 1$ and so $apaqdrd \to_R^* aprd \to_R^* 1$. Then, by the pumping lemma,

$$w'apapaqdrdrdw'' \in L,$$

but

$$w'apapaqdrdrdw'' \to_R^* w'apaprdrdw'' \to_R^* w'aprdw'' \to_R^* w'w'' \to_R^* u,$$

and so there are two representatives w and $w'apapaqdrdrdw''$ in L of $u \in M$. This is a contradiction and so shows the falsity of the assumption that insertions of depth greater than n^2 are required to obtain the representative in L of a normal form word in M.

Suppose that, in the process of performing insertions to obtain a representative $w \in L$ for an element $u \in M$, a word $w^{(k)}$ is obtained after the insertions of depth k have been performed. Suppose further that in performing the insertions of depth $k+1$, more than n insertions are made between consecutive letters of $w^{(k)}$ to obtain a word $w^{(k+1)}$. (The reasoning below also applies if $w^{(k)}$ is the empty word, which would require $k = 0$.) Then $w^{(k+1)}$ factors as

$$w^{(k+1)} = v'ab^{\alpha_1}c^{\alpha_1}dab^{\alpha_2}c^{\alpha_2}d \cdots ab^{\alpha_h}c^{\alpha_h}dv'',$$

where $h > n$, and each $ab^{\alpha_i}c^{\alpha_i}d$ is a word from G'. Then w factors as

$$w = w'ap_1dap_2d \cdots ap_hdw'',$$

where $w' \to_R^* v'$, $w'' \to_R^* v''$, and $p_i \to_R^* b^{\alpha_i}c^{\alpha_i}$ for each i. Then $\mathcal{A}$ enters the same state on reading $w'ap_1dap_2d \cdots ap_id$ and $w'ap_1dap_2d \cdots ap_jd$ for some $i < j$. So by the pumping lemma,

$$q = w'ap_1dap_2d \cdots ap_id(ap_{i+1}d \cdots ap_jd)^2ap_{j+1}d \cdots ap_kdw'' \in L.$$

But

$$\begin{aligned}
q = \quad & w'ap_1dap_2d \cdots ap_id(ap_{i+1}d \cdots ap_jd)^2ap_{j+1}d \cdots ap_kdw'' \\
\to_R^* \; & v'ab^{\alpha_1}c^{\alpha_1}dab^{\alpha_2}c^{\alpha_2}d \cdots \\
& \qquad \cdots ab^{\alpha_i}c^{\alpha_i}d(ab^{\alpha_{i+1}}c^{\alpha_{i+1}}d \cdots \\
& \qquad\qquad \cdots ab^{\alpha_j}c^{\alpha_j}d)^2ab^{\alpha_{j+1}}c^{\alpha_{j+1}}d \cdots ab^{\alpha_h}c^{\alpha_h}dv'', \\
\to_R^* \; & v'v'' \\
\to_R^* \; & u,
\end{aligned}$$

and so there are two representatives w and q of the element $u \in M$. This contradicts the uniqueness of representatives in L and shows the falsity of the supposition that more that n insertions between consecutive letters in the process of obtaining a representative in L for an element of M.

Therefore, to sum up: a representative w in L of an element u of M can be obtained by inserting elements of G' to a depth of at most n^2, with at most n consecutive words being inserted between adjacent letters at any stage. Notice that the maximum length of words in G' is $2n+2$. Thus, starting with empty word, the after depth 1 insertions, there are at most $n(2n+2)$ letters; after depth 2 insertions, at most $n^2(2n+2)^2$; and after depth n^2 insertions, at most $h = n^{n^2}(2n+2)^{n^2}$. Similarly, if one starts with a word u and performs insertions to obtain its representative in L, at most h new symbols are inserted between any adjacent pair of letters in u.

Define

$$H = \big\{w \in A^* : |w| \leq h, w \to_R^* 1\big\}.$$

Then, by the observations in the last paragraph, if $u \in M$ with $u = u_1 \cdots u_n$ is represented by $w \in L$, then $w \in Hu_1Hu_2 \cdots Hu_nH$. Define the rational relation

$$\mathcal{P} = \big(\{(a,a) : a \in A\} \cup \{(p,1) : p \in H\}\big)^*.$$

Then, since removing all subwords in H from a word in L yields the word to which it rewrites, it follows that

$$M = (L \circ \mathcal{P}) \cap (A^* - A^*HA^*) = \big\{u \in A^* - A^*HA^* : (\exists w \in L)((w,u) \in \mathcal{P})\big\},$$

and so M, which is the language of normal forms of (A, R), is regular.

However, two words $ab^\alpha c^\beta d$ and $ab^{\alpha'} c^{\beta'} d$ (where $\alpha, \beta, \alpha', \beta' \in \mathbb{N}$) represent the same element of M if and only if $\alpha = \beta$ and $\alpha' = \beta'$, in which case they both represent the identity of M. Thus, since in M the unique representative of the identity is 1, the language $K = ab^*c^*d - M$, which is also regular, consists of precisely those words of the form $ab^\alpha c^\beta d$ that represent the identity. That is, the language K is $\{ab^\alpha c^\alpha d : \alpha \in \mathbb{N}\}$, which is not regular by the pumping lemma. This is a contradiction, and so M does not admit a regular language of unique representatives. $\square$

Chapter 7

Markov Semigroups

In this chapter we will define the natural analog of the notion of 'being Markov' for semigroups; see how it interacts with two specific generalisations of hyperbolicity for semigroups; and investigate how the property of being Markov is preserved under finite Rees and Green indices. The main result we obtain is establishing an example of a monoid with linear Dehn function which does not admit a regular language of normal forms with uniqueness.

The results of this chapter were obtained in collaboration with Alan Cain and are taken from [15].

7.1 Introduction

The notion of Markov groups was introduced by Gromov in his seminal paper [37, § 5.2], and explored further in [30] and in [25]. A group is Markov if it admits a language of unique representatives, with respect to some generating set, that can be described by a Markov grammar. In this context, a Markov grammar is essentially a finite state automaton with one initial state and every state being an accept state. The connection with hyperbolic groups arises because every hyperbolic group admits such a language of *minimal-length* unique representatives. There is also a connection to automatic groups as was explored in [25]. However, it remains an open direction to investigate the connection between Markov semigroups and automatic semigroups.

Let A be a finite generating set for a monoid M. By a *combing* for M over A we will mean simply a language over A which represents all the elements of M. We will say that a combing $L \subseteq A^*$ for M is *with uniqueness* if all the words from L, viewed as elements in M, are pairwise distinct. So, a combing with uniqueness is exactly what we called normal forms before.

For $x \in M$ we will denote by $|x|_A$ the length of any shortest word over A representing x. Now we give our main definition, which we will show in Proposition 7.1.4 below to be equivalent to the original definition:

Definition 7.1.1. Let A be a finite generating set for a monoid M.

1. A *monoid Markov language* for M over A is a regular prefix-closed combing with uniqueness for M over A.

2. The monoid M is *Markov* (as a monoid) if there exists a monoid Markov language for M over some finite generating set.

In the next definition by $+$-prefix-closure we mean the closure with respect to the non-empty prefixes.

Definition 7.1.2. Let A be a finite generating set for a semigroup M.

1. A *semigroup Markov language* for M over A is a regular $+$-prefix-closed combing with uniqueness for M over A.

2. The semigroup M is *Markov* (as a semigroup) if there exists a semigroup Markov language for M over some finite generating set.

The reason for introducing two definitions is the following. When considering monoids it is natural to take the empty word for the representative of the identity. But if trying to introduce the property of being Markov for semigroups, we must in general consider $+$-prefix-closure rather than just prefix-closure. Anyway, for monoids our two definitions do not collide by the following proposition:

Proposition 7.1.3. *A monoid is Markov as a semigroup if and only if it is Markov as a monoid.*

Proof. Suppose that M is Markov as a monoid. Let A be a finite generating set for M such that there is a monoid Markov language L for M over A. Then L is prefix-closed, regular, and contains a unique representative for each element of M. In particular, the identity of M is represented by $1 \in L$. Let e be a new symbol representing the identity for M. Then $K = (L - \{1\}) \cup \{e\}$ is $+$-prefix-closed, regular, and contains a unique representative for every element of M. Hence K is a semigroup Markov language for M and thus M is Markov as a semigroup.

Suppose now that M is Markov as a semigroup. Let A be a finite semigroup generating set for M such that there is a semigroup Markov language L for M over A. Let w be the unique word in L representing the identity of M. Let

$$K = \big(L - wA^*\big) \cup \{u \in A^* : wu \in L\}.$$

Since L is $+$-prefix-closed and wA^* is closed under concatenation on the right, $L - wA^*$ is also $+$-prefix closed. Furthermore, $\{u \in A^* : wu \in L\}$ is prefix-closed. (Notice that this set contains 1 since w lies in L.) So K is prefix-closed. Moreover, wu and u represent the same element of M for any $u \in A^*$, so $\{u \in A^* : wu \in L\}$ consists of unique representatives for exactly those elements of M whose representatives in L have w as a prefix. Hence every element of M has a unique representative in K. Finally, notice that K is regular. Thus K is a monoid Markov language for M and so M is Markov. □

The following result shows the connection between the definitions of Markov languages and Markov grammars as used by Ghys & de la Harpe [30].

Proposition 7.1.4. *A regular language is prefix-closed if and only if it is recognized by a finite state automaton in which every state is an accept state.*

Proof. Suppose L is prefix-closed and let $\mathcal{A}$ be a trim deterministic finite state automaton recognizing L. Let q be some state of $\mathcal{A}$. Since $\mathcal{A}$ is trim, q lies on a path from the initial state to an accept state. Let w be the label on such a path, with w' being the label before the first visit to q. Then w', being a prefix of w, also lies in L. Since $\mathcal{A}$ is deterministic, there is only one path starting at the initial state labelled by w', and this path ends at q. Since $w' \in L$, it follows that q is an accept state. Therefore, since q was arbitrary, every state of $\mathcal{A}$ is an accept state.

Suppose that L is accepted by an automaton $\mathcal{A}$ in which every state is an accept state. Let $w \in L$ and let w' be some prefix of w. Then w labels a path starting at the initial state of $\mathcal{A}$ and leading to an accept state. The prefix w' labels an initial segment of this path, ending at a state q, which, by hypothesis, is also an accept state. Thus $w' \in L$. Since $w \in L$ was arbitrary, L is prefix-closed. □

7.2 'Being Markov' vs. Hyperbolicity

As we noted above, every hyperbolic group is Markov. The following definitions of hyperbolicity for groups are equivalent: admitting a word-hyperbolic structure and having linear Dehn function. In this section we will show that neither word-hyperbolicity nor having linear Dehn function for monoids implies even being Markov.

Example 7.2.1. As we proved in Chapter 6, the monoid

$$\mathrm{Mon}\langle a, b, c, d : ab^n c^n d = 1 \quad n \geq 1\rangle$$

is word-hyperbolic. But it also does not admit a regular combing with uniqueness, so it is non-Markov.

Recall that for a finitely presented monoid $M = \mathrm{Mon}\langle A : R\rangle$, the *Dehn function* $\mathbf{D}_n(M) = \mathbf{D}_n(M; A, R)$ is defined as follows. For two words $u, v \in A^*$ such that $u =_M v$ we let $d(u, v)$ be the least number of relations from R needed to be applied in the derivation from u to v. Then

$$\mathbf{D}_n(M) = \sup\{d(u, v) : u, v \in A^*,\ |u|, |v| \leq n,\ u =_M v\}.$$

It is easy to see that the growth rate (in terms of n) of the Dehn function does not depend on the finite presentation we choose for M.

Unfortunately, the Dehn functions of finitely presented monoids behave somewhat differently relative to the Dehn functions of finitely presented groups. For instance, there exists a monoid with linear Dehn function which does not admit a finite complete rewriting system, let alone a finite confluent length-reducing system, see [69]. In the same work [69] there is also an example of an automatic monoid with exponential Dehn function.

Our next example is inspired by the monoid $\mathrm{Mon}\langle a, b, c : ba = ab,\ bc = aca,\ ac^2 = 0\rangle$ from [69], which was shown not to admit a regular combing with uniqueness. This monoid is also of intermediate growth (faster than any polynomial and slower than any exponential) and has quadratic Dehn function. A slight modification of this monoid remains non-Markov and has linear Dehn function.

Our next examples relies on the following observation, proof of which follows the same lines as in that of Proposition 6.3.1:

Proposition 7.2.2. *Let S be a semigroup that admits a regular combing with uniqueness over some finite generating set. Then for every finite generating set A for S, S admits a regular combing with uniqueness over A.*

Example 7.2.3. $M = \mathrm{Mon}\langle a, b, c : ba = a^2b,\ bc = aca,\ ac^2 = 0\rangle$ has linear Dehn function and does not admit a regular combing with uniqueness. In particular, M is not Markov.

Proof. Notice that $ba^n = a^{2n}b$ for all $n \geq 1$ and so

$$\begin{aligned} a^{2^{n+1}-1}ca^nc &= a^{2^{n+1}-2}bca^{n-1}c \\ &= ba^{2^n-1}ca^{n-1}c \\ &= \cdots \\ &= b^nac^2 \\ &= 0 \end{aligned}$$

for all $n \geq 0$. Moreover, the number of defining relations we used in this derivation is

$$(1+2^n-1)+(1+2^{n-1}-1)+\cdots+(1+2^1-1)+1+1 = 2^n+\cdots+2^2+2+2 = 2^{n+1}$$

which is less than the length of the word $a^{2^{n+1}-1}ca^nc$.

Next, it is routine to check that the system

$$\{ba \to a^2b,\ bc \to aca,\ a^{2^{n+1}-1}ca^nc \to 0 \quad n \geq 0\}$$

is confluent and noetherian. Of course this system defines M. We start proving that $\mathbf{D}_n(M)$ is linear. For this we will need the following two technical lemmas:

Lemma 7.2.4. *Let f be the function defined on the tuples of non-negative integers recursively by*

$$f(d_k, \cdots, d_1) = 2f(d_{k-1}, \cdots, d_1) + 2d_k + 1, \quad f(d) = 2d + 1.$$

Then $ba^{d_k} \cdots ba^{d_1}c \to^* a^{f(d_k,\cdots,d_1)}ca^k$.

