CAYLEY AUTOMATON SEMIGROUPS

Alexander Lewis Andrew McLeman

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

2015

Cayley Automaton Semigroups

Alexander Lewis Andrew McLeman

University of
St Andrews

This thesis is submitted in partial fulfilment for the degree of

PhD at the University of St Andrews

January 5, 2015

Abstract

Let S be a semigroup, $\mathcal{C}(S)$ the automaton constructed from the right Cayley graph of S with respect to all of S as the generating set and $\Sigma(\mathcal{C}(S))$ the automaton semigroup constructed from $\mathcal{C}(S)$. Such semigroups are termed *Cayley automaton semigroups*. For a given semigroup S we aim to establish connections between S and $\Sigma(\mathcal{C}(S))$.

For a finite monogenic semigroup S with a non-trivial cyclic subgroup C_n we show that $\Sigma(\mathcal{C}(S))$ is a small extension of a free semigroup of rank n, and that in the case of a trivial subgroup $\Sigma(\mathcal{C}(S))$ is finite.

The notion of invariance is considered and we examine those semigroups S satisfying $S \cong \Sigma(\mathcal{C}(S))$. We classify which bands satisfy this, showing that they are those bands with faithful left-regular representations, but exhibit examples outwith this classification. In doing so we answer an open problem of Cain.

Following this, we consider iterations of the construction and show that for any n there exists a semigroup where we can iterate the construction n times before reaching a semigroup satisfying $S \cong \Sigma(\mathcal{C}(S))$. We also give an example of a semigroup where repeated iteration never produces a semigroup satisfying $S \cong \Sigma(\mathcal{C}(S))$.

Cayley automaton semigroups of infinite semigroups are also considered and we generalise and extend a result of Silva and Steinberg to cancellative semigroups. We also construct the Cayley automaton semigroup of the bicyclic monoid, showing in particular that it is not finitely generated.

Candidate's Declarations

I, Alexander McLeman, hereby certify that this thesis, which is approximately 47000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for a higher degree.

I was admitted as a research student in September 2010 and as a candidate for the degree of Ph.D in September 2011; the higher study for which this is a record was carried out in the University of St Andrews between 2010 and 2014.

Date:

Signature of Candidate:

Supervisors' Declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Ph.D 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:

Date:

Signature of Supervisor:

Permission for Publication

In submitting this thesis to the University of St Andrews I understand that I am 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. I 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 my 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 my thesis into new electronic forms as required to ensure continued access to the thesis. I 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 the candidate and supervisors regarding the publication of this thesis:

PRINTED COPY

No embargo on print copy.

ELECTRONIC COPY

No embargo on electronic copy.

Date:

Signature of candidate:

Date:

Signature of supervisor:

Date:

Signature of supervisor:

Acknowledgements

My eight years in St Andrews would not have been possible without the unconditional support, both moral and financial, of my parents and grandparents. Thanks must also go to my supervisors Nik and Collin for all their help throughout the PhD, especially at the times when finding results seemed impossible, and also to Alan Cain for his many helpful comments in the final stages of writing. I am also grateful to Valerie and Tricia for basically running the department.

The Ginger Office has been a great place to work for the last four years and that is in no small part due to my fantastic office mates Rachael, Julius and Dan. I will miss our office cake days. Special thanks go to Julius for being a wonderful housemate, travelling companion and drinking buddy during my final year.

Several others that I have encountered along the way deserve a mention: thanks go to Jenni, for always lowering the tone; James, for the endless stream of (in)appropriate banter; Sam, for some of the scariest car trips of my life; Sascha, for all the stories about his dad; Tom, for always providing crosswords; Artur, for getting married thus allowing us to have a stag party; Abel, for being the butt of many jokes; Casey, for being a stalwart of A Monster Called Pickles, and Anna, for being the one with a work ethic.

The Trampoline Club has been a huge part of my time at St Andrews and it would be remiss of me not to mention it here. I've met some great people as part of the club and I'm sad to be leaving it behind, despite it at times causing me more stress than a maths PhD ever could.

I apologise for missing anyone who deserved to be mentioned here. I'm quite sure there are a few.

Contents

Chapter 1

Introduction and Preliminary Semigroup Theory

Automaton groups are groups of automorphisms of labelled rooted trees generated by actions of automata. One of the first examples of these groups was the infinite periodic group constructed by Aleshin as a means of providing a solution to the Burnside Problem (that is, is every finitely generated group in which each element has finite order necessarily finite?) – see [2]. Many other examples followed in the years after this, including Grigorchuk's example of a group with intermediate growth [16] and the Gupta–Sidki group [19]. A significant theory has developed featuring prominent works by authors such as Nekrashevych [29], Grigorchuk, Bartholdi and Šunić [4, 5, 18]. In recent years, research in this area has included topics such as applications of these groups to fractal sets and dynamical systems (see, for example, [6]).

Automaton semigroups are the natural generalisation of automaton groups. They are semigroups of endomorphisms of labelled rooted trees generated by actions of automata. The study of these objects is much more recent than that of automaton groups, with some of the early work in this area being carried out by Silva and Steinberg [32] and Grigorchuk, Nekrashevych and Sushchanskii [17]. More recently, further work has been carried out by, for example, Cain [7], Akhavi, Klimann [1] and McCune [26].

One particular class of automata that has received attention in recent years (see [7, 25, 28]) is the class of *Cayley automaton*. These are automata that intuitively are constructed from the Cayley graphs of semigroups with the transitions in the automata being defined by the multiplication in the semigroups. These semigroups, despite a recent increase in the attention they have received, have their foundations in the works of Krohn and Rhodes [3, 22]. A *Cayley automaton semigroup*, denoted $\Sigma(\mathcal{C}(S))$, is an automaton semigroup constructed from such an automaton. The overarching theme of the research in this particular area is to establish connections between a semigroup and the Cayley automaton semigroup constructed from it. For example, considerable effort has gone into establishing precisely when, for the class of finite semigroups, the Cayley automaton semigroups constructed from semigroups in this class are finite (see Theorem 3.5).

In this thesis we seek to extend the theory in the area of Cayley automaton semigroups. Preliminary semigroup theory is given in this chapter, followed by the basics of automaton semigroup theory in Chapter 2. There we will see how an automaton semigroup is constructed from a given automaton before presenting an overview of some of the main results that are known in the literature (such as all automaton semigroups are residually finite (Proposition 2.7) and that all free semigroups of rank at least two are automaton semigroups (Proposition 2.9)). This chapter should provide a good grounding in automaton semigroup theory before we specialise in Cayley automaton.

In Chapter 3 we define Cayley automata and the semigroups constructed from them, which will form the foundation for the remainder of the thesis. We will see how the Cayley Table of a semigroup can naturally be viewed as an automaton; equivalently, the Cayley automaton can be constructed from the (right) Cayley graph of the semigroup with transitions defined by (right) multiplication in the semigroup. Of fundamental importance in this field are results by Silva and Steinberg (Theorem 3.4 - for a finite non-trivial group G, $\Sigma(\mathcal{C}(G))$ is free) and by Mintz (Theorem 3.5 - for a finite semigroup S, $\Sigma(\mathcal{C}(S))$ is finite and aperiodic if and only if S is aperiodic). These results, presented in Chapter 3 will be used frequently throughout this thesis. Some elementary classes of semigroups (such as left- and right-zero semigroups and rectangular bands) will be considered and their Cayley automaton semigroups constructed. After classifying these, we turn our attention to examining how basic semigroup constructions (such as the direct product) are related to the Cayley automaton construction. The results obtained in this section will be used throughout the thesis.

Chapter 4 considers the Cayley automaton semigroups constructed from elements of a particular class of semigroups - the finite monogenic semigroups. We split into two cases, considering first those monogenic semigroups with non-trivial subgroups and then those with trivial subgroups. In the first case, we show that the Cayley automaton semigroup is a small extension of a free semigroup F_n for some n and that there is a close connection between the order of the cyclic subgroup $C_n \leq S$ and which words over the generators of $\Sigma(\mathcal{C}(S))$ coincide in $\Sigma(\mathcal{C}(S)) \setminus F_n$. In the case of trivial subgroups, we know that by Mintz's result above (Theorem 3.5) $\Sigma(\mathcal{C}(S))$ will be finite. The order of the semigroup completely determines which words over the generators of $\Sigma(\mathcal{C}(S))$ coincide and we use this to determine $\Sigma(\mathcal{C}(S))$. Since every finite semigroup contains finite monogenic subsemigroups, understanding the Cayley automaton semigroups of the monogenic semigroups may help with determining $\Sigma(\mathcal{C}(S))$ for an arbitrary finite S.

Chapter 5 considers those semigroups that are invariant under the Cayley automaton construction. In discussing these so-called *self-automaton semigroups*, we will see how the class of bands provides a plentiful source of these semigroups (as all bands with a faithful left-regular representation are self-automaton - Theorem 5.10) but that there are self-automaton semigroups outwith this class. Considering Cain's treatment of the motivating question for this chapter - can the self-automaton semigroups be classified? - we present his original notion of a self-automaton semigroup in the framework of this thesis before resolving an open problem he poses in [7] (Open Problem 5.1) where he suggests that the self-automaton semigroups are precisely the finite bands with square $\mathcal{D}$-classes in which every maximal $\mathcal{D}$-class is a singleton.

After examining which semigroups are invariant under one iteration of the Cayley automaton construction, it is natural to explore the cases where several iterations of the construction can be considered. These sequences, or *Cayley chains*, of semigroups obtained by repeatedly iterating the construction are the object of focus in Chapter 6. We will see how to construct a chain of any arbitrary finite length and exhibit an example of a finite semigroup with an infinite Cayley chain (which resolves a question posed by Maltcev in [25] where he asks if every Cayley chain is finite). Connections between the length of the Cayley chain of a semigroup S and the length of the chain of a subsemigroup of S will be discussed.

The vast majority of the work in this thesis concerns Cayley automaton semigroups arising from finite semigroups. We conclude the main body of the thesis by considering how the construction can be applied to infinite semigroups in Chapter 7. We are able to completely classify the Cayley automaton semigroups arising from infinite cancellative semigroups (we show that they are all free - Theorem 7.6) and, after looking at some general results, consider the special case of the Bicyclic Monoid.

Finally, in Chapter 8 we present some further questions relating to the work that has been carried out in this thesis.

1.1 Preliminary Semigroup Theory

This section will introduce and define the basic semigroup theory that will be used throughout this thesis. Further details on the material given here can be found in [9] and [21].

Throughout, we adopt the convention that $\mathbb{N} = \{1, 2, 3, \ldots\}$.

A *semigroup* is a set S with an associative binary operation $\cdot : S \times S \to S$. We will assume throughout that all semigroups are non-empty. For $s, t \in S$, we usually write the product $s \cdot t$ as st. A semigroup is said to be *commutative* if $st = ts$ for all $s, t \in S$. An element $1 \in S$ is called an *identity* if, for all $s \in S$ we have $1s = s1 = s$. A semigroup containing such an identity element is called a *monoid*. A monoid in which, for each $s \in S$ there exists a unique $s^{-1} \in S$ such that $ss^{-1} = s^{-1}s = 1$ is called a *group*.

Unlike a group, a semigroup does not necessarily contain an identity element. We denote the monoid obtained from the semigroup S by adjoining an identity element 1 by S^1. It is routine to verify that $S^1 = S \cup \{1\}$ is a monoid. Identity elements are necessarily unique.

An element $z \in S$ satisfying $zs = z$ for all $s \in S$ is called a *left-zero*. If $z \in S$ satisfies $sz = z$ for all $s \in S$ then z is a *right-zero*. An element which is both a left- and a right-zero is called a *two-sided zero*, or simply a zero. It is easy to show that if a semigroup has a two-sided zero element then it is unique. If S does not have a zero element then we may adjoin one and obtain a new semigroup $S^0 = S \cup \{0\}$ which satisfies $s0 = 0s = 0^2 = 0$ for all $s \in S$. A semigroup in which every element is a left- (resp. right-) zero is called a *left- (resp. right-) zero semigroup* (denoted L_n and R_n respectively in the finite cases, where $n \in \mathbb{N}$ is the size of the semigroup). Semigroups with a zero element 0 satisfying $st = 0$ for all $s, t \in S$ are called *zero* or *null semigroups*, denoted Z_n, where $n \in \mathbb{N}$ is the size of the semigroup.

A subset $T \subseteq S$ is a *subsemigroup* of S (denoted $T \leq S$) if T forms a semigroup under the operation inherited from S. Submonoids and subgroups are defined analogously. A semigroup S is a *small extension* of a subsemigroup T if $|S \setminus T| < \infty$. A non-empty subsemigroup T satisfying $st \in T$ for all $s \in S$ and $t \in T$ is a *right ideal.* A *left ideal* is a subsemigroup T satisfying $ts \in T$ for all $s \in S$ and $t \in T$. A subsemigroup which is both a right and a left ideal is a *two-sided ideal* or simply an *ideal* for short. An ideal I is *proper* if $I \neq S$ and, in the case when S has a zero element, $I \neq \{0\}$. For an ideal $I \subseteq S$, the *Rees factor semigroup* S/I is the set $(S \setminus I) \cup \{0\}$ where multiplication is defined by $s \cdot t = st$ if s, t and st are in $S \setminus I$ and 0 otherwise.

Every finite semigroup contains a unique minimal ideal (that is, it has no proper ideals strictly contained in it). This ideal takes the form of a *Rees-Matrix semigroup* which is constructed as follows: let I, Λ be non-empty sets, G be a group and $P = (p_{\lambda i})$ be a $\Lambda \times I$ matrix with entries in G. Then the Rees-Matrix semigroup is the set $I \times G \times \Lambda$ with multiplication defined by $(i_1, g_1, \lambda_1)(i_2, g_2, \lambda_2) = (i_1, g_1 p_{\lambda_1 i_2} g_2, \lambda_2)$. Such a Rees-Matrix semigroup is denoted as $\mathcal{M}[G; I, \Lambda; P]$.

The *direct product* of two semigroups S and T is the set $S \times T$ with the operation $(s_1, t_1)(s_2, t_2) = (s_1 s_2, t_1 t_2)$.

An element $s \in S$ satisfying $s^2 = s$ is called an *idempotent* and semigroups in which each element is an idempotent are called *bands*. Left- and right-zero semigroups are examples of bands. A *rectangular band* is a semigroup of the form $I \times J$ where I, J are sets and $(i_1, j_1)(i_2, j_2) = (i_1, j_2)$ for all $i_1, i_2 \in I$ and $j_1, j_2 \in J$. Observe that a rectangular band is just a Rees-Matrix semigroup in which the group is trivial, or equivalently, the direct product of a left- and a right-zero semigroup. An element $s \in S$ is called *regular* if there exists $t \in S$ such that $sts = s$. Note that every idempotent is regular.

Let $A \subseteq S$. Then the set of all elements of S that can be expressed as a finite product of elements in A is the *subsemigroup generated by* A, denoted $\langle A \rangle$. The set A is referred to as a *generating set*. If the set A is finite then $\langle A \rangle$ is *finitely generated*. A semigroup S is finitely generated if there exists *any* finite subset A such that $S = \langle A \rangle$ and is said to be *monogenic* if there exists a generating set of size one. The *right Cayley graph* with respect to a finite generating set A is the graph with vertex set $\{s : s \in S\}$ and a directed edge from s to t labelled by $a \in A$ if and only if $t = sa$. The left Cayley graph with respect to A is defined analogously.

A function $f : S \to T$ between two semigroups is a *homomorphism* if $f(s_1)f(s_2) = f(s_1 s_2)$ for all $s_1, s_2 \in S$. A homomorphism f is a *monomorphism* if it is injective and an *epimorphism* if it is surjective. A homomorphism which is both injective and surjective is an *isomorphism*. If $f : S \to S$

is a homomorphism then f is an *endomorphism*. An isomorphism $S \to S$ is called an *automorphism*. A semigroup T is a *divisor* of a semigroup S if there exists a subsemigroup U of S such that T is a homomorphic image of U.

A function f satisfying $f(s_1)f(s_2) = f(s_2 s_1)$ is called an *anti-homomorphism*. The analogues of the maps named above are defined in the obvious way.

The set of all functions from a set X to itself under composition forms a semigroup called the *full transformation semigroup on* X, denoted $\mathcal{T}_X$. This semigroup is in fact a monoid and every semigroup is isomorphic to a subsemigroup of some transformation semigroup.

An equivalence relation ρ on S is called a *congruence* if for all $(s,t),(u,v) \in \rho$ we have $(su, tv) \in \rho$. For a congruence ρ, the *congruence class* of an element $s \in S$ is the set $[s] = \{t \in S : s\rho t\}$ and the set S/ρ of congruence classes is a semigroup under the operation $[s_1][s_2] = [s_1 s_2]$ called the *quotient of* S *by* ρ. The *free semigroup* on a non-empty set A is the set of all finite non-empty words over A under concatenation of words. Finitely generated free semigroups will be denoted F_n where $|A| = n$.

If A is a generating set for S then there is a map $\phi : A \to S$ defined by $\phi(a) = a$ for all $a \in A$. There exists an epimorphism $\psi : F_{|A|} \twoheadrightarrow S$ given by $\psi(a_1 a_2 \dots a_n) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$ and so $S \cong F_{|A|}/\ker\psi$ (where $\ker\psi = \{(a,b) \in S \times S : \psi(a) = \psi(b)\}$ and is a congruence). If $|A| = n < \infty$ and there exists a finite set $R = \{(w_1, z_1), (w_2, z_2), \dots, (w_r, z_r)\}$ of elements in $F_{|A|} \times F_{|A|}$ such that the smallest congruence containing R is $\ker \psi$ then we say that S is *finitely presented* with presentation

$$\langle a_1, a_2, \ldots, a_n | w_1 = z_1, w_2 = z_2, \ldots, w_r = z_r \rangle.$$

For a semigroup S and $n \in \mathbb{N}$ (where $n \geq 2$), we have the set $S^n = \{s_1 s_2 \ldots s_n : s_i \in S\}$ of all products of length n in S. The set $S \setminus S^2$ consists of all *indecomposable elements* in S. These elements must be present in any generating set for S. If a semigroup with a zero element 0 satisfies $S^n = \{0\}$ but $S^{n-1} \neq \{0\}$ for some n then S is said to be *nilpotent of class* n. A semigroup is nilpotent of class 1 if and only if it is trivial.

Green's $\mathcal{L}$-relation is defined by $a\mathcal{L}b$ if and only if $S^1 a = S^1 b$ for $a, b \in S$. Similarly, *Green's $\mathcal{R}$-relation* is defined by $a\mathcal{R}b$ if and only if $aS^1 = bS^1$ for $a, b \in S$. Equivalently, we have $a\mathcal{L}b$ if and only if there exist $x, y \in S^1$ such that $xa = b$ and $yb = a$ and $a\mathcal{R}b$ if and only if there exist $u, v \in S^1$ such that $au = b$ and $bv = a$. The intersection of $\mathcal{L}$ and $\mathcal{R}$ is *Green's $\mathcal{H}$-relation* so we have $a\mathcal{H}b$ if and only if $a\mathcal{L}b$ and $a\mathcal{R}b$. The composition of $\mathcal{L}$ and $\mathcal{R}$ is *Green's $\mathcal{D}$-relation* and we have $a\mathcal{D}b$ if and only if there exists c such that $a\mathcal{L}c$ and $c\mathcal{R}b$. Finally, *Green's $\mathcal{J}$-relation* is defined by $a\mathcal{J}b$ if and only if $S^1 a S^1 = S^1 b S^1$. In finite semigroups we have that $\mathcal{D} = \mathcal{J}$ and so in this case we will say that $a\mathcal{D}b$ if and only if $S^1 a S^1 = S^1 b S^1$.

There is a natural partial order on the $\mathcal{J}$-classes of a semigroup S. We denote the $\mathcal{J}$-class containing a by J_a and we have that $J_a \leq J_b$ if and only if $S^1aS^1 \subseteq S^1bS^1$. The partial orders for $\mathcal{L}$ and $\mathcal{R}$ are defined similarly. The partial order for $\mathcal{J}$ is illustrated visually by an *egg-box diagram*. In the case when S is finite we have that $\mathcal{D} = \mathcal{J}$ and so we may instead consider this as a partial order on the $\mathcal{D}$-classes.

A semigroup is *right-cancellative* if for all $a, b, c \in S$ we have $ac = bc \implies a = b$ and it is *left-cancellative* if $ca = cb \implies a = b$. A semigroup that is both left- and right-cancellative is a *cancellative* semigroup. A finite semigroup is cancellative if and only if it is a group. A semigroup is called *aperiodic* if for each $s \in S$ there exists $n \in \mathbb{N}$ such that $s^n = s^{n+1}$. Equivalently, for finite semigroups, a semigroup is aperiodic if it contains no non-trivial subgroups or every $\mathcal{H}$-class is trivial.

A *left-action* of S on a set X is a map $S \times X \to X$ satisfying $(st)x = s(tx)$ for all $s, t \in S$ and $x \in X$. Dually, a *right action* is a map $X \times S \to X$ satisfying $x(st) = (xs)t$ for all $s, t \in S$ and $x \in X$.

Chapter 2

Automaton Semigroup Theory

In this chapter we will introduce the necessary theory to define and construct automaton semigroups. Having done so, we will then see some examples of automaton semigroups and consider some natural classes of semigroup that arise in this way. Finally, some of the basic properties of these semigroups will be discussed.

2.1 Construction of Automaton Semigroups

We will follow the definitions given in [7] and [32] in defining an automaton. The automata that we define are automata with outputs – this thesis will not be concerned with, for example, (non)-deterministic finite state automata or pushdown automata. Further background on automata may be found in, for example, [13].