Proof. Follows from induction and the observation that $ba^dc \to^* a^{2d}bc \to a^{2d+1}ca$. □

Lemma 7.2.5. *The analytic expression for the function f is*

$$f(d_k, \cdots, d_1) = 2d_k + 2^2d_{k-1} + \cdots + 2^kd_1 + 2^k - 1.$$

Proof. Follows directly by induction. □

Part 1: M has linear Dehn function.

Case 1: rewriting a word equal to zero to 0. Let $w \in \{a, b, c, 0\}^*$ be such that $w = 0$ in M. If 0 is present in w, then there is a derivation from w to 0, using at most $|w|$ defining relations. So let $w \in \{a, b, c\}^*$. Now, keep applying the rewrite of a^2b to ba (note that this process reverses the rewriting rule $ba \to a^2b$ from our system) as much as possible. If in the process we get a word with a subword of the form $a^{2^{n+1}-1}ca^nc$, then w can be rewritten to 0 using at most $|w| + |w| = 2|w|$ defining relations, where the first summand $|w|$ estimates from above the number of moves from a^2b to ba, and the second summand $|w|$ estimates from above the number of relations needed to rewrite $a^{2^{n+1}-1}ca^nc$ to 0. Indeed, as we noted above, for this is needed at most $2^{n+1} \leq |w|$ defining relations.

So, suppose that w in the process of the rewrite from the previous paragraph is transformed to a word w'. First of all, $|w'| \leq |w|$. Secondly, w' does not contain subwords of the form a^2b. If w' contains a subword of the form $a^{2^{n+1}-1}ca^nc$, then as above, there is a derivation from w to 0 which uses $\leq 2|w|$ defining relations. Hence we may assume that w' does not contain such subwords. Since $w' = 0$ in the monoid, there exists a derivation using our rewriting system: $w' \to^* 0$. In this derivation there must exist *the first step* when there appears a subword of the type $a^{2^{n+1}-1}ca^nc$:

$$w' \to^* \alpha a^{2^{n+1}-1}ca^nc\beta \to^* 0. \tag{7.1}$$

So, the rules used in the derivation $w' \to^* \alpha a^{2^{n+1}-1}ca^nc\beta$ are only of the form $ba \to a^2b$ or $bc \to aca$. This means that it is allowed only to 'shift' b's to the right by $ba \to a^2b$, and 'take b out' by applying the rule $bc \to aca$. In particular, the number of c's remains unchanged.

As we said above, w' does not contain subwords of the form $a^{2^{k+1}-1}ca^kc$. So that in the rewriting process (7.1) the subword $A = a^{2^{n+1}-1}ca^nc$ would appear, the following must hold with respect to the two distinguished c's of the subword A: to the left of at least one of these c's in the word w' there must take place the process of shifting several b's to the right and then taking them out by applying the rule $bc \to aca$ with the c involved in this rule being the distinguished one. To put it formally, there exist $\mu_1, \mu_2 \in \{a, b\}^*$ and α_1, β_1 such that

- $w' = \alpha_1 c\mu_1\mu_2 c\beta_1$;
- $\alpha_1 c\mu_1 \to^* \alpha a^{2^{n+1}-1}ca^p$;
- $\mu_2 c\beta_1 \to^* a^{n-p}c\beta$

for some $0 \leq p \leq n$. Since there is no way of taking out b's in μ_1, we have actually that $\mu_1 = a^m$ for some $m \leq p$.

Let us now take a closer look at the rewriting $\mu_2 c\beta_1 \to^* a^{n-p}c\beta$. As we noted above we are forced to take out all the b's from μ_2. In the process we can also do some rewriting involving the letters from β and its derivatives. But since our rewriting system is complete, we may choose first taking out all the b's from μ_2 and only then do the remainder of the rewriting of $\mu_2 c\beta_1$ to $a^{n-p}c\beta$. Formally this can be put as follows. Let $l = |\mu_2|_b \leq n - p$, then there exists $s \geq l$ such that $\mu_2 c \to^* a^s ca^l$ and $a^l\beta_1 \to^* \beta$. Later we will use the formal decomposition of μ_2, so let $t', e_l, \cdots, e_1 \geq 0$ be such that $\mu_2 = a^{t'}ba^{e_l} \cdots ba^{e_1}$.

Let us now look at the rewriting $\alpha_1 ca^m \to^* \alpha a^{2^{n+1}-1}ca^p$. In this rewriting it is only possible to shift b's to the right and to take them out by

applying the rules $bc \to aca$. There have to be applied $p - m$ (we will prove later that this number has to be zero) 'taking-out'-s of b involving the distinguished c. The $p - m$ letters b involved in this process have to be the first $p - m$ letters b *of the word* w' to the left of the distinguished letter c. Formally, this means that there exist $t, d_{p-m}, \cdots, d_1 \geq 0$ such that $\alpha_1 = \alpha_2 \cdot a^t b a^{d_{p-m}} \cdots b a^{d_1} c a^m$ and

$$a^t b a^{d_{p-m}} \cdots b a^{d_1} c a^m \to^* a^{2^{n+1}-1} c a^p.$$

To summarise the information we collected so far:

$$\begin{array}{rcl} w' & = & \alpha_2 \cdot a^t b a^{d_{p-m}} \cdots b a^{d_1} c a^m \cdot a^{t'} b a^{e_l} \cdots b a^{e_1} c \beta_1 \\ a^t b a^{d_{p-m}} \cdots b a^{d_1} c a^m & \to^* & X = a^{2^{n+1}-1} c a^p \\ a^{t'} b a^{e_l} \cdots b a^{e_1} c & \to^* & Y = a^{n-p} c a^l. \end{array}$$

Since

$$w' \to^* \alpha_2 X Y \beta_1 = \alpha_2 \cdot a^{2^{n+1}-1} c a^n c \cdot a^l \beta_1,$$

without loss of generality we may assume that $\beta = a^l \beta_1$ and $\alpha = \alpha_2$. By Lemma 7.2.4,

$$\begin{array}{rcl} 2^{n+1} - 1 & = & t + f(d_{p-m}, \cdots, d_1) \\ n & = & p + t' + f(e_l, \cdots, e_1). \end{array}$$

By Lemma 7.2.5 these transform to

$$2^{p+t'+f(\vec{e})+1} = t + 2d_{p-m} + \cdots + 2^{p-m} d_1 + 2^{p-m}, \tag{7.2}$$

where $f(\vec{e})$ stands for $f(e_l, \cdots, e_1)$ for short.

Now, in the derivation

$$W = a^t b a^{d_{p-m}} \cdots b a^{d_1} c a^m \cdot a^{t'} b a^{e_l} \cdots b a^{e_1} c \to^* a^{2^{n+1}-1} c a^n c a^l, \tag{7.3}$$

which essentially makes the derivation $w' \to^* \alpha_2 a^{2^{n+1}-1} c a^n c a^l \beta_1$, the order of the rules to be applied is as follows: in the current word to rewrite we will find the rightmost position of b and if it is possible to apply the rule $bc \to aca$ then do it, otherwise after this b there must follow a and we apply $ba \to a^2 b$. We do it until run out of b's and obtain the word $a^{2^{n+1}-1} c a^n c a^l$. Two important remarks: (A) there *do* appear b's to work with in this manner – since w' does not contain subwords of the form $a^{2^{k+1}-1} c a^k c$; (B) in the process of our rewriting, by the initial choice of the derivation $w' \to^* \alpha a^{2^{n+1}-1} c a^n c \beta$, there never appear intermediate rewritten words with subwords of the form $a^{2^{k+1}-1} c a^k c$.

Now our aim is to prove that $p = m$. Assume the converse, i.e. $p - m \geq 1$. Since w' does not contain subwords a^2b, we have that

$$t \leq 1,\ d_{p-m} \leq 1,\ \cdots,\ d_2 \leq 1.$$

Then (7.2) gives us

$$\begin{aligned} 2^{p+t'+f(\vec{e})+1} &= t + 2d_{p-m} + \cdots + 2^{p-m}d_1 + 2^{p-m} \\ &\leq 1 + 2 + \cdots + 2^{p-m-1} + 2^{p-m} + 2^{p-m}d_1 \\ &= 2^{p+1-m} + 2^{p-m}d_1 - 1. \end{aligned}$$

From this we derive

$$2^{p+t'+f(\vec{e})+1} < 2^{p+1-m} + 2^{p-m}d_1,$$

which yields $2^{m+t'+f(\vec{e})+1} < 2 + d_1$, which means

$$2^{m+t'+f(\vec{e})+1} \leq d_1 + 1. \tag{7.4}$$

Now, by our manifest how we execute the derivation (7.3) and Lemma 7.2.4, we have that

$$a^t b a^{d_{p-m}} \cdots b a^{d_1} c a^m \cdot a^{t'+f(\vec{e})} c a^l.$$

is one of the intermediate words we obtain in the process of execution. But by our remark (B), we must have

$$d_1 < 2^{m+t'+f(\vec{e})+1} - 1.$$

This contradicts (7.4) and so $p = m$.

Again let us summarise what we have obtained:

- $w' = \alpha_2 a^t c a^m \cdot a^{t'} b a^{e_l} \cdots b a^{e_1} c \beta_1$;
- $w' \to^* P = \alpha_2 a^t c a^{m+t'+f(\vec{e})} c a^l \beta_1$;
- $t + 1 = 2^{m+t'+f(\vec{e})+1}$.

Since

$$|w'| = |\alpha_2| + |\beta_1| + t + m + t' + l + 2 + (e_l + \cdots e_1),$$

we have that

$$\begin{aligned} |P| &= |\alpha_2| + |\beta_1| + t + m + t' + l + 2 + f(e_l, \cdots, e_1) \\ &\leq |w'| + f(e_l, \cdots, e_1) \\ &\leq |w| + 2^{f(e_l,\cdots,e_1)} - 1 \\ &\leq |w| + t \\ &\leq |w| + |w'| \\ &\leq 2|w|. \end{aligned}$$

Thus there is a derivation from P to 0 which uses at most $|P| \leq 2|w|$ defining relations. Also, since every application of the rules $ba \to a^2b$ and $bc \to aca$ increases the length of the word by 1, we applied at most $2|w|$ rewriting rules in the derivation $w' \to^* P$. The word w' was obtained from w by applying at most $|w|$ changes of a^2b by ba. Therefore, including the consideration in the first paragraph in the current **Case 1**, w can be rewritten to 0 by $\leq |w| + 2|w| + 2|w| = 5|w|$ defining relations.

Case 2: rewriting two equal non-zero words. Now let $w, w' \in \{a, b, c\}^*$ represent the same non-zero element of M. Then in any derivation from w to w' there can be only used the relations $a^2b = ba$ and $bc = aca$. In particular, $w = w'$ in the monoid $N = \mathrm{Mon}\langle a, b, c : a^2b = ba,\ bc = aca\rangle$. Let us prove that the Dehn function of N with respect to the given presentation is linear. This will finish the proof of that $\mathbf{D}_n(M)$ is linear. Thus in the remainder of **Case 2** we are working with the monoid N.

We see that

$$ba^nc = a^2ba^{n-1}c = \cdots = a^{2n+1}c$$

and note that the system $\Sigma = \{a, b, c; a^2b \to ba,\ ba^nc \to a^{2n+1}ca, \quad n \geq 0\}$, which obviously defines N, is confluent and noetherian. It is an easy exercise to check that N is left cancellative.

We aim to show by the complete induction on $\ell = |w_1| + |w_2|$ that if $w_1 = w_2$ in N, then $d_N(w_1, w_2) \leq \ell$. The base case is obvious.

Now we do the induction step $(< \ell) \mapsto \ell$. Take two words $w_1, w_2 \in \{a, b, c\}^*$ such that $w_1 = w_2$ in N. By at most ℓ applications of the rule $a^2b \to_\Sigma ba$ we do the rewrites $w_1 \to^*_\Sigma u_1$ and $w_2 \to^*_\Sigma u_2$ to the words u_1 and u_2 not containing a subword a^2b. The number of c's in u_1 coincides with that of in u_2. If this number is zero, then $u_1 = u_2$ and so $d_N(w_1, w_2) \leq \ell$. So, assume that $u_1 = p_1cq_1$ and $u_2 = p_2cq_2$ where $p_1, p_2 \in \{a, b\}^*$. One easily sees that $p_1 = 1$ if and only if $p_2 = 1$; and in the case when $p_1 = p_2 = 1$ we have that $cq_1 =_N cq_2$ which yields $q_1 =_N q_2$ and then by induction $d_N(w_1, w_2) \leq d_N(|q_1| + |q_2|) \leq |q_1| + |q_2| \leq \ell$. So, assume that p_1 and p_2 are non-empty. Again, for the reasons that N is left-cancellative, we may assume that p_1 and p_2 start with different letters. Without loss, $p_1 = ap_1'$ and $p_2 = bp_2'$.

If p_1' contains b's, then since p_1 does not contain a subword a^2b, we obtain that $p_1' = bp$. But then $p_1c = abpc \to^*_\Sigma a^{2r}ca^d$ and $p_2c = bp_2'c \to^*_\Sigma a^{2s+1}ca^e$, a contradiction. Therefore $p_1 = a^{2f+1}$. Then, by applying our old rewriting system, i.e. the rules $ba \to a^2b$ and $bc \to aca$, we obtain $bp_2'c \to^* a^{2f+1}ca^l$, where $l = 1 + |p_2'|_b$, and the number of rules to apply is $2f + 1 + l - (1 + |p_2'|) \leq 2f + 1 = |p_1|$. Also, from $a^{2f+1}ca^lq_2 =_N a^{2f+1}cq_1$ we obtain $a^lq_2 =_N q_1$. Finally, since $|a^lq_2| + |q_1| = l + |q_2| + |q_1| < |w_1| + |w_2|$, by

induction we deduce that

$$d_N(w_1, w_2) \leq |p_1| + d_N(a^l q_2, q_1) \leq |p_1| + l + |q_2| + |q_1| \leq \\ |p_1| + |p_2| + |q_2| + |q_1| \leq |w_1| + |w_2|.$$

This finishes the induction step proof and we are ready to conclude that M has linear Dehn function.

Part 2: M is non-Markov.

Assume that M admits a regular combing with uniqueness. Then by Proposition 7.2.2, M admits a regular combing L with uniqueness over $\{a, b, c\}$. Let N be the number of states in an automaton accepting L.