Definition 2.1. An *automaton* $\mathcal{A}$ is a triple (Q, B, δ) consisting of a finite set of states Q, a finite *alphabet* B and a function $\delta : Q \times B \to Q \times B$ called the *transition function.* The automaton will be thought of as a directed labelled graph with vertex set Q and an edge from q to r labelled by $x|y$ precisely when $\delta(q, x) = (r, y)$. Pictorially, we have

$$q \xrightarrow{x|y} r$$

In the interests of clarity, the following definitions will be adhered to throughout:

Definition 2.2. A *word* in Q is an element of

$$Q^+ = \{q_1 q_2 \dots q_n : n \geq 1, q_i \in Q\}.$$

A *sequence* in B is an element of $B^* = B^+ \cup \{\epsilon\}$, consisting of *symbols* from B. Here, ϵ denotes the empty sequence of length zero.

Sequences in B are acted on by the states in Q. We define states to act on sequences from the *left* which is in contrast to some authors (most notably [7] and [25]). The action is defined as follows: the result of state q acting on the sequence α is denoted by $q \cdot \alpha$ and is by definition the sequence outputted by the automaton after starting in state q and reading α. More precisely, if $\mathcal{A}$ reads the sequence $\alpha = \alpha_1 \alpha_2 \dots \alpha_n$ (where $\alpha_i \in B$) then $q \cdot \alpha = \beta_1 \beta_2 \dots \beta_n$ where $\delta(q_{i-1}, \alpha_i) = (q_i, \beta_i)$ for $i = 1, \dots, n$ and $q_0 = q$.

When comparing the left- and right-action approaches, it may appear that choosing to act on a particular side is simply a notational preference. However, this choice has profound implications on the resulting automaton semigroup as it induces an anti-isomorphism (see Section 5.4 for details in the setting of Cayley automaton semigroups) which will allow us in Chapter 5 to obtain a wider class of so-called self-automaton semigroups than was possible in [7]. In this chapter, and in Chapter 3, we will reprove several results from the left-action viewpoint and obtain dual results to those already known.

For each symbol read by the automaton exactly one symbol is outputted and hence $|q \cdot \alpha| = |\alpha|$ (where $|\alpha|$ denotes the length of the sequence). Automata with this property are termed *synchronous* automata. As such, the action of $\mathcal{A}$ on finite sequences determines the action on infinite sequences and vice-versa. On occasion it will be more convenient to reason about the action of an automaton $\mathcal{A}$ on a single infinite sequence rather than on sets of finite sequences of some given length. We will denote an infinite sequence that consists of countably many repetitions of a finite sequence α by α^ω and the set of all infinite sequences by B^ω. The sequences in B^ω are infinite on the right, and as such are indexed by the natural numbers rather than the integers. The set of all sequences of a given finite length n will be denoted B^n.

We can identify the regular $|B|$-ary rooted tree with the set of sequences B^*. We label the root vertex with the empty sequence and a vertex labelled α has $|B|$ children with labels $\alpha\beta$ for each $\beta \in B$. We will not make any distinction between the labels and the vertices of the tree. Each state q acting on B^* can therefore be considered as a transformation of the corresponding tree. A vertex w is mapped to the vertex $q \cdot w$.

By the definition of the action, if $q \cdot \alpha\alpha' = \beta\beta'$ (for $\alpha, \beta \in B^*$ and $\alpha', \beta' \in B$) then we have $q \cdot \alpha = \beta$. This tells us that if a vertex α is the parent of a vertex $\alpha\alpha'$ then their images under the transformation are also parent (β) and child ($\beta\beta'$). Hence the action on the tree is adjacency- and level-preserving and is thus an endomorphism of the tree.

We can naturally extend the action of a state to an action of words. A word $q_n q_{n-1} \ldots q_2 q_1$ acts on a sequence α as follows:

$$q_n \cdot (q_{n-1} \cdot \ldots \cdot (q_2 \cdot (q_1 \cdot \alpha)) \ldots).$$

There is therefore a natural homomorphism $\Phi : Q^+ \to \mathrm{End}(B^*)$ where $\mathrm{End}(B^*)$ denotes the endomorphism monoid of B^*. The image of Φ is denoted by $\Sigma(\mathcal{A})$.

We are now in a position to define an automaton semigroup.

Definition 2.3. A semigroup S is said to be an *automaton semigroup* if there exists an automaton $\mathcal{A}$ such that $S \cong \Sigma(\mathcal{A})$.

We now explain the conditions under which two words u and v in Q^+ represent the same element in $\Sigma(\mathcal{A})$. This follows immediately from the definitions but is stated here explicitly due to the fundamental nature of the results:

Lemma 2.4 ([7, Lemma 2.2]). *Let $u, v \in Q^+$. The following are equivalent:*

1. *u and v represent the same element of $\Sigma(\mathcal{A})$,*
2. *$\Phi(u) = \Phi(v)$,*
3. *$u \cdot \alpha = v \cdot \alpha$ for all $\alpha \in B^*$,*
4. *u and v have the same actions on B^n for all $n \in \mathbb{N} \cup \{0\}$,*
5. *u and v have the same actions on B^ω.*

Proof. ($1 \Rightarrow 2$) If $\Phi(u) \neq \Phi(v)$ then u and v cannot represent the same element of $\Sigma(\mathcal{A})$.

($2 \Rightarrow 3$) If $u \cdot \alpha \neq v \cdot \alpha$ for some $\alpha \in B^*$ then the words act differently on the $|B|$-ary rooted tree and so represent different endomorphisms. Thus $\Phi(u) \neq \Phi(v)$.

($3 \Rightarrow 4$) If u, v have different actions on B^n for some n then there exists $\alpha \in B^*$ such that $u \cdot \alpha \neq v \cdot \alpha$.

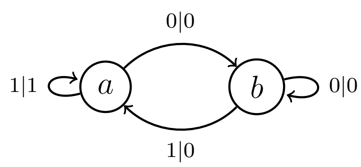
($4 \Rightarrow 5$) If u and v do not have the same action on B^ω then there exists $\alpha = \alpha_1\alpha_2 \ldots \in B^\omega$ and i such that $u \cdot \alpha = \beta_1\beta_2 \ldots \beta_{i-1}\beta_i\beta_{i+1} \ldots$ and $v \cdot \alpha = \beta_1\beta_2 \ldots \beta_{i-1}\gamma_i\gamma_{i+1} \ldots$ where $\beta_j, \gamma_j \in B$ and $\beta_i \neq \gamma_i$. Hence u and v act differently on B^i.

($5 \Rightarrow 1$) If u and v do not represent the same element of $\Sigma(\mathcal{A})$ then there exists $\alpha = \alpha_1\alpha_2 \ldots \in B^\omega$ and i such that $u \cdot \alpha = \beta_1\beta_2 \ldots \beta_{i-1}\beta_i\beta_{i+1} \ldots$ and

$v \cdot \alpha = \beta_1\beta_2 \ldots \beta_{i-1}\gamma_i\gamma_{i+1} \ldots$ where $\beta_j, \gamma_j \in B$ and $\beta_i \neq \gamma_i$. Hence u and v act differently on B^ω. $\square$

At this point is would be instructive to consider an example of an automaton semigroup being constructed from a given automaton. We will follow an example from [7].

Example 2.5. Let $\mathcal{A} = (\{a, b\}, \{0, 1\}, \delta)$ be the automaton below:



If, for example, $\mathcal{A}$ is in state a and reads the sequence 0011 then the calculation will proceed as follows: $a{\cdot}0011 = 0(b{\cdot}011) = 00(b{\cdot}11) = 000(a{\cdot}1) = 0001$.

We must consider the actions of a and b on sequences to determine the automaton semigroup. Let α be an infinite sequence. Observe that $b \cdot \alpha$ must start with 0 for all sequences α and so we may write $b \cdot \alpha = 0\beta$ for some sequence β. Observe now that

$$a \cdot b \cdot \alpha = a \cdot 0\beta = 0(b \cdot \beta)$$

and

$$b \cdot b \cdot \alpha = b \cdot 0\beta = 0(b \cdot \beta).$$

Hence in $\Sigma(\mathcal{A})$ we have the relation $ab = b^2$. This means that any element in $\Sigma(\mathcal{A})$ can be written in the form $b^i a^j$ for some $i, j \in \mathbb{N} \cup \{0\}$.

We show now that every product in $\Sigma(\mathcal{A})$ can be uniquely expressed as $b^i a^j$ for some $i, j \in \mathbb{N} \cup \{0\}$. By writing b^i as a state we mean $\underbrace{b \cdot \ldots \cdot b}_{i \text{ times}}$. Let $i, j \geq 0$. We have that

$$b^i \cdot a^j \cdot 01^\omega = b^i \cdot 0^{j+1} 1^\omega = 0^{i+j+1} 1^\omega \tag{2.1}$$

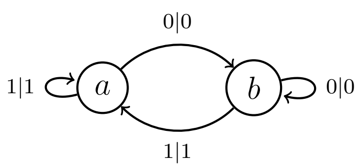
and, for $n > i$

$$b^i \cdot a^j \cdot 1^n 0^\omega = b^i \cdot 1^n 0^\omega = 0^i 1^{n-i} 0^\omega. \tag{2.2}$$

Now suppose that $b^i \cdot a^j = b^k \cdot a^l$ for some $k, l \geq 0$. Then by (2.2) $n - i = n - k$ and hence $i = k$. By (2.1) $i + j + 1 = k + l + 1$ which gives $j = l$. The semigroup $\Sigma(\mathcal{A})$ is therefore presented by $\langle a, b | ab = b^2 \rangle$.

Having seen an example of a finitely presented infinite semigroup arising as an automaton semigroup, we conclude this section by showing that small changes in the automaton can lead to a radically different automaton semigroup.

Example 2.6. Let $\mathcal{B} = (\{a, b\}, \{0, 1\}, \epsilon)$ be the automaton below:



Then for any sequence $\alpha \in \{0, 1\}^*$, $a \cdot \alpha = b \cdot \alpha = a \cdot a \cdot \alpha = \alpha$ and consequently $\Sigma(\mathcal{B})$ is trivial.

2.2 Basic Properties of Automaton Semigroups

Some authors make use of *wreath recursions* when studying automaton semigroups. This is not the approach that will be favoured in this thesis. However, we outline it here and make use of it to establish some fundamental properties of automaton semigroups. The results in this section can be found in [7] and further details about wreath products can be found in [10] and [30].

The endomorphism semigroup of B^* can be written as a recursive wreath product $\mathrm{End}(B^*) = \mathcal{T}_B \wr \mathrm{End}(B^*)$ where $\mathcal{T}_B$ denotes the transformation semigroup on the set B (see [4, 17, 18] for more details). Hence we have

$$\mathrm{End}(B^*) = \mathcal{T}_B \ltimes \underbrace{(\mathrm{End}(B^*) \times \ldots \times \mathrm{End}(B^*))}_{n \text{ times}}$$

where $\mathcal{T}_B$ acts from the left on the co-ordinates of the elements in the direct product.