Take $M \geq 1$ such that as soon as $(N+1)(2^{k+1}-1) \geq 2^{2^{M+1}-1} - 2$, then $k > N$.

Consider the word $W = a^{2^{2^{M+1}-1}-2} c a^{2^{M+1}-2} c a^M c$. This word is irreducible with respect to our rewriting system, and so $w \neq 0$. Let $w \in L$ be the word representing W. Then w must be of the form

$$w = a^t b a^{d_k} \cdots b a^{d_1} c a^{t'} b a^{e_l} \cdots b a^{e_1} c a^m c.$$

Furthermore,

$$\begin{aligned} a^t b a^{d_k} \cdots b a^{d_1} c &\to^* a^{2^{2^{M+1}-1}-2} c a^k \\ a^{t'} b a^{e_l} \cdots b a^{e_1} c a^m c &\to^* a^{2^{M+1}-2-k} c a^M c. \end{aligned}$$

Assume that $d_i > N$ for some i. Then we can pump some power of a in a^{d_i}:

$$w_k = a^t b a^{d_k} \cdots b a^{d_{i+1}} \cdot b a^{p+qn} \cdot b a^{d_{i-1}} \cdots b a^{d_1} c a^{t'} b a^{e_l} \cdots b a^{e_1} c a^m c \in L$$

for all $n \geq 1$, where $q \geq 1$ and $p + q = d_i$. But

$$b a^{d_{i-1}} \cdots b a^{d_1} c a^{t'} b a^{e_l} \cdots b a^{e_1} c a^m c \to^* a^u c a^v c a^f c$$

with u, v, f bounded in length by $|w|$. Then starting from some $n_0 \geq 1$, for all $n \geq n_0$ we will have that $p + qn + u \geq 2^{v+1} - 1$ and so $w_n = 0$ for all $n \geq n_0$, a contradiction.

Thus all $d_i \leq N$. Analogously $t \leq N$. Then

$$\begin{aligned} 2^{2^{M+1}-1} - 2 &= t + 2d_k + \cdots + 2^k d_1 + 2^k - 1 \\ &\leq N(1 + 2 + \cdots + 2^k) + 2^k - 1 \\ &= N(2^{k+1} - 1) + 2^k - 1 \\ &\leq (N+1)(2^{k+1} - 1) \end{aligned}$$

and so $k > N$. But then

$$w \to^* a^{2^{2^{M+1}-1}-2} ca^k \cdot a^{t'} ba^{e_l} \cdots ba^{e_1} ca^m c,$$

and by similar arguments we show by pumping a power of a in a^k that there are two distinct words in L both representing 0. Again we get a contradiction and so M does not admit a regular combing with uniqueness. $\square$

7.3 'Being Markov' under Finite Rees and Green Indices

Theorem 7.3.1. *The class of Markov semigroups is closed under forming finite Rees index extensions and subsemigroups.*

Proof. Let $T \leq S$ with $S - T$ finite.

Suppose that T is Markov and that L is a Markov language for T over some finite generating set A for T. Let B be a (finite) alphabet in bijection with $S - T$. Without loss of generality, assume that $A \cap B = \varnothing$. Then $L \cup B$ is a Markov language for S.

Now suppose that S admits a Markov language L over an alphabet A. Let $\varphi : A \to S$ be the corresponding representation map, so we have that $L\varphi = S$. Define

$$L(A, T) = \{w \in A^+ : w\varphi \in T\}.$$

Let C be an alphabet representing the elements of $S - T$, that is there is a bijection ψ from C onto $S - T$. For any word $w \in A^* - L(A, T)$, let $\underline{w}$ be the unique element of $C \cup \{1\}$ representing, under ψ, the element $w\varphi$, or 1 if $w\varphi = 1$. Define the alphabet

$$D = \{d_{\rho,a,\sigma} : \rho, \sigma \in C \cup \{1\}, a \in A, (a\varphi)(\sigma\psi) \in T \wedge (\rho\psi)(a\varphi)(\sigma\psi) \in T\},$$

and let it represent elements of T by the map ϕ as follows:

$$(d_{\rho,a,\sigma})\phi = (\rho\psi)(a\varphi)(\sigma\psi).$$

Notice that since A is finite, D too must be finite. Let $R \subseteq A^+ \times D^+$ be the relation consisting of pairs

$$\left(w_{n+1}a_n w_n a_{n-1} w_{n-1} \cdots a_2 w_2 a_1 w_1, d_{\underline{w_{n+1}},a_n,\underline{w_n}} d_{1,a_{n-1},\underline{w_{n-1}}} \cdots d_{1,a_2,\underline{w_2}} d_{1,a_1,\underline{w_1}}\right)$$

where the left-hand side lies in $L(A, T)$ and its factorization is obtained in the following way: start by letting the left-hand side be w_1'; a partial factorization

$$w_{i+1}' a_i w_i \cdots a_1 w_1$$

is complete if $w'_{i+1} \notin L(A,T)$; if on the other hand $w'_{i+1} \in L(A,T)$ set $a_{i+1}w_{i+1}$ to be the shortest suffix of w'_{i+1} lying in $L(A,T)$ and let w'_{i+2} be the remainder of w'_{i+1}.

Notice that if $(w,u) \in R$ then $w\varphi = u\phi$ by the definition of how the alphabet D represents elements of T. Note also that each word w determines a unique word $u \in D^+$ such that $(w,u) \in R$.

Lemma 7.3.2. *The relation R is rational.*

Proof. We will explain how a two-tape finite state automaton $\mathcal{A}$ can recognize R when reading from right-to-left; since the class of rational relations is closed under reversal, it will then follow that R is rational.

By the dual of [76, Theorem 4.3], S admits a left congruence Λ of finite index (that is, having finitely many equivalence classes) contained within $(T \times T) \cup \Delta_{S-T}$, where Δ_{S-T} is the diagonal relation on $S - T$.

Imagine the automaton $\mathcal{A}$ reading letters from A from its left-hand input tape and outputting symbols from D on its right-hand tape. Suppose the content of its left-hand tape is w. As it reads symbols from w (moving from right to left along the tape), it keeps track of the Λ-class of the element represented by the suffix of w read so far. (This is possible because Λ is a left congruence with only finitely many equivalence classes.) In particular, $\mathcal{A}$ knows whether the element represented by the suffix read so far lies in T (or equivalently, whether the suffix read so far lies in $L(A,T)$), or, if the element so represented lies in $S - T$, which letter of $C \cup \{1\}$ represents it. When $\mathcal{A}$ reads a symbol a such that the suffix read so far — say aw' — lies in $L(A,T)$, it non-deterministically chooses one of two actions:

1. It outputs $d_{1,a,\underline{w'}}$, resets its store of the suffix read so far to 1, and continues to read from its left-hand tape.

2. It outputs $d_{c,a,\underline{w'}}$, where c is a non-deterministically chosen element of $C \cup \{1\}$, then reads the remainder v of its left-hand tape and accepts if and only if $\underline{v} = c$. (Notice that this is the only way that $\mathcal{A}$ can accept.)

By induction on the subscripts of the letters a_i, the automaton $\mathcal{A}$ can accept only by outputting letters $d_{1,a,\underline{w_i}}$ immediately after reading the suffix $a_iw_i \cdots a_1w_1$ and the letter $d_{\underline{w_{n+1}},a_n,\underline{w_n}}$ immediately after reading $a_nw_n \cdots a_1w_1$, and can accept only when $w_{n+1} \notin L(A,T)$. So $\mathcal{A}$ recognizes R. $\square$

By Lemma 7.3.2,

$$K = L \circ R = \big\{v \in D^* : (\exists u \in L)\big((u,v) \in R\big)\big\}.$$

is regular. Since the set of left-hand sides of elements of R is $L(A,T)$, the language K maps under ϕ onto T.

Suppose $u_1, u_2 \in K$ are such that $u_1\phi =_S u_2\phi$. Let $w_1, w_2 \in L$ be such that $(w_1, u_1), (w_2, u_2) \in R$. Since L maps bijectively under φ onto S and $w_1\varphi =_S u_1\phi =_S u_2\phi =_S w_2\varphi$, the words w_1 and w_2 must be identical. Since every $w \in L(A,T)$ determines a unique $u \in D^+$ with $(w,u) \in R$, it follows that u_1 and u_2 are identical. So K maps bijectively under ϕ onto T.

Finally, let $u \in K$ with $|u| \geq 2$. Then $u = d_{c_{n+1},a_n,c_n} \cdots d_{1,a_2,c_2} d_{1,a_1,c_1}$, with $n \geq 2$. Then there is some word $w \in L$ with $(w,u) \in R$. By the definition of R, the word w factorizes as $w_{n+1}a_nw_n \cdots a_2w_2a_1w_1 \in L$ with $\underline{w_i} = c_i$, and $a_1w_1, a_2w_2, \ldots, w_{n+1}a_nw_n \in L(A,T)$.

Since L is prefix-closed, $w_{n+1}a_nw_n \cdots a_2w_2 \in L$. Since $a_2w_2, \ldots, w_{n+1}a_nw_n \in L(A,T)$, it follows that $w_{n+1}a_nw_n \cdots a_2w_2 \in L(A,T)$. So, by the definition of R, it follows that $d_{c_{n+1},a_n,c_n} \cdots d_{1,a_2,c_2} \in K$.

This shows that K is closed under taking longest proper non-empty prefixes. By induction, K is $+$-prefix-closed. Hence K is a Markov language for T. $\square$

The following example shows that the class of Markov semigroups is not closed under finite Green index extensions:

Example 7.3.3. Let G a finitely generated infinite torsion group. Let B be an alphabet representing a generating set for G. Let A be a finite alphabet in bijection with B and F be the free group with basis A. The bijection from A to B naturally extends to a surjective homomorphism $\phi : F \to G$. Let S be the *strong semilattice of groups* $\mathcal{S}(F, G, \phi)$, which is defined as follows: as a set S is the disjoint union of F and G, and the multiplication on S is defined by the following rule. Let $x, y \in S$. If $x, y \in F$, then define xy to be the product of x and y in F. If $x, y \in G$, then define xy to be the product of x and y in G. If $x \in F$ and $y \in G$, then define xy to be $x\phi \cdot y$. If $x \in G$ and $y \in F$, then define xy to be $x \cdot y\phi$.

F is hyperbolic and hence F is Markov. Moreover, F is a finite Green index subsemigroup of S, with $S - F = G$ forming of a single $\mathcal{H}^F$-class.

Suppose that S is Markov. Then by Proposition 7.2.2, S admits a regular combing with uniqueness L over $A \cup B$. By the definition of multiplication in a strong semilattice of monoids, the words in L representing elements of G are precisely those that include at least one letter B. That is, the language of words in L representing elements of G is $K = L - A^*$. Since L is regular, K is also. Since L maps bijectively onto S and $K \subseteq L$, it follows that K maps bijectively onto G. So if each letter $a \in A$ is interpreted as representing the element $a\phi$ of G, then K is a regular combing

with uniqueness for G. However, G, as a finitely generated infinite torsion group, does not admit a regular language of unique normal forms by the reasoning in [25, Example 2.5.12]. This is a contradiction, and so S cannot be Markov.

This example is similar in spirit to examples showing that neither the class of finitely presented semigroups nor the class of automatic semigroups is closed under forming finite Green index extensions [13, Examples 6.5 & 10.3]. However, with an extra condition on the Schützenberger groups of the T-relative $\mathcal{H}$-classes in the complement, a positive result does hold. First of all, recall the definition of Schützenberger groups:

Definition 7.3.4. Let T be a subsemigroup of a semigroup S. Let H be an $\mathcal{H}^T$-class. Let $\mathrm{Stab}(H) = \{t \in T^1 : Ht = H\}$, and define an equivalence $\sigma(H)$ on $\mathrm{Stab}(H)$ by $(x, y) \in \sigma(H)$ if and only if $hx = hy$ for all $h \in H$. Then $\sigma(H)$ is a congruence on $\mathrm{Stab}(H)$ and $\mathrm{Stab}(H)/\sigma(H)$ is a group, called the *Schützenberger group* of the $\mathcal{H}^T$-class H and denoted $\Gamma(H)$.

Proposition 7.3.5. *Let S be a semigroup and T a subsemigroup of S of finite Green index. Suppose that T is Markov and that the Schützenberger group of every T-relative $\mathcal{H}$-class in $S - T$ is Markov. Then S is Markov.*

Proof. Let L be a semigroup Markov language for T over some finite alphabet A representing a generating set for T under the map $\phi : A \to T$. Since T has finite Green index in S, there are finitely many T-relative $\mathcal{H}$-classes $H_1, \ldots, H_n$ in $S - T$. By hypothesis, every Schützenberger group $\Gamma(H_i)$ admits a semigroup Markov language L_i over some finite alphabet A_i representing a generating set for $\Gamma(H_i)$ under the map $\phi_i : A_i \to \Gamma(H_i)$. For brevity, let $\sigma_i = \sigma(H_i)$.

For each $i = 1, \ldots, n$, fix an element $h_i \in H_i$. For each $i = 1, \ldots, n$ and $a \in A_i$, fix elements $s_{i,a} \in \mathrm{Stab}(H_i)$ such that $a\phi_i = [s_{i,a}]_{\sigma_i}$.

Let A_i' be a new alphabet in bijection with A_i under the map $\alpha_i : A_i \to A_i'$. (Without loss of generality, assume that the alphabet A and the various alphabets A_i and A_i' are pairwise disjoint.) Define a map $\psi_i : A_i \cup A_i' \to S$ as follows:

$$a\psi_i = \begin{cases} s_{i,a} & \text{if } a \in A_i, \\ h_i s_{i,a} & \text{if } a \in A_i'. \end{cases} \tag{7.5}$$

Let

$$L_i' = \left\{(a\alpha_i)u \in A_i' A_i^* : au \in L_i, a \in A_i\right\}.$$

(So L_i' is the language obtained from L_i by taking each word in $L_i \subseteq A_i^+$ and replacing its first letter with the corresponding letter from A_i'.) Notice that since L_i is regular and $+$-prefix-closed, so is L_i'.