If we have $p = \tau(x_1, \ldots, x_n)$ and $q = \rho(y_1, \ldots, y_n)$ (where $\tau, \rho \in \mathcal{T}_\mathcal{B}$ and $x_i, y_j \in \mathrm{End}(B^*)$) then

$$\begin{aligned} pq &= \tau(x_1, \ldots, x_n)\rho(y_1, \ldots, y_n) \\ &= \tau\rho^\rho(x_1, \ldots, x_n)(y_1, \ldots, y_n) \\ &= \tau\rho(x_{\rho(1)}y_1, \ldots, x_{\rho(n)}y_n) \end{aligned}$$

where ${}^{\rho}(x_1, \ldots, x_n)$ denotes the result of ρ acting on $(x_1, \ldots, x_n)$.

If $p \in \mathrm{End}(B^*)$ then τ describes the action of p on B and each x_i is an element of $\mathrm{End}(B^*)$ whose action on B^* mimics the action of p on the subtree $b_i B^*$. So to act on B^* by p we act on each subtree with the corresponding x_i and then act on the collection of subtrees that result by τ.

Let $\mathcal{A} = (Q, B, \delta)$ be an automaton where $B = \{b_1, \ldots, b_n\}$. Define the maps $\tau_p : B \to B$ by $\tau_p(b) = p \cdot b$ and $\pi_b : Q \to Q$ by $\pi_b(q) = r$ where $\delta(q, b) = (r, z)$ for some $z \in B$. If $p \in Q$ then $\tau = \tau_p$ and $x_i = \pi_{b_i}(p)$. That is,

$$p = \tau_p(\pi_{b_1}(p), \ldots, \pi_{b_n}(p)).$$

The main purpose of the wreath recursion is, by using the multiplication outlined above, to determine the action of a word $w \in Q^+$ on B^*.

If we have a wreath recursion $\tau(u_1, \ldots, u_n)$ which describes the action of $w \in Q^+$ then we may add a state w to $\mathcal{A}$ with an edge from w to u_i labelled by $b_i|\tau(b_i)$ for each i (this may require extra states u_i to be added). The new automaton $\mathcal{A}'$ results in the same semigroup as $\mathcal{A}$.

Let us return briefly to Example 2.5 and consider it in the context of wreath recursions. We obtain as the wreath recursions corresponding to the states $a = \mathrm{id}(b, a)$ and $b = \lambda(b, a)$ where $\mathrm{id}, \lambda : \{0, 1\} \to \{0, 1\}$ are the identity map and the map defined by $\lambda(0) = \lambda(1) = 0$ respectively. Using the multiplication defined above we see that

$$\begin{array}{rclclcl}
a^2 & = & \mathrm{id}(b,a)\mathrm{id}(b,a) & = & \mathrm{idid}(bb,aa) & = & \mathrm{id}(b^2,a^2), \\
ab & = & \mathrm{id}(b,a)\lambda(b,a) & = & \mathrm{id}\lambda(bb,ba) & = & \lambda(b^2,ba), \\
ba & = & \lambda(b,a)\mathrm{id}(b,a) & = & \lambda\mathrm{id}(bb,aa) & = & \lambda(b^2,a^2), \\
b^2 & = & \lambda(b,a)\lambda(b,a) & = & \lambda\lambda(bb,ba) & = & \lambda(b^2,ba).
\end{array}$$

Notice that this agrees with the earlier conclusion that $ab = b^2$.

Recall that a semigroup is said to be *residually finite* if for any $u, v \in S$ with $u \neq v$ there is a homomorphism θ from S onto a finite semigroup with the property that $\theta(u) \neq \theta(v)$.

Proposition 2.7 ([7, Proposition 3.2])**.** *Every automaton semigroup is residually finite.*

Proof. Let $\mathcal{A} = (Q, B, \delta)$ be an automaton and let u, v be distinct elements of $\Sigma(\mathcal{A})$. Then there exists n such that u and v act differently on B^n.

Define a new automaton $\mathcal{A}_1 = (Q_1, B_1, \delta_1)$ where $Q_1 = Q$ and $B_1 = B^n$. This new automaton $\mathcal{A}_1$ essentially simulates $\mathcal{A}$ but instead considers a block of n symbols from B as a single new symbol. Therefore $\Sigma(\mathcal{A}) \cong \Sigma(\mathcal{A}_1)$. Notice also that in $\mathcal{A}_1$ we have $\tau_u \neq \tau_v$ where τ_u, τ_v are defined as above. The semigroup $T = \{\tau_w : w \in (Q_1)^+\}$ is finite and is a homomorphic image of $\Sigma(\mathcal{A})$ under the map $w \mapsto \tau_w$. One sees that the map is well-defined and u and v have different images. Hence $\Sigma(\mathcal{A})$ is residually finite. $\square$

Proposition 2.8 ([7, Proposition 3.4])**.** *Automaton semigroups have a soluble word problem.*

Proof. It is shown originally in [17, Theorem 2.22] that this result is true for automaton groups and that it generalises to automaton semigroups.

Let $\mathcal{A} = (Q, B, \delta)$ be an automaton with $B = \{1, \ldots, n\}$. Let $u, v \in Q^+$. Suppose that the wreath recursions for u and v are $u = \tau_u(w_1, \ldots, w_n)$ and $v = \tau_v(y_1, \ldots, y_n)$.

We have that $u = v$ in $\Sigma(\mathcal{A})$ if and only if $\tau_u = \tau_v$ and $w_i = y_i$ in $\Sigma(\mathcal{A})$ for each $i \in B$. First check whether $\tau_u = \tau_v$. If $\tau_u \neq \tau_v$ then stop as we have shown $u \neq v$. If $\tau_u = \tau_v$ then proceed as follows:

For each $i \in B$ repeat the above process to check if $w_i = y_i$. That is, compute the wreath recursions for w_i and y_i and check to see if $\tau_{w_i} = \tau_{y_i}$.

If, at some iteration, all of the pairs of words to be compared have already been encountered in a previous iteration then stop with the conclusion that $u = v$.

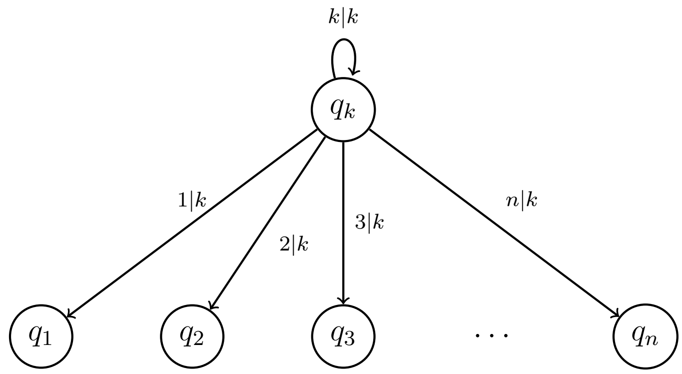
This process terminates as the words w_i and y_i whose equality is to be checked have length at most $|u|$ and $|v|$ respectively. This gives us at most $|Q|^{|u|}$ possibilities for w_i and $|Q|^{|v|}$ possibilities for y_i. Therefore there are at most $|Q|^{|u|+|v|}$ possible pairs of words to be compared. In the worst case, we obtain only one such new pair at each iteration and so any differences in the actions of u and v must occur within $|Q|^{|u|+|v|}$ iterations. $\square$

2.3 Natural Classes of Automaton Semigroups

In this section we will see that some classes of semigroup occur naturally as automaton semigroups before looking at some semigroup constructions that interact nicely with the automaton semigroup construction. Again, we will mostly be following [7].

Example 2.9 ([7, Proposition 4.1])**.** For any integer $n \geq 2$ the free semigroup of rank n is an automaton semigroup.

Proof. Let $n \geq 2$. We define an automaton $\mathcal{A} = (Q, B, \delta)$ as follows: the alphabet B will be $\{1, \ldots, n\}$, the state set is $Q = \{q_i : i \in B\}$ and the transition function is given by $\delta(q_i, j) = (q_j, i)$. This is illustrated in the diagram below:



If $\mathcal{A}$ reads the symbol i it moves to state q_i and the next output will be i. An infinite sequence α is sent to the sequence $i\alpha$ under the action of state q_i.

So for a word $w = q_{i_1} q_{i_2} \dots q_{i_n}$ where $i_j \in B$ we have

$$w \cdot 1^\omega = i_1 i_2 \dots i_n 1^\omega$$

and

$$w \cdot 2^\omega = i_1 i_2 \dots i_n 2^\omega.$$

The common prefix of $w \cdot 1^\omega$ and $w \cdot 2^\omega$ determines w and so $\Sigma(\mathcal{A})$ is free on Q. Finally note that $|Q| = |B| = n$. □

An alternative way to construct free semigroups as automaton semigroups will be presented later in Sections 3.2 and 3.3. This will make use of Cayley automaton semigroups, which will be introduced in Chapter 3.

Example 2.10 ([7, Proposition 4.3])**.** The free semigroup of rank one is not an automaton semigroup.

Proof. We identify the free semigroup of rank one with the natural numbers. Suppose that $\mathbb{N} = \Sigma(\mathcal{A})$ for some automaton $\mathcal{A} = (Q, B, \delta)$. First note that if $|Q| = 1$ then $\Sigma(\mathcal{A})$ is isomorphic to the subsemigroup of $\mathrm{End}(B^*)$ generated by $\{\tau_q : q \in Q\}$ and so is finite, which is a contradiction. Hence we may assume that $|Q| \geq 2$. The element 1 is indecomposable in $\mathbb{N}$ so must be present in any generating set for $\mathbb{N}$. Hence we may assume that $1 \in Q$ as Q generates $\Sigma(\mathcal{A})$.

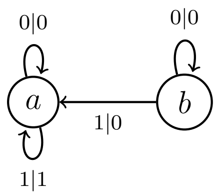
With respect to the usual ordering of $\mathbb{N}$, let k be the largest element in Q.

Suppose that we have used the wreath recursion for 1 to calculate the wreath recursion for k and have found that it is $\tau(q_{1,1}\cdots q_{1,k},\ldots,q_{|B|,1}\cdots q_{|B|,k})$ where $q_{i,j}\in Q$. In $\mathbb{N}$, each string $q_{i,1}\cdots q_{i,k}$ is equal to an element of Q which appears in the wreath recursion for k. As we chose k to be maximal we must have $q_{i,j}=1$ for all i,j. Hence $1=\sigma(1,\ldots,1)$ for some σ and so is a periodic element of $\mathbb{N}$ which is a contradiction. Hence the free semigroup of rank one is not an automaton semigroup. □

By way of contrast, the free monoid of rank one is an automaton semigroup.

Example 2.11 ([7, Proposition 4.4])**.** The free monoid of rank one is an automaton semigroup.

Proof. Consider the following automaton $\mathcal{A}$:



For any $x\in Q$ and any sequence α notice that $a\cdot x\cdot\alpha = x\cdot a\cdot\alpha = x\cdot\alpha$ and so a is the identity in $\Sigma(\mathcal{A})$. We also have that $\underbrace{b\cdot\ldots\cdot b}_{k\text{ times}}\cdot 1^\omega = 0^k1^\omega$ and hence all powers of b are distinct. Thus $\Sigma(\mathcal{A})$ is the free monoid of rank one. □

Example 2.12 ([7, Proposition 4.6])**.** All finite semigroups are automaton semigroups.

Proof. Let S be a finite semigroup. For each $x \in S$ define the map λ_x in $\mathcal{T}_{S^1}$ by $\lambda_x(s) = xs$ where $s \in S^1$. This gives the extended left-regular representation of S in $\mathcal{T}_{S^1}$ (see [21, Theorem 1.1.2] for details). Therefore the subsemigroup $T = \{\lambda_x : x \in S\} \leq \mathcal{T}_{S^1}$ is isomorphic to S. Let $\mathcal{A} = (S, S^1, \delta)$ be an automaton where δ is given by $\delta(x, s) = (x, \lambda_x(s))$. Then
$\Sigma(\mathcal{A}) \cong T$. $\square$

Proposition 2.13 ([7, Proposition 5.5]). *Let S and T be automaton semigroups. Then $S \times T$ is an automaton semigroup if and only if it is finitely generated.*

Proof. By Proposition 2.12 there is nothing to prove if S and T are both finite so we may assume that at least one of S and T is infinite.

If $S \times T$ is an automaton semigroup then it is clearly finitely generated.

For the converse, suppose that $S \times T$ is finitely generated. We have that $S \times T$ is generated by $X \times Y$ for some finite subsets $X \subseteq S$ and $Y \subseteq T$. Let $\mathcal{A} = (P, C, \delta)$ and $\mathcal{B} = (Q, D, \epsilon)$ be automata such that $S = \Sigma(\mathcal{A})$ and $T = \Sigma(\mathcal{B})$. We calculate wreath recursions for elements of P^m and Q^n (for $m, n \in \mathbb{N}$) such that $X \subseteq P^m$ and $Y \subseteq Q^n$. We obtain new automata $\mathcal{A}_1 = (P^m, C, \delta)$ and $\mathcal{B}_1 = (Q^n, D, \epsilon)$ by adding new states corresponding to these wreath recursions to $\mathcal{A}$ and $\mathcal{B}$.

Let $\mathcal{C}$ be the automaton with state set $P^m \times Q^n$ that acts on $C \times D$ in the natural way. Then $\Sigma(\mathcal{C}) \cong \Sigma(\mathcal{A}_1) \times \Sigma(\mathcal{B}_1) \cong S \times T$. $\square$

Proposition 2.14 ([7, Proposition 5.6])**.** *Let S and T be automaton semigroups. The normal ideal extension of S by T is an automaton semigroup.*

Proof. A semigroup U is the normal ideal extension of S by T if $U = S \cup T$ and $st = ts = t$ for all $s \in S$ and $t \in T$ (see [9, Section 4.4] for details).

Let $\mathcal{A} = (Q, C, \delta)$ and $\mathcal{B} = (R, D, \epsilon)$ be automata such that $S = \Sigma(\mathcal{A})$ and $T = \Sigma(\mathcal{B})$.

Define a new automaton $\mathcal{K} = (Q \cup R, C \cup D \cup \{0\}, \theta)$ where $0 \notin C \cup D$. The transition function θ is defined by:

$$\begin{aligned}
(q, c) &\mapsto \delta(q, c) \\
(q, d) &\mapsto (q, d) \\
(q, 0) &\mapsto (q, 0) \\
(r, c) &\mapsto (r, 0) \\
(r, d) &\mapsto \epsilon(r, d) \\
(r, 0) &\mapsto (r, 0)
\end{aligned}$$

where $q \in Q, r \in R, c \in C$ and $d \in D$.

We go on to show that $\Sigma(\mathcal{K})$ is the normal ideal extension of S by T.

In a state $q \in Q$, $\mathcal{K}$ acts on symbols from C like $\mathcal{A}$ does. It skips over symbols in $D \cup \{0\}$ leaving them unchanged and remains in state q. Similarly, if $\mathcal{K}$ is in a state $r \in R$ then it acts on D in the same way as $\mathcal{B}$ and sends symbols in $C \cup \{0\}$ to 0 whilst staying in state r.

Let $\alpha \in (C \cup D \cup \{0\})^\omega$. We can write α as $\alpha = \beta_1\gamma_1\beta_2\gamma_2\ldots$ where $\beta_i \in C^*$ and $\gamma_i \in (D \cup \{0\})^*$. Now let $u \in Q^+$. Then

$$u \cdot \alpha = \beta_1'\gamma_1\beta_2'\gamma_2\ldots$$

where the β_i' are given by $u \cdot \beta_1\beta_2\ldots = \beta_1'\beta_2'\ldots$ and $|\beta_i| = |\beta_i'|$.

Thus the action of a word over Q is completely determined by its action on C^*. As it has no effect on symbols from $D \cup \{0\}$, the subsemigroup of $\Sigma(\mathcal{K})$ generated by Q is isomorphic to S.

Now decompose α as $\alpha = \beta_1\gamma_1\beta_2\gamma_2\ldots$ where $\beta_i \in (C \cup \{0\})^*$ and $\gamma_i \in D^*$. For a word $v \in R^+$ we have

$$v \cdot \alpha = 0^{k_1}\gamma_1'0^{k_2}\gamma_2'\ldots$$

where γ_i' is determined by $v \cdot \gamma_1\gamma_2\ldots = \gamma_1'\gamma_2'\ldots$ and $|\gamma_i'| = |\gamma_i|$. We also have $k_i = |\beta_i|$. So the action of a word over R is determined only by its action on D^* and so the subsemigroup of $\Sigma(\mathcal{K})$ generated by R is isomorphic to T.

For any sequence $\alpha \in (C \cup D \cup \{0\})^\omega$ and words $u \in Q^+$ and $v \in R^+$ we have

$$uv \cdot \alpha = vu \cdot \alpha = v \cdot \alpha$$

as u does not alter symbols in $D \cup \{0\}$ and v sends all symbols from $C \cup \{0\}$ to 0. Hence $\Sigma(\mathcal{K})$ is the normal ideal extension of S by T. $\square$

Immediate corollaries of Proposition 2.14 are the following:

Corollary 2.15 ([7, Proposition 5.1])**.** *Let S be an automaton semigroup. Then S^0 is also an automaton semigroup.*

Corollary 2.16 ([7, Proposition 5.2])**.** *Let S be an automaton semigroup. Then S^1 is also an automaton semigroup.*

Proposition 2.17 ([7, Proposition 5.7])**.** *Let S and T be automaton semigroups. The $S \cup_0 T$ is also an automaton semigroup.*

Proof. Recall that the zero-union of two semigroups S and T is the semigroup $U = S \cup T \cup \{0\}$ where $st = ts = 0$ for all $s \in S$ and $t \in T$.

Let $\mathcal{A} = (Q, C, \delta)$ and $\mathcal{B} = (R, D, \epsilon)$ be automata such that $S = \Sigma(\mathcal{A})$ and $T = \Sigma(\mathcal{B})$. Define a new automaton $\mathcal{H} = (Q \cup R \cup \{0\}, C \cup D \cup \{z\}, \nu)$ where $0 \notin Q \cup R$, $z \notin C \cup D$ and ν is defined by:

$$
\begin{aligned}
(q, c) &\mapsto \delta(q, c) \\
(q, d) &\mapsto (0, z) \\
(r, c) &\mapsto (0, z) \\
(r, d) &\mapsto \epsilon(r, d) \\
(x, z) &\mapsto (0, z) \\
(0, e) &\mapsto (0, z)
\end{aligned}
$$

where $q \in Q, r \in R, c \in C, d \in D, x \in Q \cup R \cup \{0\}$ and $e \in C \cup D \cup \{z\}$.

The action of a state $q \in Q$ in $\mathcal{H}$ on C^ω is the same as the action in $\mathcal{A}$. If $\alpha \in C^*$ and $\beta \in (D \cup \{z\})(C \cup D \cup \{z\})^\omega$ then $q \cdot \alpha\beta = (q \cdot \alpha)z^\omega$. Hence the action of states in Q in the automaton $\mathcal{H}$ is defined by their action in $\mathcal{A}$. Therefore the subsemigroup of $\Sigma(\mathcal{H})$ generated by Q is isomorphic to S. By a similar argument, we obtain that T is isomorphic to the subsemigroup of $\Sigma(\mathcal{H})$ generated by R. Evidently 0 is the zero element in $\Sigma(\mathcal{H})$.

For any words $u \in Q^+$ and $v \in R^+$ and any sequence $\alpha \in (C \cup D \cup \{z\})^\omega$ we have $uv \cdot \alpha = vu \cdot \alpha = 0 \cdot \alpha = z^\omega$ and so $\Sigma(\mathcal{H}) \cong S \cup_0 T$. $\square$

Chapter 3

Cayley Automaton Semigroup Theory

Having considered general automaton semigroups in Chapter 2 we go on now to define *Cayley automata*. These are automata that are constructed from the Cayley Tables of finite semigroups. We shall term the automaton semigroups arising from these automata *Cayley automaton semigroups*. These semigroups will be the focus of study for the remainder of this thesis.

We will begin by defining Cayley automata before looking at some of their basic properties. Several examples will be constructed and some fundamental results established.

3.1 Definition

Following [7, 25, 27, 28, 32] we make the following definition:

Definition 3.1. Let S be a finite semigroup. The *Cayley automaton* is the automaton $\mathcal{C}(S) = (S, S, \delta)$ where the transition function is defined by $\delta(s, t) = (st, st)$ for $s, t \in S$.

Since st is a product in the semigroup note that this is still a synchronous automaton. A typical edge in such an automaton has the following form:

$$\begin{tikzcd} s \arrow[r, "t|st"] & st \end{tikzcd}$$

Intuitively, if outputs are ignored, the automaton obtained is simply the right Cayley graph of S with respect to S as the generating set.

Having defined Cayley automata, we can now make the following definition:

Definition 3.2. A semigroup T is said to be a *Cayley automaton semigroup* if there exists a finite semigroup S such that $T \cong \Sigma(\mathcal{C}(S))$.

In Definition 3.1 above, notice that the state set and the alphabet used are the same. In order to avoid confusion, we adopt the following convention:

Notation 3.3. For $s \in S$ the state in the Cayley automaton corresponding to s will be denoted $\overline{s}$ and the symbol as s.

Let $s \in S$ and $\alpha = \alpha_1\alpha_2 \ldots \alpha_n \in S^*$. A direct calculation shows that

$$\overline{s} \cdot \alpha = (s\alpha_1)(s\alpha_1\alpha_2) \ldots (s\alpha_1\alpha_2 \ldots \alpha_n).$$

Each state $\overline{s}$ in the Cayley automaton therefore gives rise to a transformation $S^* \to S^*$ given by

$$\overline{s} : \alpha_1\alpha_2 \ldots \alpha_n \mapsto (s\alpha_1)(s\alpha_1\alpha_2) \ldots (s\alpha_1\alpha_2 \ldots \alpha_n).$$

We may therefore view $\Sigma(\mathcal{C}(S))$ as the subsemigroup of $\mathrm{End}(S^*)$ generated by $\{\overline{s} : s \in S\}$ under composition of transformations.