Since $\Gamma(H_i)$ acts regularly on H_i via

$$x \cdot [s]_{\sigma_i} = xs,$$

it follows that for every $y \in H_i$ there is a unique element $[s]_{\sigma_i} \in \Gamma(H_i)$ such that $h_i \cdot [s]_{\sigma_i} = y$. Thus it follows from (7.5) and the fact that L_i is a Markov language for $\Gamma(H)$ that for every $y \in H_i$ there is a unique $w \in L_i$ such that $h_i(w\phi_i) = y$. Hence, by (7.5) and the definition of L'_i, for every $y \in H_i$ there is a unique word $v \in L'_i$ with $v\psi_i = y$. Thus L'_i maps bijectively onto H_i.

Finally, let

$$K = L \cup \bigcup_{i=1}^{n} L'_i.$$

Then K is $+$-prefix-closed and regular. Define

$$\psi : A \cup \bigcup_{i=1}^{n} \left(A_i \cup A'_i\right) \to S, \qquad a\psi = \begin{cases} a\phi & \text{if } w \in A, \\ a\psi_i & \text{if } w \in A_i \cup A'_i. \end{cases}$$

Then ϕ maps K bijectively onto S. Hence K is a semigroup Markov language for L . $\square$

Proposition 7.3.5 parallels [13, Theorem 6.1], which shows that if T is a finite Green index subsemigroup of S, and T *and* all the Schützenberger groups of the T-relative $\mathcal{H}$-classes in $S - T$ are finitely presented, then S is finitely presented.

Question 7. Let T be a subsemigroup of finite Green index in a semigroup S. Let also S be Markov. Is T Markov?

Chapter 8

Decision Problems for Finitely Presented and One-Relator Semigroups and Monoids

In this chapter, for some distinguished properties of semigroups we study the following: whether that property or its negation is a Markov property, and whether it is decidable for finitely presented semigroups and for one-relator semigroups and monoids. All the results and open problems are summarized in a table.

The results of this chapter were obtained in collaboration with Alan Cain and appeared in [14].

8.1 Introduction

At the beginning of 20th century Max Dehn posed the question whether every one-relator group has soluble word problem. Later this was answered in the affirmative by Magnus [55]. At that stage it was natural to find an example of algorithmically insoluble problem. Based upon the results of Turing and Post it was possible to find the first undecidability result of an algebraic nature: Markov [61] and Post [71] established examples of finitely presented semigroups with insoluble word problem. This result was used later for proving other undecidability results like insolubility of the word problem for finitely presented groups [2]. Markov also used the word problem for finitely presented semigroups to prove that the so-called *Markov properties* are undecidable for finitely presented semigroups, see Section 8.2. Even though there has been much success in dealing with algorithmic problems using semigroup theory, the original question of Dehn for one-relator semigroups still remains open. A major step in the approach to this problem uses combinatorics on words [1, 3, 50]. An interesting result is obtained in [46] where the word problem for one-relator semigroups is reduced to the word problem for one-relator inverse

semigroups, the latter being closer to the class of groups. Some partial results, using the geometric approach of the so-called *word diagrams*, were obtained in [72]. The least known number of relations in a finitely presented semigroup one needs to take to obtain a semigroup with insoluble word problem is 3, due to Matiyasevich [62].

As a natural continuation, there appeared in literature some works on other algorithmic problems for finitely presented and one-relator semigroups, with greater emphasis on the latter. It was proved by Adian [1] that cancellativity is decidable for one-relator semigroups. Lallement [50] showed that it is decidable whether a one-relator semigroup has idempotents (we reprove this result in another fashion in Section 8.4).

In this chapter we do the following. We construct a list of 'distinguished' properties for semigroups. For each property from this list we ask whether it or its negation is a Markov property. If so then this property is undecidable for finitely presented semigroups. If neither the property nor its negation is a Markov property (or we do not know the answer to these) then we use a certain type of construction to prove that it is undecidable for finitely presented semigroups. After that we ask whether this property is decidable for one-relator semigroups and one-relator monoids. For some properties like 'having an identity' this clearly should be separated between semigroup and monoid cases. The summary of results we put into Table 8.1.

Before we start, let us agree on the following notation: if w is a word over some generating set for a semigroup S, then $\overline{w}$ is the element from S which is represented by w.

8.2 Markov Properties

In studying whether a given property is decidable for finitely presented semigroups, it turns out to be useful to know if it is a so-called Markov property, as such properties are undecidable for finitely presented semigroups. (By a 'property of semigroups' we mean those properties that are preserved under isomorphisms.) In most cases it is easy to check whether a particular property is a Markov property:

Definition 8.2.1. Let $\mathfrak{P}$ be a property of semigroups. Then $\mathfrak{P}$ is a *Markov property* if it satisfies the following two conditions:

1. There exists a finitely presented semigroup S_1 with property $\mathfrak{P}$.

2. There exists a finitely presented semigroup S_2 that does not embed into any finitely presented semigroup with property $\mathfrak{P}$.

Table 8.1: Shows, for particular properties of semigroups, whether it or its negation is a Markov property and whether it is decidable for general finitely presented semigroups and one-relator semigroups. [In each column: Y = Yes, N = No, ? = Unknown; in the decidability columns: T = Always true, F = Always false].

PROPERTY $\mathfrak{P}$	MARKOV PROPERTY		DECIDABLE		
	$\mathfrak{P}$	$\neg\mathfrak{P}$	FIN. PRES.	ONE-RELATOR	
				SEMIGROUP	MONOID
Having an identity	N (Pr. 8.3.1)	N (Pr. 8.3.1)	N (Pr. 8.3.3)	Y (Pr. 8.3.5)	T (By def.)
Having a zero	N (Pr. 8.3.2)	N (Pr. 8.3.2)	N (Pr. 8.3.4)	Y (Co. 8.3.7)	Y (Pr. 8.3.6)
Having idempotents	N (Th. 8.2.3)	Y (Trivial)	N (Th. 8.2.2)	Y (Th. 8.4.2)	T (By. def.)
Being a group	Y (Pr. 8.5.1)	N (Th. 8.2.3)	N (Th. 8.2.2)	Y (Pr. 8.5.6)	Y (Pr. 8.5.5)
Group-embeddability	Y (Pr. 8.5.1)	N (Th. 8.2.3)	N (Th. 8.2.2)	Y (Pr. 8.5.7)	Y (Pr. 8.5.8)
Cancellativity	Y (Pr. 8.5.10)	N (Th. 8.2.3)	N (Th. 8.2.2)	Y (Re. 8.5.11)	Y (Pr. 8.5.12)
Non-trivial subgroup	N (Th. 8.2.3)	Y (Trivial)	N (Th. 8.2.2)	?	?
Being inverse	Y (Pr. 8.5.1)	N (Th. 8.2.3)	N (Th. 8.2.2)	Y (Pr. 8.5.9)	?
Orthodoxy	Y (Pr. 8.5.1)	N (Th. 8.2.3)	N (Th. 8.2.2)	?	?
Regularity	?	N (Pr. 8.5.2)	N (Pr. 8.5.3)	Y (Pr. 8.5.4)	?
$\min_R$	Y (Pr. 8.6.1)	N (Th. 8.2.3)	N (Th. 8.2.2)	Y (Co. 8.6.3)	Y (Pr. 8.6.2)
Right-stability	Y (Pr. 8.6.1)	N (Th. 8.2.3)	N (Th. 8.2.2)	?	?
$J = D$	?	N (Pr. 8.7.1)	N (Pr. 8.7.2)	?	?
Being the bicyclic monoid	Y (Re. 8.8.3)	N (Th. 8.2.3)	N (Th. 8.2.2)	F (Co. 8.8.5)	Y (Pr. 8.8.4)
Being a BR-ext.	N (Pr. 8.8.1)	N (Pr. 8.8.1)	N (Pr. 8.8.2)	F (Co. 8.8.5)	?
Simplicity	N (Pr. 8.9.1)	N (Pr. 8.9.1)	N (Pr. 8.9.2)	Y (Co. 8.9.6)	?
Bisimplicity	?	N (Pr. 8.9.1)	N (Co. 8.9.5)	Y (Co. 8.9.6)	?
Semisimplicity	N (Pr. 8.9.3)	N (Pr. 8.9.3)	N (Pr. 8.9.4)	?	?
Hopficity	N (Pr. 8.10.1)	N (Pr. 8.10.1)	N (Pr. 8.10.2)	?	?

The following theorem is folklore: the Markov properties are undecidable for finitely presented semigroups. The way *how* it is proved will help us later to prove undecidability results for finitely presented semigroups, so we include a sketch proof for the monoid case.

Theorem 8.2.2 ([9, Theorem 7.3.7])**.** *Let $\mathfrak{P}$ be a property of semigroups, and suppose that either $\mathfrak{P}$ or $\neg\mathfrak{P}$ is a Markov property. Then $\mathfrak{P}$ is undecidable for finitely presented semigroups.*

Proof. Let $\mathfrak{P}$ be a Markov property and let S_1 and S_2 be two monoids as in Definition 8.2.1. Take any finitely presented monoid T with undecidable word problem. Set $S = T *_{\mathrm{M}} S_2$. The monoid S has undecidable word problem and does not have property $\mathfrak{P}$. Also S is a finitely presented monoid: let $S = \mathrm{Mon}\langle A : R\rangle$ be any finite presentation for S. Now for arbitrary $u, v \in A^*$ define

$$S_{u,v} = \mathrm{Mon}\langle A, c, d : R,\ cud = 1,\ acvd = cvd \quad (\forall a \in A \cup \{c, d\})\rangle. \tag{8.1}$$

$S_{u,v}$ satisfies the following two conditions: if $\overline{u} = \overline{v}$, then $S_{u,v}$ is trivial; if $\overline{u} \neq \overline{v}$ then S_2 embeds into $S_{u,v}$ and so $S_{u,v}$ does not have property $\mathfrak{P}$.

Thus whether the monoid $S_1 *_{\mathrm{M}} S_{u,v}$ has property $\mathfrak{P}$ is equivalent to whether $\overline{u} = \overline{v}$. All the constructions used are effective, so the word problem reduces to the problem of deciding $\mathfrak{P}$: thus $\mathfrak{P}$ is undecidable.

If $\neg\mathfrak{P}$ is a Markov property, the result follows from the same proof on noting that $\mathfrak{P}$ is decidable if and only if $\neg\mathfrak{P}$ is decidable. □

Notice that the construction (8.1) appears in some other branches of mathematics, e.g. using it, Bernhard Neumann proved that every existentially closed monoid has only two congruences [52, Chapter IV]. Constructions of this type will be a principal tool for proving undecidability results for finitely presented semigroups later in the chapter.

The following theorem, although not difficult, does not seem to have been explicitly stated hitherto:

Theorem 8.2.3. *Let $\mathfrak{P}$ be a property of semigroups. Then at most one of $\mathfrak{P}$ and $\neg\mathfrak{P}$ is a Markov property.*

Proof. Suppose $\mathfrak{P}$ and $\neg\mathfrak{P}$ are both Markov properties. Then there exists a finitely presented semigroup S that does not embed into any finitely presented $\mathfrak{P}$-semigroup and a finitely presented semigroup T that does not embed into any finitely presented semigroup that is $\neg\mathfrak{P}$. Both S and T embed into $S *_{\mathrm{S}} T$, which is finitely presented; thus $S *_{\mathrm{S}} T$ can be neither $\mathfrak{P}$ nor $\neg\mathfrak{P}$. This is a contradiction, so at least one of $\mathfrak{P}$, $\neg\mathfrak{P}$ fails to be a Markov property. □

8.3 Identity? Zero?

Proposition 8.3.1. *Neither the property of having an identity, nor its negation, is a Markov property.*

Proposition 8.3.2. *Neither the property of having a zero, nor its negation, is a Markov property.*

These results can be proved in parallel:

Proof. Let S be a finitely presented semigroup. Then S embeds into the finitely presented semigroup S^1 (respectively, S^0); thus having an identity (respectively, a zero) is not a Markov property.

On the other hand, S embeds into the free product $S *_{\mathrm{S}} \mathbb{N}$, which does not contain an identity (respectively, a zero); thus lacking an identity (respectively, a zero) is not a Markov property. □

Proposition 8.3.3. *It is undecidable whether a finitely presented semigroup has an identity.*

Proof. Let $S = \mathrm{Sg}\langle A : R\rangle$ be a semigroup with insoluble word problem. Take any $u, v \in A^*$ and construct a new semigroup

$$\begin{aligned} S'_{u,v} = \mathrm{Sg}\langle A, c, d, e \ : \ & R,\ cud = e,\ acvd = cvd \quad (\forall a \in A \cup \{c, d\}) \\ & ae = a \quad (\forall a \in A \cup \{c, d, e\})\rangle. \end{aligned}$$

If $\overline{u} = \overline{v}$ then every generator for $S'_{u,v}$ equals e, which is an idempotent, and so $S'_{u,v}$ is trivial.

If $\overline{u} \neq \overline{v}$ then $S'_{u,v}$ does not have an identity. To see this, suppose the contrary and observe that since e is a right identity, e would be this identity and thus we would have $ec = c$. Then, having that $e = cud \in \langle A, c, d\rangle$ and so $e = ecvd$, we would have $cud = e = ecvd = cvd$. This leads to a contradiction since $cud \neq cvd$ in the semigroup $S_{u,v}$ which is a homomorphic image of $S'_{u,v}$.

Therefore $S'_{u,v}$ contains an identity if and only if $\overline{u} = \overline{v}$. □

Proposition 8.3.4. *It is undecidable whether a finitely presented semigroup has a zero.*

Proof. Notice that a group has a zero if and only if it is trivial. In addition, every finitely presented group is also a finitely presented semigroup. Hence, since 'being trivial' is a Markov property for groups, the claim follows immediately. □

Proposition 8.3.5. *It is decidable whether a one-relator semigroup has an identity.*

Proof. Let $S = \mathrm{Sg}\langle A : u = v\rangle$ be a semigroup with identity $\overline{w}$. Then for every $a \in A$, we have that $\overline{a} = \overline{aw}$. Therefore there is a sequence of transitions from a to aw and so a is either u or v. So A contains at most two symbols. If $A = \{a, b\}$, then $u = a$ and $v = b$, whence $S \simeq \mathbb{N}$, which is a contradiction. If A is a singleton $\{a\}$ then, using elementary reasonings about monogenic semigroups, S has an identity if and only if the defining relation $u = v$ is either $a = a^k$ or $a^k = a$ for some $k \geq 2$. □

Proposition 8.3.6. *It is decidable whether a one-relator monoid has a zero.*

Proof. Let $S = \mathrm{Mon}\langle A : u = v\rangle$ be a monoid with a zero $\overline{w}$, where $w \in A^*$.