3.2 Known Results

We give now two major results in this area which will be used throughout this thesis.

The following is proved in [32, Theorem 4.1]:

Theorem 3.4. *Let G be a non-trivial finite group. Then $\Sigma(\mathcal{C}(G))$ is a free semigroup of rank equal to the order of G.*

The original proof of this result makes use of the properties of reset automata, something which we will not discuss here. An alternative proof using actions on sequences will be given in Section 7.1

Having considered groups, we now consider aperiodic semigroups (recall that in the finite case, these are the semigroups with no non-trivial subgroups). Mintz establishes the following in [28]:

Theorem 3.5. *Let S be a finite semigroup. Then $\Sigma(\mathcal{C}(S))$ is finite and aperiodic if and only if S is aperiodic.*

The proof of this result is long and involved and as such is not presented here. The main idea of the proof is to consider the ideal structure of an aperiodic semigroup and act on sequences of elements from these ideals. Alternative proofs of this result are given in [7] and [25] using actions on sequences and wreath recursions respectively. Although shorter than Mintz's proof, both proofs are still lengthy and technical.

3.3 Basic Properties and Examples of Cayley Automaton Semigroups

We begin by proving a simple, yet fundamental, theorem regarding when two elements of a semigroup give rise to the same transformation in the Cayley automaton semigroup.

Theorem 3.6. *Let S be a semigroup and let $x, y \in S$. Then $\overline{x} = \overline{y} \in \Sigma(\mathcal{C}(S))$ if and only if $xa = ya$ for all $a \in S$.*

A proof of this appears in [25] using wreath recursions. An alternative proof using actions on sequences is given here:

Proof. $(\Rightarrow)$ Let $a \in S$ and $\alpha \in S^*$. Since $\overline{x} = \overline{y}$ we have that

$$(xa)(\overline{xa} \cdot \alpha) = \overline{x} \cdot a\alpha = \overline{y} \cdot a\alpha = (ya)(\overline{ya} \cdot \alpha)$$

and hence $xa = ya$ as the outputs must agree on all terms (in particular, the first term).

$(\Leftarrow)$ Since $xa = ya$ we have that

$$\overline{x} \cdot a\alpha = (xa)(\overline{xa} \cdot \alpha) = (ya)(\overline{ya} \cdot \alpha) = \overline{y} \cdot a\alpha$$

and hence $\overline{x} = \overline{y}$. $\square$

Proposition 3.7 ([7, Proposition 6.3])**.** *Let S be a finite semigroup. Then $\Sigma(\mathcal{C}(S^0)) \cong (\Sigma(\mathcal{C}(S)))^0$.*

Proof. Let $\alpha \in S^\omega$ and $s \in S$. Then

$$\overline{s} \cdot_{\mathcal{C}(S^0)} \alpha = \overline{s} \cdot_{\mathcal{C}(S)} \alpha$$

where the subscripts denote which automaton is acting on α.

If $\beta \in S^n$ and $\gamma \in (S \cup \{0\})^\omega$ then

$$\overline{s} \cdot_{\mathcal{C}(S^0)} \beta 0 \gamma = (\overline{s} \cdot_{\mathcal{C}(S^0)} \beta) 0^\omega = (\overline{s} \cdot_{\mathcal{C}(S)} \beta) 0^\omega$$

and $0 \cdot \gamma = 0^\omega$. Hence $\Sigma(\mathcal{C}(S^0)) \cong (\Sigma(\mathcal{C}(S)))^0$. □

Proposition 3.8 ([7, Proposition 6.5])**.** *Let U, V be finite semigroups. Then $\Sigma(\mathcal{C}(U \cup_0 V)) \cong \Sigma(\mathcal{C}(U)) \cup_0 \Sigma(\mathcal{C}(V))$.*

Proof. This is a consequence of Proposition 2.17. In that proof, let $\mathcal{A} = \mathcal{C}(U)$ and $\mathcal{B} = \mathcal{C}(V)$. It remains to replace the symbol z by 0. Then we have $\mathcal{K} = \mathcal{C}(U \cup_0 V)$. □

Proposition 3.9. *Let $x \in S$ be a left-zero. Then $\overline{x} \in \Sigma(\mathcal{C}(S))$ is a left-zero.*

Proof. Let $x \in S$ be a left-zero, $a \in S$ be arbitrary and $\alpha = \alpha_1\alpha_2 \dots \alpha_n \in S^*$. Then

$$\begin{aligned}
\overline{x} \cdot \overline{a} \cdot \alpha &= (xa\alpha_1)(xa\alpha_1 a\alpha_1\alpha_2) \dots (xa\alpha_1 a\alpha_1\alpha_2 \dots a\alpha_1 \dots \alpha_n) \\
&= (x)^n \\
&= \overline{x} \cdot \alpha
\end{aligned}$$

and hence $\overline{x}$ is a left-zero. □

Proposition 3.10. *Let $x \in S$ be a right-zero. Then $\overline{x} \in \Sigma(\mathcal{C}(S))$ is a right-zero.*

Proof. Let $x \in S$ be a right-zero, $a \in S$ be arbitrary and $\alpha = \alpha_1\alpha_2 \dots \alpha_n \in$

S^*. Then

$$\begin{aligned}\overline{a} \cdot \overline{x} \cdot \alpha &= (ax\alpha_1)(ax\alpha_1 x\alpha_1\alpha_2)\dots(ax\alpha_1 x\alpha_1\alpha_2 \dots x\alpha_1\dots\alpha_n) \\ &= (x\alpha_1)(x\alpha_1\alpha_2)\dots(x\alpha_1\dots\alpha_n) \\ &= \overline{x} \cdot \alpha\end{aligned}$$

and hence $\overline{x}$ is a right-zero. □

Combining Propositions 3.9 and 3.10 we immediately obtain the following:

Corollary 3.11. *Let $0 \in S$ be a two-sided zero. Then $\overline{0} \in \Sigma(\mathcal{C}(S))$ is a two-sided zero.*

Having considered left/right/two-sided zero elements, let us now construct the Cayley automaton semigroups arising from left-zero, right-zero and null semigroups.

Example 3.12. Let $L_n = \{x_1, x_2, \dots, x_n\}$ be a left-zero semigroup. Then by Proposition 3.9, $\overline{x_i}$ is a left-zero in $\Sigma(\mathcal{C}(L_n))$ for all $i \in \{1, \dots, n\}$. Also, for $i \neq j$ we have $\overline{x_i} \neq \overline{x_j}$ by Theorem 3.6. Hence $\Sigma(\mathcal{C}(L_n)) \cong L_n$.

This is the first non-trivial example of a *self-automaton semigroup* (that is, one that is isomorphic to its Cayley automaton semigroup). These semigroups will be the main object of study in Chapter 5.

Example 3.13. Let $R_n = \{x_1, x_2 \dots, x_n\}$ be a right-zero semigroup. Then by Proposition 3.10, $\overline{x_i}$ is a right-zero in $\Sigma(\mathcal{C}(S))$ for all $i \in \{1, \dots, n\}$. By

Theorem 3.6 we have that $\overline{x_i} = \overline{x_j}$ for all $i, j \in \{1, \ldots, n\}$. Hence $\Sigma(\mathcal{C}(R_n))$ is generated by $\{\overline{x_1}\}$ and so is trivial.

Example 3.14. Let $Z_n = \{0, x_1, x_2 \ldots, x_{n-1}\}$ be a null semigroup (that is, a semigroup satisfying $ab = 0$ for all a, b). By Theorem 3.6 we have that $\overline{x_i} = \overline{x_j} = \overline{0}$ for all $i, j \in \{1, \ldots, n-1\}$. Consequently $\Sigma(\mathcal{C}(Z_n))$ is generated by $\overline{0}$ and is trivial.

Example 3.15. Let $S = I \times J$ be a rectangular band where $I = \{1, \ldots, i\}$ and $J = \{1, \ldots, j\}$. Then by Theorem 3.6 we have $\overline{(i, j_1)} = \overline{(i, j_2)}$ for all $i \in I, j_1, j_2 \in J$. Hence $\Sigma(\mathcal{C}(S))$ is generated by $\{\overline{(1,1)}, \overline{(2,1)}, \ldots, \overline{(i,1)}\}$ (note also that $\overline{(i_1, 1)} \neq \overline{(i_2, 1)}$ for all $i_1, i_2 \in I$). We have, for $\overline{(i_1, 1)}, \overline{(i_2, 1)} \in \Sigma(\mathcal{C}(S))$ and $\alpha = (\lambda_1, \mu_1)(\lambda_2, \mu_2) \ldots (\lambda_n, \mu_n) \in S^*$ (where $\lambda_i \in I$ and $\mu_j \in J$)

$$\overline{(i_2, 1)} \cdot \alpha = (i_2, \mu_1)(i_2, \mu_2) \ldots (i_2, \mu_n).$$

Hence

$$\begin{aligned}
\overline{(i_1, 1)} \cdot \overline{(i_2, 1)} \cdot \alpha &= \overline{(i_1, 1)} \cdot (i_2, \mu_1)(i_2 \mu_2) \ldots (i_2 \mu_n) \\
&= (i_1, \mu_1)(i_1, \mu_2) \ldots (i_1, \mu_n) \\
&= \overline{(i_1, 1)} \cdot \alpha
\end{aligned}$$

and so $\overline{(i_1, 1)}$ is a left-zero. Consequently, $\Sigma(\mathcal{C}(S)) \cong L_i$.

So far we have established that left-zero semigroups and rectangular bands give rise to left-zero semigroups when we construct the Cayley automaton semigroups. We now classify exactly which semigroups give rise to left-zero semigroups.

Proposition 3.16. *Let S be a finite semigroup. Then $\Sigma(\mathcal{C}(S))$ is a left-zero semigroup if and only if $abc = ac$ for all $a, b, c \in S$.*

Maltcev establishes a dual result to this in [25] via his use of right actions. We give an amended version of his proof here in the setting of left-actions.

Proof. ($\Rightarrow$) Assume that $\Sigma(\mathcal{C}(S))$ is a left-zero semigroup and let $a, b \in S$. Then $\overline{a} \cdot \overline{b} \cdot \alpha = \overline{a} \cdot \alpha$ for all $\alpha \in S^*$. Consider the sequence $\alpha = c$ of length one. Then

$$abc = \overline{a} \cdot \overline{b} \cdot c = \overline{a} \cdot c = ac$$

and hence $abc = ac$ for all $a, b, c \in S$.

($\Leftarrow$) Suppose that $abc = ac$ for all $a, b, c \in S$ and let $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$. Then

$$\begin{aligned} \overline{a} \cdot \overline{b} \cdot \alpha &= (ab\alpha_1)(ab\alpha_1 b\alpha_1\alpha_2) \ldots (ab\alpha_1 b\alpha_1\alpha_2 \ldots b\alpha_1 \ldots \alpha_n) \\ &= (a\alpha_1)(a\alpha_1\alpha_2) \ldots (a\alpha_1\alpha_2 \ldots \alpha_n) \\ &= \overline{a} \cdot \alpha \end{aligned}$$

and hence $\overline{a}$ is a left-zero for all $a \in S$. Thus $\Sigma(\mathcal{C}(S))$ is a left-zero semigroup.

□

We can also classify which semigroups give rise to right-zero semigroups.

Proposition 3.17. *Let S be a finite semigroup. Then $\Sigma(\mathcal{C}(S))$ is a right-zero semigroup if and only if S^2 is the minimal ideal of S and this ideal forms a right-zero semigroup.*

Again, a dual result is established in [25] and a proof for the left-action case is presented here:

Proof. ($\Rightarrow$) Suppose that $\Sigma(\mathcal{C}(S))$ is a right-zero semigroup. Since it is finitely generated it must be finite. Let $I = \{i_1, \ldots, i_k\}$ be the minimal ideal of S.

Since $I^* \subseteq S^*$ and I is an ideal of S we have that I^* is invariant under the actions of $\{\overline{i_1}, \ldots, \overline{i_k}\}$. Hence, the subsemigroup of $\Sigma(\mathcal{C}(S))$ generated by $\{\overline{i_1}, \ldots, \overline{i_k}\}$ can be homomorphically mapped onto $\Sigma(\mathcal{C}(I))$ via the map $\overline{i_j} \mapsto \overline{i_j \restriction_{I^*}}$. The ideal I must be a Rees-Matrix semigroup and since $\Sigma(\mathcal{C}(S))$ is finite we conclude by Theorem 3.5 that S is aperiodic. Hence I must in fact be a rectangular band $X \times Y$ where X is a left-zero semigroup and Y is a right-zero semigroup. As per Example 3.15, $\Sigma(\mathcal{C}(I)) \cong L_{|X|}$.

Since $\Sigma(\mathcal{C}(S))$ is a right-zero semigroup, every subsemigroup and homomorphic image of $\Sigma(\mathcal{C}(S))$ must also be a right-zero semigroup. In particular, $\Sigma(\mathcal{C}(I))$ must be a right-zero semigroup, which forces $|X| = 1$. Hence I is a right-zero semigroup.

Let $s \in S$ and $i \in I$. Then $\overline{i} \cdot \overline{s} = \overline{s}$ since $\overline{s}$ is a right-zero and by acting on the sequence $\alpha = x$ (where $x \in S$) we obtain $isx = sx$ for all $x \in S$. Hence

$sS = isS \subseteq I$ for all $s \in S$ and so $S^2 \subseteq I$. However, since I was assumed to be minimal, this forces $S^2 = I$.

($\Leftarrow$) Now suppose that $\{i_1, \ldots, i_k\} = I = S^2$ is the minimal ideal of S and is a right-zero semigroup. Let $s \in S$ and fix $i \in I$. Then $sx \in I$ and $isx = sx$ for any $x \in S$. By Theorem 3.6 $\overline{is} = \overline{s}$ and so for every $s \in S$ there exists $j \in I$ such that $\overline{s} = \overline{j}$. Consequently, $\Sigma(\mathcal{C}(S))$ can be generated by $\{\overline{i_1}, \ldots, \overline{i_k}\}$.

Let $\alpha \in S^*$. Then $\overline{i_2} \cdot \alpha = \beta$ where $\beta \in I^*$. Now since each term in β is a right-zero and $i_1 \in I$ we have $\overline{i_1} \cdot \beta = \beta$. Hence $\overline{i_1} \cdot \overline{i_2} = \overline{i_2}$ and hence $\Sigma(\mathcal{C}(S))$ is a right-zero semigroup. □

Having established which semigroups give rise to left- and right-zero semigroups, one may now consider if it is possible to obtain a rectangular band as a Cayley automaton semigroup. Such semigroups do arise as Cayley automaton semigroups and an example is exhibited after Proposition 3.24.

Recall that a semigroup is *nilpotent of class n* if $S^n = \{0\}$ but $S^{n-1} \neq \{0\}$ where 0 denotes the zero element of S.

Proposition 3.18 ([7, Proposition 6.13])**.** *Let S be a finite nilpotent semigroup of class n. Then $\Sigma(\mathcal{C}(S))$ is a finite nilpotent semigroup of class $n-1$.*

Proof. Let $x_1, \ldots, x_{n-1} \in S$. Also let $\alpha \in S^\omega$. Then

$$\overline{x_1} \cdot \ldots \cdot \overline{x_{n-1}} \cdot \alpha = 0^\omega$$

as every symbol in the output sequence is a product of at least n terms. Hence $\Sigma(\mathcal{C}(S))$ is nilpotent of class at most $n-1$.

Now let $x_1, \ldots, x_{n-1} \in S$ be such that $x_1 \ldots x_{n-1} \neq 0$. Then

$$\overline{x_1} \cdot \ldots \cdot \overline{x_{n-2}} \cdot x_{n-1} = (x_1 \ldots x_{n-1}) \neq 0 = \overline{0} \cdot x_{n-1}$$

and so $\overline{x_1} \cdot \ldots \cdot \overline{x_{n-2}} \neq \overline{0}$. Thus $\Sigma(\mathcal{C}(S))$ is $n-1$ nilpotent. $\square$

We now classify which semigroups give rise to free Cayley automaton semigroups. This result is proved from the perspective of wreath recursions in [25]. A simpler proof by acting on sequences is given here.

Proposition 3.19 ([25, Proposition 3])**.** *Let S be a finite semigroup. Then $\Sigma(\mathcal{C}(S))$ is free if and only if the minimal ideal K of S consists of a single $\mathcal{R}$-class in which every $\mathcal{H}$-class is non-trivial and there exists $k \in K$ such that $st = skt$ for all $s, t \in S$.*

Proof. ($\Rightarrow$) Let $\Sigma(\mathcal{C}(S))$ be free and K be the minimal ideal of S. Then K is isomorphic to a Rees-Matrix semigroup $K = \mathcal{M}[G; I, J; P]$ where G is a group with identity e, I and J are finite sets and P is a $J \times I$ matrix with entries in G. We may assume by [21, Theorem 3.4.2] that all entries in the first row and column of P are e. Thus the element $k = (1, e, 1)$ is an idempotent.

First we show that $st = skt$ for all $s, t \in S$.

Let $\alpha = \alpha_1\alpha_2\ldots\alpha_n \in S^*$. Then $\overline{k} \cdot \alpha = \beta_1\beta_2\ldots\beta_n$ where $\beta_i = k\alpha_1\alpha_2\ldots\alpha_i$. We have, for $s \in S$

$$\begin{aligned}\overline{sk} \cdot \overline{k} \cdot \alpha &= \overline{sk} \cdot \beta \\ &= (sk\beta_1)(sk\beta_1\beta_2)\ldots(sk\beta_1\beta_2\ldots\beta_n) \\ &= (s\beta_1)(s\beta_1\beta_2)\ldots(s\beta_1\beta_2\ldots\beta_n) \\ &= \overline{s} \cdot \beta \\ &= \overline{s} \cdot \overline{k} \cdot \alpha\end{aligned}$$

since $sk\beta_1 = skk\alpha_1 = sk\alpha_1 = s\beta_1$. Hence $\overline{sk} \cdot \overline{k} = \overline{s} \cdot \overline{k}$. Since $\Sigma(\mathcal{C}(S))$ is free, and hence cancellative, we have that $\overline{sk} = \overline{s}$ which implies by Theorem 3.6 that $skt = st$ for all $t \in S$.

Now we show that $kst = st$ for all $s, t \in S$. We will use this fact in determining the number of $\mathcal{R}$-classes in K.

Now let $\overline{ks} \cdot \alpha = \beta_1\beta_2\ldots\beta_n$ where $\beta_i = ks\alpha_1\ldots\alpha_i$ and $\overline{s} \cdot \alpha = \gamma_1\gamma_2\ldots\gamma_n$ where $\gamma_i = s\alpha_1\ldots\alpha_i$ (so $\beta_i = k\gamma_i$ and $k\beta_i = \beta_i$). Observe that

$$\begin{aligned}\gamma_i\beta_{i+1} &= s\alpha_1\alpha_2\ldots\alpha_{i-1}\alpha_i ks\alpha_1\alpha_2\ldots\alpha_{i+1} \\ &= s\alpha_1\alpha_2\ldots\alpha_{i-1}(\alpha_i ks)\alpha_1\alpha_2\ldots\alpha_{i+1} \\ &= s\alpha_1\alpha_2\ldots\alpha_{i-1}\alpha_i s\alpha_1\alpha_2\ldots\alpha_{i+1} \\ &= \gamma_i\gamma_{i+1}\end{aligned}$$

since $skt = st$ for all $s, t \in S$. Hence

$$\begin{aligned}
\overline{k} \cdot \overline{ks} \cdot \alpha &= \overline{k} \cdot \beta_1 \beta_2 \ldots \beta_n \\
&= (k\beta_1)(k\beta_1\beta_2) \ldots (k\beta_1\beta_2 \ldots \beta_n) \\
&= (\beta_1)(\beta_1\beta_2) \ldots (\beta_1\beta_2 \ldots \beta_n) \\
&= (k\gamma_1)(k\gamma_1\gamma_2) \ldots (k\gamma_1\gamma_2 \ldots \gamma_n) \\
&= \overline{k} \cdot \gamma_1\gamma_2 \ldots \gamma_n \\
&= \overline{k} \cdot \overline{s} \cdot \alpha
\end{aligned}$$

and so $\overline{k} \cdot \overline{ks} = \overline{k} \cdot \overline{s}$. Since $\Sigma(\mathcal{C}(S))$ is cancellative we obtain $\overline{ks} = \overline{s}$. Therefore by Theorem 3.6 $kst = st$ for all $s, t \in S$.

Finally, we consider the structure of the minimal ideal.

Now let $s = (i_s, g_s, j_s)$ and $t = (i_t, g_t, j_t)$ be elements of K. Then

$$(1, g_s P_{j_s i_t} g_t, j_t) = kst = st = (i_s, g_s P_{j_s i_t} g_t, j_t).$$

Hence $i_s = 1$ for all $i_s \in I$ so I is a singleton and K has only one $\mathcal{R}$-class.

Since $st = kst$ we have $S^2 \subseteq K$. Suppose that H is a non-singleton $\mathcal{H}$-class containing elements a and b. Then there exist elements u, v, x, y such that $a = vb = by$ and $b = ua = ax$. Hence $a, b \in S^2 \subseteq K$. Therefore the only non-singleton $\mathcal{H}$-classes of S must lie in K. If K contains only singleton $\mathcal{H}$-classes then S is aperiodic and so $\Sigma(\mathcal{C}(S))$ would be finite by Theorem

3.5, which is a contradiction. Hence all $\mathcal{H}$-classes in K are non-trivial (and isomorphic to each other).

($\Leftarrow$) Since K has only one $\mathcal{R}$-class it is of the form $G \times R$ where G is a non-trivial group with identity e and R is a right-zero semigroup. Let $k = (g, r)$ (where $g \in G$ and $r \in R$) be such that $st = skt$ for all $s, t \in S$ (so $\overline{s} = \overline{s(g, r)}$ by Theorem 3.6).