Assume first that $v = 1$. Then for any $a \in A$ we have $\overline{wa} = \overline{w}$. Thus there is a sequence of elementary transitions from wa to w. Since such a sequence can lead from wa only to words with length $|wa| + k|u|$ for some $k \in \mathbb{Z}$, we obtain $|u| = 1$. Thus a Tietze transformation can be used to remove a redundant generator from A and so S is a free monoid and does not contain a zero, unless it is trivial.

Now assume that $|u|, |v| \geq 1$. Obviously $w \in A^+$. Note that in a left-cancellative semigroup every idempotent is a left identity. So S cannot be left-cancellative and so, by Adjan's Theorem, u and v start with the same letter. Now, for any $a \in A$, the equality $\overline{aw} = \overline{w}$ holds. So there is a sequence of elementary transitions from aw to w. Thus w begins with the letter a. Since $a \in A$ was arbitrary, we obtain that $|A| = 1$. Therefore S contains a zero if and only if $A = \{a\}$ and $u = v$ is $a^k = a^{k+1}$ or $a^{k+1} = a^k$ for some $k \in \mathbb{N}$. □

Since S contains a zero if and only if S^1 does, the following result is a corollary of the preceding proposition.

Corollary 8.3.7. *It is decidable whether a one-relator semigroup has a zero.*

8.4 Idempotents?

Lallement proved in [50] that it is decidable whether a one-relator semigroup contains an idempotent. We provide an alternative, shorter, proof for this. We will need an auxiliary lemma which was proved in [53, Lemma 2]. We give a new proof of this lemma which, unlike the original one from [53], avoids inductive reasonings:

Lemma 8.4.1. *Let $s, x, y \in A^*$ be such that $sx = ys$ with $|x| = |y| < |s|$. Then there exist $u, v \in A^*$ and $n \in \mathbb{N}$ with $s = (uv)^n u$, $x = vu$ and $y = uv$.*

Proof. Take the maximal n such that $s = y^n u$ for some $u \in A^*$. We have $y^n ux = y^{n+1}u$ and so $ux = yu$. So either y is a prefix of u or u is a prefix of y. By the choice of n, the former case is impossible. So $y = uv$ for some $v \in A^*$ and thus $s = (uv)^n u$. Therefore $(uv)^n ux = (uv)^{n+1}u$ and so $x = vu$. □

Theorem 8.4.2. *Let S be the one-relator semigroup $\mathrm{Sg}\langle A : p = q\rangle$ with $|p| \geq |q|$. Then S contains an idempotent if and only if one of the following two conditions hold:*

1. *$A = \{a\}$ (for some symbol a), $p = a^k$ (for some $k \geq 2$), and $q = a$, in which case S is a finite cyclic group.*
2. *S is neither left- nor right-cancellative, and q is both a prefix and a suffix of p.*

Proof. First we note that if S contains an idempotent then $|p| \neq |q|$. Indeed, otherwise there would exist $w \in A^+$ such that the words ww and w represent the same element of S. But then, having $|p| = |q|$, we would have that $|ww| = |w|$, a contradiction.

Lemma 8.4.3. *If S is left-cancellative and contains an idempotent, then A contains a single symbol a, $p = a^k$ (for some $k \geq 2$), $q = a$, and thus S is a finite cyclic group.*

Proof. Suppose S is left-cancellative and let $w \in A^+$ represent an idempotent of S. Then w is a left identity for S. So, for any $a \in A$, wa and a must represent the same element of S. Thus wa and a are linked by a sequence of elementary transitions. The last transition must have right-hand side a. That is, $q = a$ for every $a \in A$. Thus A must contain a single letter a, and $p = a^k$ for some $k \geq 2$ since $|p| > |q|$. □

Lemma 8.4.4. *If S is not left-cancellative (respectively, right-cancellative) and contains an idempotent and $|A| \geq 2$, then q is a prefix (respectively, suffix) of p.*

Proof. If S is not left-cancellative, then p and q must start with the same letter. Let u be the longest common prefix of p and q, with $p = up'$ and $q = uq'$. Assume $q' \neq 1$. Then the semigroup $T = \mathrm{Sg}\langle A : p' = q'\rangle$ is left-cancellative and contains an idempotent since S does. By the previous lemma, $A = \{a\}$, which is a contradiction. □

Lemma 8.4.5. *If S is neither left- nor right-cancellative and $|A| \geq 2$, S has an idempotent if and only if q is both a prefix and a suffix of p.*

Proof. The forward implication holds by the previous lemma.

Suppose q is both a prefix and suffix of p. If $|q| \leq (1/2)|p|$, then $p = qwq$ for some $w \in A^*$. In this case, qw represents an idempotent of S.

If $|q| > (1/2)|p|$, then $p = xq = qy$, and therefore $p = (uv)^{n+1}u$ and $q = (uv)^n u$ by Lemma 8.4.1. So $(uv)^{n+2}$ and $(uv)^{n+1}$ represent the same element of S, and hence $(uv)^{n+1}$ represents an idempotent of S. □

The above lemmas together imply the theorem. □

Corollary 8.4.6. *Let S be the one-relator semigroup $\mathrm{Sg}\langle A : p = q\rangle$. Assume without loss that $|p| \geq |q|$. Then S contains an idempotent if and only if q is a proper prefix and a proper suffix of p. In particular, it is decidable whether a one-relator semigroup has an idempotent.*

8.5 A Group? Group-embeddable? Inverse? Orthodox? Regular? Cancellative?

A semigroup is called *orthodox* if it is regular and all the idempotents form a subsemigroup.

Proposition 8.5.1. *Orthodoxy, being inverse, group-embeddability, and being a group are all Markov properties.*

Proof. Group-embeddability is a Markov property since there are examples of finitely presented semigroups embeddable into groups and the semigroup $\mathrm{Sg}\langle a, b : a^2 = a,\ b^2 = b\rangle$ is not embeddable into a group.

For the remaining three properties, orthodoxy is the weakest property, so it suffices to exhibit a finitely presented semigroup that does not embed into any finitely presented orthodox semigroup. Again, $\mathrm{Sg}\langle a, b : a^2 = a,\ b^2 = b\rangle$ is not embeddable into any orthodox semigroup: it is generated by idempotents but does not consist entirely of idempotents. □

Proposition 8.5.2. *Non-regularity is not a Markov property.*

Proof. Follows from that any finitely presented regular semigroup S embeds into the finitely presented non-regular semigroup $S *_{\mathrm{S}} \mathbb{N}$. □

It remains an open problem whether regularity is a Markov property. However we can prove that regularity is undecidable for general finitely presented semigroups:

Proposition 8.5.3. *Regularity is undecidable for finitely presented semigroups.*

Proof. Take an arbitrary finitely presented semigroup $S = \mathrm{Sg}\langle A : R\rangle$ with insoluble word problem and indecomposable generators (e.g., Tseitin's semigroup, see [2, Theorem 2.2]). Pick $u, v \in A^+$. If $\overline{u} = \overline{v}$ then the semigroup $S_{u,v}$ (as defined by Eq. (8.1)) is trivial and so is regular. Suppose, with the aim of obtaining a contradiction, that $\overline{u} \neq \overline{v}$ and $S_{u,v}$ is regular. Then for any letter a, there exists a word $w \in (A \cup \{c, d\})^*$ such that $\overline{a} = \overline{awa}$.

We will prove now by induction on k that every chain of transitions $a = w_0 \to w_1 \to \cdots \to w_k$ is such that none of w_i contains a factor cpd where $\overline{p} = \overline{v}$ and $p \in (A \cup \{c, d\})^*$. The base case is obvious since $\overline{u} \neq \overline{v}$. Assume that for chains of lengths $\leq k$ the hypothesis holds and take a chain $a = w_0 \to w_1 \to \cdots \to w_k \to w_{k+1}$ contradicting the hypothesis. Then w_{k+1} contains a factor cpd with $\overline{p} = \overline{v}$. Clearly the transition $w_k \to w_{k+1}$ cannot correspond to a relation from $R \cup \{bcvd = cvd\}$. If $w_k \to w_{k+1}$ corresponded to the insertion of the word cud, then w_k would contain the factor cpd. Hence $w_k \to w_{k+1}$ corresponds to the deletion of the word cud. Then w_k must contain a factor cp_1cudp_2d with $p_1p_2 = p$. This is a contradiction since $\overline{p_1cudp_2} = \overline{v}$. Thus the statement of induction is proved.

In any chain of transitions from a to awa there can be used only insertions or deletions of cud and relations from R. Hence by a routine induction one shows that $w = cpd$ for some $p \in (A \cup \{c, d\})^*$. Let $a = w_0 \to w_1 \to \cdots \to w_{k-1} \to w_k = acpda$ be a chain from a to a word of the type $acpda$ with minimal possible length. If $w_{k-1} \to w_k$ is the insertion of cud, then $w_{k-1} \in ac(A \cup \{c, d\})^*da$, a contradiction. If $w_{k-1} \to w_k$ corresponds to a relation from R, then, since a is indecomposable element in S, we again have $w_{k-1} \in ac(A \cup \{c, d\})^*da$. Therefore $w_{k-1} \to w_k$ is the deletion of cud. Hence either $w_{k-1} = cudawa$ or $w_{k-1} = awacud$, without loss of generality we may assume the first case. In order to reach $cudawa$ from a, there must exist r such that $w_{r+1} = cudw_r$. Find the largest such r. Then $w_i = cudw'_i$ for every i with $r + 1 \leq i \leq k - 1$. Then $a = w_0 \to w_1 \to \cdots w_r \to w'_{r+2} \to \cdots w'_{k-1} = awa$ is a chain with length shorter than the initial one, a contradiction.

Thus, $S_{u,v}$ is regular if and only if $\overline{u} = \overline{v}$ in S. □

Although we do not know the answer to the question on decidability of regularity for one-relator monoids, we provide it for one-relator semigroups:

Proposition 8.5.4. *It is decidable whether a one-relator semigroup is regular.*

Proof. Take an arbitrary one-relator semigroup $S = \mathrm{Sg}\langle A : u = v\rangle$ and assume that it is regular. Since every generator must be decomposable,

we have that either A is a singleton or that the relation is of the type $a = b$ for some $a, b \in A$. The latter case is obviously impossible. So that S is regular if and only if A is a singleton $\{a\}$ and the relation is of the type $a^k = a$ or $a = a^k$ for some $k \geq 2$. □

Proposition 8.5.5. *It is decidable whether a one-relator monoid is a group.*

Proof. Consider an arbitrary one-relator monoid $S = \mathrm{Mon}\langle A : u = v\rangle$.

Suppose first that both u and v are non-empty. Then no sequence of elementary transitions links the empty word 1 and a non-empty word. Thus no non-empty word u can represent an invertible element, for if $v \in A^*$ represents its inverse, there would have to be a transition sequence from uv to 1. So in this case, S can never be a group.

Suppose now, without loss of generality, that $v = 1$. Then S is a group if and only if every letter from the alphabet is both right and left invertible. This is equivalent to that every letter from the alphabet divides 1 both from left and right, and the division problem for one-relator special monoids is soluble [1]. □

Proposition 8.5.6. *It is decidable whether a one-relator semigroup is a group.*

Proof. If a semigroup is a group, it contains an identity. By the proof of Proposition 8.3.5, a one-relator semigroup contains an identity if and only if it is a group. This is possible only in the case when $A = \{a\}$ and the relation is $a^k = a$ or $a = a^k$ where $k \geq 2$. □

Proposition 8.5.7. *It is decidable whether a one-relator semigroup is group-embeddable.*

Proof. If A is a singleton $\{a\}$ then a semigroup $\mathrm{Sg}\langle A : u = v\rangle$ is group-embeddable if and only if the relation is of the type $a = a^k$ or $a^k = a$ for some $k \geq 1$. If $|A| > 1$ then, by Adjan's theorem [1], $\mathrm{Sg}\langle A : u = v\rangle$ embeds into a group if and only if u and v start and end with different letters. □

Proposition 8.5.8. *It is decidable whether a one-relator monoid is group-embeddable.*

Proof. Let $S = \mathrm{Mon}\langle A : u = v\rangle$ be a one-relator monoid. Suppose that $u, v \in A^+$. Then $S \simeq T^1$, where $T = \mathrm{Sg}\langle A : u = v\rangle$, and S is group-embeddable if and only if T is group-embeddable and does not contain an identity: both of these properties are decidable by Propositions 8.5.7 and 8.3.5.

Now suppose that S is a special monoid with, say, $v = 1$. We will show that S is group embeddable if and only if $\mathrm{Mon}\langle \mathrm{cont}(u) : u = 1\rangle$ is a group where $\mathrm{cont}(u)$ is the content of the word u. To see this, let $u = pq$

for some $p, q \in A^*$. Then $\overline{pq} = \overline{1}$ and so $\overline{qp} = \overline{1}$, for otherwise S would contain a copy of the bicyclic monoid (see [18, Lemma 1.31]) and so could not be group-embeddable. Therefore every letter from $\mathrm{cont}(u)$ is invertible and so the claim follows. The sufficiency is obvious. It remains to use Proposition 8.5.5. □

Unfortunately we do not know if it is decidable whether a one-relator monoid is inverse, but we can do it for one-relator semigroups:

Proposition 8.5.9. *It is decidable whether a one-relator semigroup is inverse.*

Proof. Take an arbitrary one-relator semigroup $S = \mathrm{Sg}\langle A : u = v\rangle$ and suppose that it is inverse.

Suppose first that $u, v \in A^+$. The semigroup S contains idempotents and so by Theorem 8.4.2 we have that u and v start with the same letter. Take now an arbitrary $a \in A$ and $w \in A^+$. Then we have

$$\overline{a}\,\overline{a}^{-1}\overline{w}\,\overline{w}^{-1} = \overline{w}\,\overline{w}^{-1}\overline{a}\,\overline{a}^{-1},$$

and so w must start with a. This means that A is a singleton and, using elementary reasonings about monogenic semigroups, S must be a group.

Thus a one-relator semigroup is an inverse semigroup if and only if it is a group. The result now follows from Proposition 8.5.6. □

The last property of this section we discuss is the cancellativity. First we deal with the general finitely presented semigroups case:

Proposition 8.5.10. *Cancellativity is a Markov property.*

Proof. Obviously there are examples of cancellative finitely presented semigroups. On the other hand the bicyclic monoid is not embeddable into a cancellative finitely presented semigroup. □

Remark 8.5.11. It is a classical result of Adjan [1] that a one-relator semigroup $\mathrm{Sg}\langle A : u = v\rangle$ is cancellative if and only if either A is a singleton, or u and v start with different letters and end with different letters.

Proposition 8.5.12. *It is decidable whether a one-relator monoid is cancellative.*

Proof. Take a one-relator monoid $S = \mathrm{Mon}\langle A : u = v\rangle$. If $|u|, |v| \geq 1$ then S is cancellative if and only if $\mathrm{Sg}\langle A : u = v\rangle$ is, and so it remains to use Remark 8.5.11. If, say, $v = 1$ then S is cancellative if and only if $S' = \mathrm{Mon}\langle \mathrm{cont}(u) : u = 1\rangle$ is a group. The sufficiency is obvious. For the other direction, using the same methods as in the proof of Proposition 8.5.8, we prove that either S' is a group or S contains a copy of the bicyclic monoid. In the latter case S cannot be cancellative. It remains to use Proposition 8.5.5. □

8.6 Right Stable? $\min_R$?

Proposition 8.6.1. *Right stability and* $\min_R$ *are Markov properties.*

Proof. Since right stability is the weaker property among the two, it suffices to exhibit an example of a finitely presented semigroup, which cannot embed into a finitely presented right stable semigroup.

Take the bicyclic monoid $B = \mathrm{Mon}\langle b, c : cb = 1\rangle$. Assume that B is embeddable into a finitely presented right stable semigroup S. We have a strictly descending chain of $\mathcal{R}$-classes in B:

$$R_b^B > R_{b^2}^B > R_{b^3}^B > \cdots .$$

This gives a descending chain of $\mathcal{R}^S$-classes in S: $R_b^S \geq R_{b^2}^S \geq R_{b^3}^S \geq \cdots$. This latter chain must stabilise since all the $\mathcal{R}$-classes from it come from the same $\mathcal{J}^B$-class and so from the same $\mathcal{J}^S$-class. So that there exist $k < n$ such that $R_{b^k}^S = R_{b^n}^S$. Now, since B is a regular subsemigroup of S, we have by [45, Proposition 2.4.2] that $\mathcal{R}^B = \mathcal{R}^S \cap (B \times B)$. This means that $R_{b^k}^B = R_{b^n}^B$, a contradiction. Thus right stability is a Markov property. $\square$

We do not know whether it is decidable for one-relator semigroups or monoids to be right stable. However we prove that the corresponding question for the property $\min_R$ is decidable:

Proposition 8.6.2. *It is decidable whether a one-relator monoid has* $\min_R$.

Proof. Take an arbitrary one-relator monoid $S = \mathrm{Mon}\langle A : u = v\rangle$.

Assume first that both u and v come from A^+. The aim is to show that S has $\min_R$ if and only if A is a singleton $\{a\}$ and the relation has the form $a^k = a^n$ for distinct k and n. The sufficiency is obvious. So assume that S has $\min_R$ and suppose, with the aim of obtaining a contradiction, that A contains distinct letters a and b. Let $d \in \{a, b\}$. Then, since the chain $R_d \geq R_{d^2} \geq R_{d^3} \geq \cdots$ must stabilise, we have that there exist $k < n$ and $x \in A^*$ such that $\overline{d^k} = \overline{d^n x}$. This implies that one of u and v is a power of d. Therefore, interchanging u and v if necessary, $u = a^p$ and $v = b^q$. If either p or q is equal to 1, then S is isomorphic to $\mathbb{N} \cup \{0\}$. If, on the other hand, $p, q \geq 2$ then we obtain a strict descending chain $R_{ab} > R_{(ab)^2} > R_{(ab)^3} > \cdots$. In either case, we have a contradiction. Hence, $A = \{a\}$ and so the relation is as above (for otherwise S would be isomorphic to $\mathbb{N} \cup \{0\}$ and so not $\min_R$).

Assume now that $v = 1$. The aim is to show that S is $\min_R$ if and only if it is a group, the sufficiency being obvious. Then this would imply, in view of Proposition 8.5.5, that $\min_R$ is decidable for one-relator monoids.

So, suppose that S has $\min_R$. Let $u = pa$ where $a \in A$. Consider the chain $R_a \geq R_{a^2} \geq R_{a^3} \geq \cdots$. Since it must stabilise, there exist $k < n$ and $x \in S$ such that $\overline{a^k} = \overline{a^n x}$. This implies $\overline{1} = \overline{p^k a^k} = \overline{p^k a^n x} = \overline{a^{n-k} x}$ and so a is invertible. Hence $\overline{p}$ is invertible and similarly the last letter from p represents an invertible element. Continuing in this way, one sees that all the letters from u represent invertible elements. Obviously all the letters from A must appear in u. Thus every generator is invertible and so S is a group, as required. □

Corollary 8.6.3. *It is decidable whether a one-relator semigroup has* $\min_R$.

Proof. It is easy to see that a semigroup S has $\min_R$ if and only if S^1 has. So that $\mathrm{Sg}\langle A : u = v\rangle$ has $\min_R$ if and only if $\mathrm{Mon}\langle A : u = v\rangle$ has. The statement now follows from Proposition 8.6.2. □

8.7 $\mathcal{J} = \mathcal{D}$?

We do not know whether the property of having $\mathcal{J} = \mathcal{D}$ is a Markov property. However we prove that its negation is not:

Proposition 8.7.1. *The negation of* $\mathcal{J} = \mathcal{D}$ *is not a Markov property.*

Proof. Take an arbitrary finitely presented semigroup S. If T is an arbitrary finitely presented monoid with $\mathcal{J}^T \neq \mathcal{D}^T$ (for example $T = \mathrm{Mon}\langle a, b, c : abc = 1\rangle$, see [51, Excercise 9, Chapter 2]) then $S^1 \times T$ is finitely presented, contains S and does not possess $\mathcal{J} = \mathcal{D}$. □

Proposition 8.7.2. *The property of having* $\mathcal{J} = \mathcal{D}$ *is undecidable for finitely presented semigroups.*

Proof. As in the proof of Proposition 8.5.3, consider an arbitrary finitely presented semigroup $S = \mathrm{Sg}\langle A : R\rangle$ with insoluble word problem and indecomposable generators. Pick $u, v \in A^+$. If $\overline{u} = \overline{v}$ then $S_{u,v}$ is trivial and so has $\mathcal{J} = \mathcal{D}$. So suppose $\overline{u} \neq \overline{v}$. Any any letter a, appearing in u, is $\mathcal{J}$-related to 1. We claim that $(\overline{a}, 1) \notin \mathcal{D}$. Indeed, if $\overline{a}\mathcal{D}1$ then a is regular in $S_{u,v}$ and so we would be able to find $w \in S_{u,v}$ such that $\overline{a} = \overline{awa}$. As in the proof of Proposition 8.5.3, this is a contradiction. □

We do not know whether $\mathcal{J} = \mathcal{D}$ is decidable for one-relator semigroups or monoids. Possible hints could be taken from [50], where one-sided and two-sided divisibility problems are solved for some important classes of one-relator monoids.

8.8 A Bruck–Reilly Extension? Bicyclic?

Recall that the *Bruck–Reilly extension* of a monoid $M = \mathrm{Mon}\langle A : R\rangle$ with respect to a (monoid) endomorphism $\vartheta : M \to M$ is the monoid

$$\mathrm{BR}(M, \vartheta) = \mathrm{Mon}\langle A, b, c : R, bc = 1, ac = c(a\vartheta), ba = (a\vartheta)b \quad (\forall a \in A)\rangle,$$

where b, c are new symbols not in A and $a\vartheta$ is interpreted as some fixed word in A^* representing $a\vartheta$. If S is a semigroup without an identity and ϑ is an endomorphism of S, then the Bruck–Reilly extension of S with respect to ϑ is defined to be $\mathrm{BR}(S^1, \vartheta^*)$, where $\vartheta^* : S^1 \to S^1$ is defined by $s \mapsto s\vartheta$ for all $s \in S$ and $1 \mapsto 1$. The bicyclic monoid B is the Bruck–Reilly extension of the trivial monoid:

$$B = \mathrm{Mon}\langle b, c : bc = 1\rangle.$$

Note that any semigroup S embeds into any of its Bruck–Reilly extensions. If W is a set of canonical forms for M, then the set $\{c^k w b^n : k, n \geq 0,\ w \in W\}$ forms the canonical forms for $\mathrm{BR}(M, \vartheta)$. It turns out that $\mathrm{BR}(M, \vartheta)$ is isomorphic to the semigroup of triples (k, m, n) (where $k, n \geq 0$ and $m \in M$) subject to the multiplication

$$(k, m_1, n) \cdot (p, m_2, q) = (k - n + r, (m_1\vartheta^{r-n})(m_2\vartheta^{r-p}), q - p + r),$$

where $r = \max(n, p)$. The use of Bruck-Reilly extensions is that $\mathrm{BR}(S^1, \vartheta)$, where ϑ maps all $s \in S^1$ to 1, is a simple semigroup, and so every semigroup embeds in a simple semigroup. The definition of Bruck-Reilly extensions makes them an analogue of HNN-extensions.

Let $\mathfrak{P}$ be the property of being a Bruck–Reilly extension.

Proposition 8.8.1. *Neither $\mathfrak{P}$ nor $\neg\mathfrak{P}$ is a Markov property.*

Proof. Let S be a finitely presented semigroup. Then S embeds into $S *_{\mathrm{S}} \mathbb{N}$, which is finitely presented and $\neg\mathfrak{P}$, for the latter semigroup has no identity. On the other hand, S embeds into $\mathrm{BR}(S^1, \vartheta^*)$ which is manifestly $\mathfrak{P}$. □

Nonetheless, $\mathfrak{P}$ is undecidable for the general finitely presented semigroups.

Proposition 8.8.2. *For finitely presented semigroups, $\mathfrak{P}$ is undecidable.*

Proof. Let $S = \mathrm{Sg}\langle A : R\rangle$ be a finitely presented semigroup with unsolvable word problem. Pick $u, v \in A^+$ and construct

$$\begin{aligned} S_{u,v,x,y} &= \mathrm{Mon}\langle A, c, d, x, y : R, xy = 1, cud = 1, bcvd = cvd \text{ where } b \in A \cup \{c, d\}\rangle \\ &= S_{u,v} *_{\mathrm{M}} \mathrm{Mon}\langle x, y : xy = 1\rangle. \end{aligned}$$

We will now prove that $S_{u,v,x,y}$ is a Bruck–Reilly extension precisely when $S_{u,v}$ is trivial (in which case $S_{u,v,x,y}$ is the bicyclic monoid). The sufficiency is obvious.

Suppose now that $S_{u,v}$ is not trivial and $S_{u,v,x,y}$ is a Bruck–Reilly extension $\mathrm{BR}(M, \vartheta)$ so that every element is a triple (t^k, m, r^n) such that $rt = 1$ and $\langle r, t\rangle$ is the bicyclic monoid, and $m \in M$. Since $xy = 1$, we obtain that $x = (1, m_1, r^k)$ and $y = (t^k, m_2, 1)$ for some $k \geq 0$ and $m_1, m_2 \in M$ with $m_1 m_2 = 1_M$. We have two cases to consider:

Case 1. $k > 0$. Let w represent a canonical form in the free product for $(t, 1_M, r)$. Then since $(t, 1_M, r)\cdot(t^k, m_2, 1) = (t^k, m_2, 1)$, we have that $wy = y$. Thus $w \in \mathrm{Mon}\langle x, y \mid (xy, 1)\rangle$ and either $w = 1$ or $w = yx$. The first case is impossible, for w does not represent 1. Hence $yx = w = (t, 1_M, r)$. On the other hand, $yx = (t^k, m_2 m_1, r^k)$. So that $k = 1$ and $m_2 m_1 = 1_M$. Note that $\overline{1_M} = 1$.

We also have that there are no invertible elements in $S_{u,v}$ except 1. Indeed, in every chain of transitions from 1 to a word p there can be used only the relations from $R \cup \{cud = 1\}$. Hence, if $p \neq 1$, then p starts with c, ends with d and the corresponding subsequence of c's and d's in p forms the correct bracketing sequence. Thus if $\overline{w_1 w_2} = \overline{w_2 w_1} = \overline{1}$ and $\overline{w_1} \neq \overline{1}$, then $|w_1|_c > |w_2|_c$ and $|w_2|_c > |w_2|_c$, a contradiction.

Now, in both components $S_{u,v}$ and $\mathrm{Mon}\langle x, y : xy = 1\rangle$ there are no invertible elements except 1, hence $S_{u,v,x,y}$ does not have invertible elements but 1. Hence $m_1 = m_2 = 1$. So, $x = (1, 1, r)$ and $y = (t, 1, 1)$. Thus $yx = (t, 1, r)$. Since $S_{u,v}$ is not trivial, we have that M is not trivial (otherwise $S_{u,v,x,y}$ would coincide with $\mathrm{Mon}\langle x, y : xy = 1\rangle$). Take $m \in M \setminus \{1\}$. Now,

$$(t, m\vartheta, r) = (t, 1, r) \cdot (1, m, 1) = (1, m, 1) \cdot (t, 1, r).$$

So, if $w_0 = c_1 \cdots c_p$ is the normal form for $(1, m, 1)$ then $c_1 \in \langle x, y\rangle$. Moreover, we have that $yxc_1 = c_1$. Then $c_1 = y^e x^f$ for some $e \geq 1$ and $f \geq 0$. This implies that w_0 represents (t^g, m', r^h) for some $g \geq e$, a contradiction.

Case 2. $k = 0$. Then we have $x = (1, m_1, 1)$ and $y = (1, m_2, 1)$ with $m_1 m_2 = 1_M$. Notice that

$$(1, m_2 m_1, 1) \cdot (t, (m_2 m_1)\vartheta, r) = (t, (m_2 m_1)\vartheta \cdot (m_2 m_1)\vartheta, r) = (t, (m_2 m_1)\vartheta, r).$$

Let $w = c_1 \cdots c_p$ be the normal form for $(t, (m_2m_1)\vartheta, r)$. Since $(1, m_2m_1, 1) = yx$, we have that $c_1, c_p \in \langle x, y\rangle$. Now notice that $(t, (m_2m_1)\vartheta, r)$ is an idempotent. Hence $c_pc_1 = 1$ and so $c_1 = y^n$ and $c_p = x^n$ for some $n \geq 1$. So $w = y^n w_0 x^n$ for some w_0 which starts and ends with a component from $S_{u,v}$. Now,

$$w_0 = x^n w y^n = (t, (m_1^n)\vartheta(m_2m_1)\vartheta(m_2^n)\vartheta, r) = (t, (1_M)\vartheta, r) = (t, 1_M, r).$$

Therefore $yx \cdot w_0 = w_0 \cdot yx$, a contradiction.

Thus the word problem for finitely presented semigroups reduces to the question of being $\mathfrak{P}$ for finitely presented semigroups; thus the latter is undecidable. □

Remark 8.8.3. 'Being the bicyclic monoid' *is* a Markov property: for example, no non-trivial finitely presented group embeds into the bicyclic monoid.

Proposition 8.8.4. *The bicyclic monoid admits a unique one-relator monoid presentation (up to relabelling of generators and exchanging the two sides of the defining relation), namely* $\mathrm{Mon}\langle b, c : bc = 1\rangle$.

Before embarking on the proof, witness that this result implies that it is decidable whether a one-relator monoid is the bicylic monoid.

Proof. Let $\mathfrak{S} = \mathrm{Mon}\langle A : u = v\rangle$ be a presentation for the bicyclic monoid B.

If both u and v come from A^+, then the identity of B would not be possible to decompose in a non-trivial way, a contradiction.

So assume that $v = 1$. The alphabet A must contain at least two symbols. Furthermore, all the letters from A appear in u, since otherwise $\mathfrak{S}$ would present a proper free product, which is a contradiction. If $|A| > 2$, by the Freiheitssatz for one-relator monoids [81], we have that any two elements of $\overline{A}$ generate a free submonoid of B. But from Descalço and Ruškuc's description of all subsemigroups of B [21], it follows that B does not contain a 2-generated free subsemigroup. Therefore A is a 2-set.

Suppose that $A = \{b, c\}$. Assume without loss of generality that $u = pc$. Clearly, $p \neq 1$. If p starts with c then c is right- and left-invertible and, since the only invertible element in B is the identity, B is monogenic, which is a contradiction. So $p = bqc$ for some $q \in A^*$ and the relation has the form $bqc = 1$. Since the monoid presentation $\mathrm{Mon}\langle b, c : bqc = 1\rangle$ presents B, the group presentation $\mathrm{Gp}\langle b, c : bqc = 1\rangle$ presents $\mathbb{Z}$ [18, Corollary 1.32].

Suppose that u is not of the form b^kc^n where $k, n \geq 0$. Then $u = b^{k_1}c^{n_1} \cdots b^{k_s}c^{n_s}$ for some $k_i, n_i \geq 1$. By [52, Lemma V.11.8], $\mathbb{Z} = \mathrm{Gp}\langle b, c :$

$bqc = 1\rangle$ has a presentation $\mathfrak{H} = \mathrm{Gp}\langle x, y : y^{l_1}x^{m_1} \cdots y^{l_t}x^{m_t} = 1\rangle$ for some $t \geq s$, $l_i, m_i \in \mathbb{Z} \setminus \{0\}$, and such that either x or y has zero exponent sum. But in this case, $\mathfrak{H}$ will present an HNN-extension of a non-trivial group (see [52, Chapter IV.5]), and so cannot be $\mathbb{Z}$, which is a contradiction.

Thus $u = b^k c^n$ for some $k, n \in \mathbb{N}$. The aim is now to complete the proof by proving that $k = n = 1$.

Suppose that $n > 1$. Then $\overline{c^n b^k}$ and $\overline{cb^k c^{n-1}}$ are idempotents and, so since B is an inverse monoid, must commute. Therefore

$$\begin{aligned}
&\overline{c^n b^k} \\
&= \overline{cb^k c^n c^{n-1} b^k} && \text{(by the defining relation } b^k c^n = 1\text{)} \\
&= \overline{cb^k c^{n-1} c^n b^k} \\
&= \overline{c^n b^k c b^k c^{n-1}} && \text{(by the commutativity of the idempotents).}
\end{aligned}$$

But $\{b, c; b^k c^n = 1\}$ is a confluent noetherian rewriting system and $c^n b^k$ and $c^n b^k c b^k c^{n-1}$ are in normal forms but not equal: this is a contradiction. Therefore $n = 1$. Analogously, one can prove that $k = 1$. □

The following result follows from the proof of Proposition 8.3.5:

Corollary 8.8.5. *A one-relator semigroup is never a Bruck–Reilly extension.*

We conjecture that a one-relator monoid is a Bruck–Reilly extension if and only if it is the bicyclic monoid.

8.9 Simple? Bisimple? Semisimple?

Recall that a semigroup S is *simple* if it has no ideals other than S itself; it is *bisimple* if it consists of a single D-class. A semigroup S with a zero 0 is 0-*simple* if $S^2 \neq \{0\}$ and its only ideals are S and $\{0\}$. It is *semisimple* if every principal factor of S is 0-simple or simple. For further information about these notions we refer the reader to [18].

Proposition 8.9.1. *Neither simplicity nor non-simplicity is a Markov property; non-bisimplicity is not a Markov property.*

Proof. Every semigroup S embeds into the non-simple semigroup S^0. Thus neither non-simplicity nor non-bisimplicity is a Markov property.

On the other hand, every semigroup S embeds into the Bruck–Reilly extension $\mathrm{BR}(S^1, \vartheta)$, where $\vartheta : S^1 \to S^1$ is the trivial endomorphism: $s\vartheta = 1$ for all $s \in S^1$. Since $S^1\vartheta$ is contained in the group of units of S^1, the extension $\mathrm{BR}(S^1, \vartheta)$ is simple [45, Proposition 5.6.6(1)]. □

The question on whether bisimplicity is a Markov property remains open.

Proposition 8.9.2. *Simplicity is undecidable for finitely presented semigroups.*

Proof. Let S be a finitely presented group with unsolvable word problem and let $S = \mathrm{Mon}\langle A : R\rangle$ be a finite monoid presentation for S. Pick $v \in A^+$ and consider the monoid $S_{1,v}$. Let $I_{1,v} = S_{1,v}\overline{cvd}S_{1,v}$. If $\overline{1} = \overline{v}$, then $S_{1,v}$ is trivial and so simple.

So let $\overline{1} \neq \overline{v}$. We will prove that $\overline{1} \notin I_{1,v}$, which will yeild that S is non-simple. So, assume that $\overline{1} \in I_{1,v}$. Then there exist p, q such that $\overline{p}\overline{cvd}\overline{q} = \overline{1}$. Then $\overline{cvd}\overline{q} = \overline{1}$ and so $\overline{a} = \overline{a}\overline{cvdq} = \overline{cvdq} = \overline{1}$ for all $a \in A \cup \{c, d\}$, a contradiction.

Thus the word problem for finitely presented groups reduces to the question of simplicity for finitely presented semigroups. □

Recall that if S is semisimple and I is an ideal in S then every ideal in I is an ideal in S, see [18, Theorem 2.41].

Proposition 8.9.3. *Neither semisimplicity, nor non-semisimplicity, is a Markov property.*

Proof. Let S be a finitely presented semigroup. Then S embeds into the simple finitely presented semigroup $\mathrm{BR}(S^1, \vartheta)$, where $s\vartheta = 1$ for all $s \in S$ [45, Proposition 5.6.6(1)]. It remains to note that every simple semigroup is semisimple.

Let T be any non-semisimple finitely presented monoid (for example $T = \mathbb{N}_0$: it has an ideal $\{2, 3, \cdots\}$, in which $\{3, 5, 6, 7, \cdots\}$ is an ideal, and in T not). Then a finitely presented semigroup $S^1 \times T^1$ contains S and is not semisimple. □

Proposition 8.9.4. *Semisimplicity is undecidable for finitely presented semigroups.*

Proof. Let $S = \mathrm{Sg}\langle A : R\rangle$ be any finitely presented semigroup with insoluble word problem. Pick $u, v \in A^+$. If $\overline{u} = \overline{v}$ then $S_{u,v}$ is trivial and so semisimple.

So let $\overline{u} \neq \overline{v}$. Consider the ideal $I = S_{u,v}\overline{cd}S_{u,v}$ in $S_{u,v}$. Take the ideal $J = I\overline{cd}I$ in I. We will prove that $\overline{c^2d} \notin J$ and this will complete the proof. Suppose that $\overline{c^2d} \in J$, i.e. $\overline{c^2d} \in \overline{X^*cdX^*cdX^*cdX^*}$ where $X = A \cup \{c, d\}$. By a straightforward induction on lengths of chains, it follows that any chain of transitions starting from c^2d cannot lead to a word with a factor cpd such that $\overline{p} = \overline{v}$. Take now any chain $c^2d = w_0 \to w_1 \to \cdots \to w_{k-1} \to$

w_k to a word w_k of the form $p_1cdp_2cdp_3cdp_4$ with shortest possible length. Without loss of generality we may assume that p_1, p_2 and p_3 do not contain the factor cd. Each transition in this chain corresponds to a relation from $R \cup \{cud = 1\}$. Hence the transition $w_{k-1} \to w_k$ can be only the deletion of cud from a subword $ccudd$ of w_{k-1} which leads to some of first three factors cd appearing in w_k. By the same method as in the proof of Proposition 8.5.3 it is easy to provide a chain from c^2d to $p_1cdp_2cdp_3cdp_4$ of length less than k. □

In the proof of Proposition 8.7.2, if $S_{u,v}$ is non-trivial, then $\overline{a}$ does not lie in the same D-class as the identity and so $S_{u,v}$ is bisimple if and only if it is trivial.

Corollary 8.9.5. *Bisimplicity is undecidable for finitely presented semigroups.*

We do not know whether it is decidable for one-relator monoids to be simple (or bisimple). A one-relator semigroup is simple or bisimple if and only if it is a group:

Corollary 8.9.6. *It is decidable whether a one-relator semigroup is simple, and whether it is bisimple.*

Proof. For a non-trivial semigroup S to be simple (respectively, bisimple), each of its elements must be decomposable. Thus $S^2 = S$ and so obviously S is a group. So S is simple (respectively, bisimple) if and only if $S^2 = S$, which is decidable. □

The question of semisimplicity for one-relator semigroups and monoids remains open. The following is a partial result:

Proposition 8.9.7. *Let $S = \mathrm{Sg}\langle A : u = v\rangle$ where $|u|, |v| \geq 2$ and $|A| \geq 2$. Then S is not semisimple.*

Proof. Suppose, with the aim of obtaining a contradiction, that S is semisimple. Let $a \in A$. Let $I = S^1\overline{a}S^1$; then I is an ideal of S. Let $J = I^1\overline{a}I^1$; then J is an ideal of I. Therefore J is an ideal of S.

Let $b \in A - \{a\}$. Now, $\overline{a} \in J$ and so $\overline{ab} \in J$ (since J is an ideal). So there are words $p, q \in (A^*aA^*) \cup \{1\}$ with $\overline{paq} = \overline{ab}$. Since $q \neq b$, a sequence of transitions must lead from paq to ab. But u and v are of length at least 2, so either $u = ab$ or $v = ab$; assume, without loss of generality $u = ab$.

Similarly, $\overline{ba} \in J$ for any $b \in A$, which forces $v = ba$, and, furthermore, $|A| = 2$ (otherwise S would split into a semigroup free product with one factor being a free semigroup, and so would not be semisimple). Thus

$$S = \mathrm{Sg}\langle A : ab = ba\rangle = \mathbb{N}_0 \times \mathbb{N}_0 - \{(0,0)\}.$$

Let $T = \{(x, y) : x \geq 2 \wedge y \geq 2\}$; then T is an ideal of S. Let $U = T - \{(x, y) : x = 3 \vee y = 3\}$. Then U is an ideal of T but not of S. Therefore S is not semisimple, which is a contradiction; this completes the proof. □

8.10 Hopfian?

Proposition 8.10.1. *Neither hopficity nor non-hopficity is a Markov property.*

Proof. Consider an arbitrary finitely presented semigroup S. Let T be a non-hopfian semigroup. Then S embeds into $S *_{\mathrm{S}} T$, which is non-hopfian since any non-injective surjection from T onto itself can be extended in a natural way to a non-injective surjection from $S *_{\mathrm{S}} T$ onto itself.

Let S be presented by $\mathrm{Sg}\langle A : R\rangle$, where $A = \{a_1, \ldots, a_n\}$. Let $C = \{c, d\}$ and in each relation from R replace each letter a_i with cd^i and denote the resulting relations by R'. Let T be the semigroup $\mathrm{Sg}\langle C : R'\rangle$. Notice that, since c and d are indecomposable in T, the only non-trivial surjective endomorphism ϑ of T onto itself could be those which is given by $c \mapsto d$ and $d \mapsto c$, but then ϑ^2 would be the identity mapping and so ϑ is injective. Hence T is hopfian. It remains to note that the subsemigroup in T, generated by $\{cd^i : 1 \leq i \leq n\}$, is isomorphic to S. □

Proposition 8.10.2. *Hopficity is undecidable for finitely presented semigroups.*

Proof. Consider the Baumslag-Solitar group $B = \mathrm{Gp}\langle x, y : yx^3 = x^2y\rangle$. Then the mapping $\vartheta : B \to B$ extending $\overline{x} \mapsto \overline{x^2}$, $\overline{y} \mapsto \overline{y}$ is a surjective endomorphism of B (see [52]).

Now consider an arbitrary finitely presented group G with insoluble word problem. Take any finite monoid presentation $\mathrm{Mon}\langle A : R\rangle$ for G. Let $S = G \times B$. Choose $v \in A^*$ and form the monoid $S_{1,v}$.

Now, if $\overline{v} = \overline{1}$, then $S_{1,v}$ is trivial and so hopfian. Suppose that $\overline{v} \neq \overline{1}$. Then S embeds into $S_{1,v}$. Notice that $S_{1,v}$ is generated by $\overline{A} \cup \overline{\{c, d, x, x^{-1}, y, y^{-1}\}}$ and define the mapping $\vartheta^* : S_{1,v} \to S_{1,v}$ by extending $\vartheta : B \to B$ by setting $\overline{a}\vartheta^* = \overline{a}$ for $a \in A \cup \{c, d\}$. Then ϑ^* is a surjective endomorphism of $S_{1,v}$, but ϑ^* is not injective since ϑ is not injective on B. Thus, when $\overline{v} \neq \overline{1}$, the semigroup $S_{1,v}$ is non-hopfian.

Since the word problem for G is insoluble, hopficity is undecidable for finitely presented semigroups. □

Chapter 9

Open problems

Open Problem 9.1. Let T be a subsemigroup of finite Rees index in a semigroup S, and let S have Bergman's property. Does T then have Bergman's property?

Open Problem 9.2. Are all Cayley automaton semigroups $\mathcal{H}$-trivial?

Open Problem 9.3. Let T be a subsemigroup in a semigroup S with finite Green index. Let also S be regular and $\mathcal{J} = \mathcal{D}$ in S. Is it true then that $\mathcal{J} = \mathcal{D}$ in T?

Open Problem 9.4. Is it true that if a finitely generated semigroup S has a hopfian subsemigroup T of finite Green index then S itself must be hopfian?

Open Problem 9.5. Let T be a subsemigroup of finite Green index in a semigroup S. Let also S be Markov. Is T Markov?

Open Problem 9.6. Is hopficity decidable for one-relation semigroups (or one relator groups)?

Open Problem 9.7. Is residual finiteness decidable for one-relation semigroups (or one relator groups)?

Open Problem 9.8. Is every one-relation semigroup Markov?

Open Problem 9.9. Are $\mathcal{J} = \mathcal{D}$, regularity and bisimplicity Markov properties?

Finally, let us pose 'the problem' of Combinatorial Semigroup Theory:

Open Problem 9.10. Is the word problem for one-relation monoids decidable?

Bibliography

[1] S. I. Adjan, Defining relations and algorithmic problems for groups and semigroups, *Proceedings of the Steklov Institute of Mathematics* **85**, *American Mathematical Society* (1966). [Translated from the Russian by M. Greendlinger]

[2] S. I. Adyan, V. G. Durnev, Algorithmic problems for groups and semigroups, *Uspekhi Mat. Nauk* **55** (2000), 3–94.

[3] S. I. Adyan, G. U. Oganesyan, On the word and divisibility problems for semigroups with one relation, *Mat. Zametki* **41** (1987), 412–421.

[4] J. Araújo, J. D. Mitchell, Relative ranks in the semigroup of endomorphisms of an independence algebra, *Monatsh. Math.* **151** (2007), 1–10.

[5] J. Araújo, J. D. Mitchell, N. Silva, On generating countable sets of endomorphisms, *Algebra Universalis* **50** (2003), 61–67.

[6] M. Arbib, K. Krohn, J. L. Rhodes, Algebraic theory of machines, languages and semigroups, *Academic Press, New York* (1968).

[7] G. Baumslag, and D. Solitar, Some two-generator one-relator non-Hopfian groups, *Bull. Amer. Math. Soc.* **68** (1962), 199–201.

[8] G. M. Bergman, Generating infinite symmetric groups, *Bull. London Math. Soc.* **38** (2006), 429–440.

[9] R. V. Book and F. Otto, String-Rewriting Systems, *Springer, New York* (1993).

[10] A. Cain, Presentations for Subsemigroups of Groups, Ph.D. Thesis, University of St Andrews, 2005.

[11] A. Cain, Automaton semigroups, *Theoret. Comp. Sci.* **410** (2009), 5022-5038.

[12] A. Cain, Hyperbolicity of monoids presented by confluent monadic rewriting systems, submitted.

[13] A. Cain, R. Gray and N. Ruškuc, Green index in semigroup theory: generators, presentations, and automatic structures, submitted.

[14] A. Cain, V. Maltcev, Decision problems for finitely presented and one-relation semigroups and monoids, *Internat. J. Algebra and Comput.* **19** (2009), 747–770.

[15] A. Cain, V. Maltcev, Markov semigroups, monoids, and groups, submitted.

[16] A. J. Cain, V. Maltcev, Context-free rewriting systems and word-hyperbolic structures with uniqueness, submitted.

[17] C. M. Campbell, E. F. Robertson, N. Ruškuc, R. M. Thomas, Reidemeister-Schreier type rewriting for semigroups, *Semigroup Forum* **51** (1995), 47–62.

[18] A. H. Clifford, G. B. Preston, The algebraic theory of semigroups. Vol. I, *American Mathematical Society, Providence, R.I.* (1961).

[19] A. H. Clifford, G. B. Preston, The Algebraic Theory of Semigroups. Vol. II, *American Mathematical Society, Providence, R.I.* (1967).

[20] Y. de Cornulier, Strongly bounded groups and infinite powers of finite groups, *Comm. Algebra* **34** (2006), 2337–2345.

[21] L. Descalço, N. Ruškuc, Subsemigroups of the bicyclic monoid, *Internat. J. Algebra Comput.* **15** (2005), 37–57.

[22] M. Droste, R. Göbel, Uncountable cofinalities of permutation groups, *J. London Math. Soc.* **71** (2005), 335–344.

[23] M. Droste, W. C. Holland, G. Ulbrich, On full groups of measure-preserving and ergodic transformations with uncountable cofinalities, *Bull. Lond. Math. Soc.* **40** (2008), 463–472.

[24] A. Duncan, R. H. Gilman, Word hyperbolic semigroups. *Math. Proc. Cambridge Philos. Soc.*, **136** (2004), 513–524.

[25] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, W. P. Thurston, Word Processing in Groups (1992).

[26] P. Gallagher, On the finite and non-finite generation of finitary power semigroups, *Semigroup Forum* **71** (2005), 481–494.

[27] P. Gallagher, On finite generation and presentability of diagonal acts, finitary power semigroups and Schützenberger products, Ph.D. Thesis, University of St Andrews, 2005.

[28] P. Gallagher, N. Ruškuc, Finitary power semigroups of infinite groups are not finitely generated, *Bull. London Math. Soc.* **37** (2005), 386–390.

[29] F. Galvin, Generating countable sets of permutations, *J. London Math. Soc.* **51** (1995), 230–242.

[30] É. Ghys, P. de la Harpe, La propriété de Markov pour les groupes hyperboliques, *In Ghys & de la Harpe*, 165–187.

[31] R. H. Gilman, On the definition of word hyperbolic groups. *Math. Z.*, **242** (2002), 529–541.

[32] R. Gray, V. Maltcev, J. Mitchell, N. Ruškuc, Ideals, finiteness conditions and Green index for subsemigroups, submitted.

[33] R. Gray, N. Ruškuc, Green index and finiteness conditions for semigroups, *J. Algebra* **320** (2008), 3145–3164.

[34] R. I. Grigorchuk, Semigroups with cancellations of degree growth (Russian), *Mat. Zametki* **43** (1988), 305–319.

[35] R. I. Grigorchuk, A. Żuk, The lamplighter group as a group generated by a 2-state automaton, and its spectrum, *Geom. Dedicata* **87** (2001), 209–244.

[36] M. Gromov, Groups of Polynomial growth and Expanding Maps, *Publications mathematiques I.H.E.S.* **53** (1981).

[37] M. Gromov, Hyperbolic groups. In S. M. Gersten, ed., *Essays in group theory* **8** (1987), 75–263.

[38] P. M. Higgins, Techniques of semigroup theory, *Oxford Science Publications, New York* (1992).

[39] P. M. Higgins, J. M. Howie, J. D. Mitchell, N. Ruškuc, Countable versus uncountable ranks in infinite semigroups of transformations and relations, *Proc. Edinb. Math. Soc.* **46** (2003), 531–544.

[40] G. Higman, E. Scott, Existentially closed groups, *LMS Monographs, Oxford University Press, New York* (1988).

[41] R. Hirshon, Some theorems on hopficity, *Trans. Amer. Math. Soc.* **141** (1969), 229–244.

[42] M. Hoffmann, N. Ruškuc, R. M. Thomas, Automatic semigroups with subsemigroups of finite Rees index, *Internat. J. Algebra Comput.* **12**(3) (2002), 463–476.

[43] J. E. Hopcroft, J. D. Ullman, Introduction to Automata Theory, Languages, and Computation, *Addison–Wesley* (1979).

[44] H. Hopf, Beiträge zur Klassifizierung der Flächenabbildungen, *J. Reine Angew. Math.* **165** (1931), 225–236.

[45] J. M. Howie, Fundamentals of Semigroup Theory, *Clarendon Press, Oxford* (1995).

[46] S. V. Ivanov, S. W. Margolis, J. C. Meakin, On one-relator inverse monoids and one-relator groups, *J. Pure Appl. Algebra* **159** (2001), 83–111.

[47] A. Jura, Determining ideals of a given finite index in a finitely presented semigroup, *Demonstratio Mathematica* **11** (1978), 813–827.

[48] A. S. Kechris, C. Rosendal, Turbulence, amalgamation, and generic automorphisms of homogeneous structures, *Proc. Lond. Math. Soc.* **94** (2007), 302–350.

[49] A. Khelif, À propos de la propriété de Bergman, *C. R. Math. Acad. Sci. Paris* **342** (2006), 377–380.

[50] G. Lallement, On monoids presented by a single relation, *J. Algebra* **32** (1974), 370–388.

[51] G. Lallement, Semigroups and combinatorial applications, *John Wiley & Sons* (1979).

[52] R. C. Lyndon, P. E. Schupp, Combinatorial Group Theory, *Springer-Verlag* (1977).

[53] R. C. Lyndon, M. P. Schützenberger, The equation $a^M = b^N c^P$ in a free group, *Michigan Math. J.* **9** (1962), 289–298.

[54] H. D. Macpherson, P. M. Neumann, Subgroups of infinite symmetric groups, *J. London Math. Soc.* **42** (1990), 64–84.

[55] W. Magnus, Das Identitätsproblem für Gruppen mit einer definierenden Relation, *Math. Ann.* **106** (1932), 295–307.

[56] A.I. Malcev, On isomorphic matrix representations of infinite groups, *Mat. Sb* **8** (1940), 405–422.

[57] A. Malheiro, Finite derivation type for large ideals, *Semigroup Forum* **78** (2009), 450–485.

[58] V. Maltcev, Cayley automaton semigroups, *Internat. J. Algebra Comput.* **19** (2009), 79–95.

[59] V. Maltcev, J. D. Mitchell, N. Ruškuc, The Bergman property for semigroups, *J. London Math. Soc.* **80** (2009), 212-232.

[60] V. Maltcev, N. Ruškuc, Hopfian property and Rees index for semigroups, submitted.

[61] A. Markoff, On the impossibility of certain algorithms in the theory of associative systems, *Doklady Acad. Sci. USSR* **55** (1947), 583–586.

[62] Yu. Matiyasevich, Word problem for Thue systems with a few relations, *Lecture Notes in Comput. Sci., Springer* (1995).

[63] Z. Mesyan, Generating self-map monoids of infinite sets, *Semigroup Forum* **75** (2007), 649–676.

[64] A. Mintz, On the Cayley semigroup of a finite aperiodic semigroup, to appear in *Internat. J. Algebra and Comput.* **19** (2009), 723–746.

[65] J. D. Mitchell, Y. Péresse, M. R. Quick, Generating sequences of functions, *Q. J. Math.* **58** (2007), 71–79.

[66] D. E. Muller, P. E. Schupp, Groups, the geometry of ends, and context-free languages, *J. of Computer and System Sci.* **26** (1983), 295–310.

[67] V. Nekrashevych, Self-similar groups, *Mathematical Surveys and Monographs* **117** *American Mathematical Society, Providence, RI* (2005).

[68] B. H. Neumann, Algebraically closed semigroups, *Studies in Pure Mathematics, Academic Press, London* (1971), 185–194.

[69] F. Otto, M. Katsura, Y. Kobayashi, Infinite convergent string-rewriting systems and cross-sections for finitely presented monoids, *J. Symbolic Comput.* **26** (1998), 621–648.

[70] D. Perrin, J.-E. Pin, Infinite words: automata, semigroups, logic and games, *Elsevier Academic Press, Amsterdam* (2004).

[71] E. L. Post, Recursive unsolvability of a problem of Thue, *J. Symbolic Logic* **12** (1947), 1–11.

[72] J. H. Remmers, On the geometry of semigroup presentations, *Adv. in Math.* **36** (1980), 283–296.

[73] E. F. Robertson, N. Ruškuc, M. R. Thomson, On diagonal acts of monoids, *Bull. Austral. Math. Soc.* **63** (2001), 167–175.

[74] N. Ruškuc, Semigroup Presentations, University of St Andrews, Ph.D. Thesis, 1995.

[75] N. Ruškuc, On large subsemigroups and finiteness conditions of semigroups, *Proc. London Math. Soc.* **76** (1998), 383–405.

[76] N. Ruškuc, R. M. Thomas, Syntactic and Rees indices of subsemigroups, *Journal of Algebra* **205** (1998), 435–450.

[77] M. Sapir, Residual properties of 1-relator groups, *Groups St Andrews, Bath* (2009), to appear.

[78] W. R. Scott, Algebraically closed groups, *Proc. Amer. Math. Soc.* **2** (1951), 118–121.

[79] W. Sierpiński, Sur les suites infinies de fonctions définies dans les ensembles quelconques, *Fund. Math.* **24** (1935), 209–212.

[80] P. V. Silva, B. Steinberg, On a class of automata groups generalizing lamplighter groups, *Internat. J. Algebra Comput.* **15** (2005), 1213–1234.

[81] C. Squier, C. Wrathall, The Freiheitssatz for one-relation monoids, *Proc. Amer. Math. Soc.* **89** (1983), 423–424.

[82] A. D. Wallace, Relative ideals in semigroups. II. The relations of Green, *Acta Math. Acad. Sci. Hungar* **14** (1963), 137-148.

[83] J. Wang, Finite complete rewriting systems and finite derivation type for small extensions of monoids, *J. Algebra* **204** (1998), 493–503.

[84] K.B. Wong, P. C. Wong, On finite complete rewriting systems and large subsemigroups, preprint, `arXiv:1005.0882v1`.