Let $s \in S$ be arbitrary. Then $s(g, r) = (h, r_1)$ for some $h \in G$ and $r_1 \in R$. Since $(g, r)(e, r) = (g, r)$ we have

$$s(g, r) = s(g, r)(e, r) = (h, r_1)(e, r) = (h, r)$$

and so $s(g, r) = (h, r)$. Hence $\overline{s(g, r)} = \overline{(h, r)}$.

Hence for every $s \in S$ we can write $\overline{s} = \overline{s(g, r)} = \overline{(h, r)}$ for some $(h, r) \in H_{(e,r)}$ (where $H_{(e,r)}$ denotes the $\mathcal{H}$-class containing (e, r)) and so $\Sigma(\mathcal{C}(S))$ is generated by $\{\overline{(g_1, r)}, \overline{(g_2, r)}, \ldots, \overline{(g_n, r)}\}$ where $|G| = n$. Since $H_{(e,r)}$ is a non-trivial group isomorphic to G we conclude that $\Sigma(\mathcal{C}(S)) \cong \Sigma(\mathcal{C}(H_{(e,r)}))$, which is free of rank $|G|$ by Theorem 3.4. $\square$

We conclude this section by stating a theorem that describes precisely when the Cayley automaton semigroup of a finite semigroup is a group. The proof, due to its length, is not given here.

Proposition 3.20 ([25, Theorem 6])**.** *Let S be a finite semigroup. Then the following are equivalent:*

1. $\Sigma(\mathcal{C}(S))$ *is a group,*

2. $\Sigma(\mathcal{C}(S))$ *is trivial,*

3. S *is an inflation of a right-zero semigroup by null semigroups.*

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

Maltcev's proof follows via the chain (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1). The implication (2) $\Rightarrow$ (1) is clear and (3) $\Rightarrow$ (2) is also fairly short. The difficulty is in the step (1) $\Rightarrow$ (3).

3.4 Subsemigroups, Quotients and Direct Products

In this final section we consider how the Cayley automaton semigroup construction behaves with respect to taking subsemigroups, direct products and quotients.

Proposition 3.21 ([28, Lemma 9(2)])**.** *Let* S *be a finite semigroup and let* $T \leq S$*. Then* $\Sigma(\mathcal{C}(T))$ *is a divisor of* $\Sigma(\mathcal{C}(S))$*.*

Proof. Recall that a semigroup W *divides* a semigroup U if there exists $V \leq U$ such that $U \geq V \twoheadrightarrow W$.

Let $Y = \langle \bar{t} : t \in T \rangle \leq \Sigma(\mathcal{C}(S))$. The elements of Y act on S^* and notice that $T^* \subseteq S^*$. Hence T^* is invariant under the action of Y. Hence the map $\bar{t} \mapsto \bar{t} \restriction_{T^*}$ is an epimorphism $Y \to \Sigma(\mathcal{C}(T))$. $\square$

In general it is not the case that if $T \leq S$ then $\Sigma(\mathcal{C}(T)) \leq \Sigma(\mathcal{C}(S))$. If, for example we consider $\{1\} \leq G$ where G is a non-trivial finite group then $\{1\} \not\leq F_{|G|}$.

However, we can state the following:

Proposition 3.22. *Let S be a finite semigroup and let G be a non-trivial subgroup of S. Then $\Sigma(\mathcal{C}(G))$ is isomorphic to a subsemigroup of $\Sigma(\mathcal{C}(S))$.*

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$. Then by Proposition 3.21 F_n divides $\Sigma(\mathcal{C}(S))$. We have

$$F_n = \Sigma(\mathcal{C}(G)) = \langle \overline{g_1} \restriction_{G^*}, \overline{g_2} \restriction_{G^*} \ldots \overline{g_n} \restriction_{G^*} \rangle \twoheadleftarrow \langle \overline{g_1}, \overline{g_2}, \ldots \overline{g_n} \rangle.$$

Hence $F_n \cong \langle \overline{g_1}, \overline{g_2}, \ldots \overline{g_n} \rangle$. $\square$

Proposition 3.23 ([28, Lemma 9(1)])**.** *Let S, T be semigroups and let $f : S \to T$ be an epimorphism. Then $\Sigma(\mathcal{C}(T))$ is a quotient of $\Sigma(\mathcal{C}(S))$.*

Proof. Let $s \in S$ and $\alpha = \alpha_1 \alpha_2 \ldots \alpha_n \in S^*$. Then $\overline{s} \cdot \alpha = (s\alpha_1)(s\alpha_1\alpha_2) \ldots (s\alpha_1\alpha_2 \ldots \alpha_n)$. Now let $\beta = \beta_1 \beta_2 \ldots \beta_n$ where

$\beta_i = f(\alpha_i)$. Applying the map f gives us

$$\begin{aligned}\overline{f(s)} \cdot \beta &= (f(s)\beta_1)(f(s)\beta_1\beta_2)\dots(f(s)\beta_1\beta_2\dots\beta_n)\\ &= (f(s\alpha_1))(f(s\alpha_1\alpha_2))\dots(f(s\alpha_1\alpha_2\dots\alpha_n))\end{aligned}$$

Hence the map $s \mapsto f(s)$ extends to a map $\overline{s} \mapsto \overline{f(s)}$. Extend this again to a map $\Sigma(\mathcal{C}(S)) \to \Sigma(\mathcal{C}(T))$. Now it follows from the previous calculation that if $\overline{x_1} \cdot \overline{x_2} \dots \overline{x_n} = \overline{y_1} \cdot \overline{y_2} \dots \overline{y_m}$ in $\Sigma(\mathcal{C}(S))$ then

$$\overline{f(x_1)} \cdot \overline{f(x_2)} \dots \overline{f(x_n)} = \overline{f(y_1)} \cdot \overline{f(y_2)} \dots \overline{f(y_m)}$$

in $\Sigma(\mathcal{C}(T))$. This shows that the map is well-defined and that any relation in $\Sigma(\mathcal{C}(S))$ is satisfied in $\Sigma(\mathcal{C}(T))$. Hence $\Sigma(\mathcal{C}(T))$ is a quotient of $\Sigma(\mathcal{C}(S))$. $\square$

Proposition 3.24 ([28, Lemma 20])**.** *Let S and T be semigroups. Then $\Sigma(\mathcal{C}(S \times T)) \leq \Sigma(\mathcal{C}(S)) \times \Sigma(\mathcal{C}(T))$.*

Proof. Define $\phi : \Sigma(\mathcal{C}(S \times T)) \to \Sigma(\mathcal{C}(S)) \times \Sigma(\mathcal{C}(T))$ by

$$\phi : \prod_{i=1}^{n} \overline{(s_i, t_i)} \mapsto (\prod_{i=1}^{n} \overline{s_i}, \prod_{i=1}^{n} \overline{t_i}).$$

This maps $\Sigma(\mathcal{C}(S \times T))$ onto the subsemigroup of $\Sigma(\mathcal{C}(S)) \times \Sigma(\mathcal{C}(T))$ of pairs of words of equal length. To see that this is well defined, let $\overline{f_1} \cdot \ldots \cdot \overline{f_n} \in \Sigma(\mathcal{C}(S \times T))$ map a string $w = (s_1, t_1)(s_2, t_2) \dots (s_n, t_n)$ (where $s_i \in S, t_j \in T$) to w'. Denote by w_S the string obtained from w by replacing each pair (s_i, t_i)

with s_i and we see that $\phi(\overline{f_1} \cdot \ldots \cdot \overline{f_n})$ maps w_S to w'_S regardless of how we expressed $\overline{f_1} \cdot \ldots \cdot \overline{f_n}$ as a product of generators. A similar argument works for T. The converse of this argument shows that the map ϕ is injective.

We now show that this is a homomorphism. Let $f = \prod_{i=1}^{n} \overline{(s_i, t_i)}$ and $g = \prod_{i=1}^{m} \overline{(u_i, v_i)}$. Then $\phi(f) = (\prod_{i=1}^{n} \overline{s_i}, \prod_{i=1}^{n} \overline{t_i})$ and $\phi(g) = (\prod_{i=1}^{m} \overline{u_i}, \prod_{i=1}^{m} \overline{v_i})$. Hence

$$\begin{aligned}\phi(f)\phi(g) &= (\prod_{i=1}^{n} \overline{s_i}, \prod_{i=1}^{n} \overline{t_i}) \cdot (\prod_{i=1}^{m} \overline{u_i}, \prod_{i=1}^{m} \overline{v_i}) \\ &= (\prod_{i=1}^{n} \overline{s_i} \cdot \prod_{i=1}^{m} \overline{u_i}, \prod_{i=1}^{n} \overline{t_i} \cdot \prod_{i=1}^{m} \overline{v_i}) \\ &= \phi(fg)\end{aligned}$$

□

We conclude this section by using Proposition 3.24 to show by example that rectangular bands can arise as Cayley automaton semigroups.

Example 3.25. Let T be the semigroup defined by the following Cayley Table:

	a	b	c	d
a	a	b	c	a
b	a	b	c	a
c	a	b	c	b
d	a	b	c	a

First we show that the multiplication in T is associative. A three-element product is determined entirely by the third element unless it is d. Consider a product of the form xyd where $x, y \in \{a, b, c, d\}$. If $y \neq c$ then $(xy)d = yd = a = xa = x(yd)$. In the remaining case we have $(xc)d = cd = b = xb = x(cd)$. Hence the multiplication is associative.

By Theorem 3.6 $\Sigma(\mathcal{C}(T)) = \langle \overline{a}, \overline{c} \rangle$. Observe that $T^2 = \{a, b, c\} \cong R_3$. Let $\alpha \in T^\omega$. Then

$$\overline{x} \cdot \overline{y} \cdot \alpha = (xy\alpha_1)(xy\alpha_1 y\alpha_1\alpha_2) \ldots = (y\alpha_1)(y\alpha_1\alpha_2) \ldots = \overline{y} \cdot \alpha$$

(where $x, y \in \{a, c\}$) since each $y\alpha_1\alpha_2 \ldots \alpha_n$ is a right-zero. Hence $\overline{x} \cdot \overline{y} = \overline{y}$ and $\Sigma(\mathcal{C}(T)) \cong R_2$.

Now let $L_2 = \{x, y\}$ and $S = L_2 \times T$. By Proposition 3.24,

$$\Sigma(\mathcal{C}(S)) \leq \Sigma(\mathcal{C}(L_2)) \times \Sigma(\mathcal{C}(T)) = L_2 \times R_2$$

and so $|\Sigma(\mathcal{C}(S))| \leq 4$. By Theorem 3.6 $\Sigma(\mathcal{C}(S)) = \langle \overline{(x, a)}, \overline{(x, c)}, \overline{(y, a)}, \overline{(y, c)} \rangle$ and so we conclude that $\Sigma(\mathcal{C}(S)) \cong L_2 \times R_2$.

Chapter 4

Cayley Automaton Semigroups of Finite Monogenic Semigroups

A semigroup is said to be *monogenic* if it can be generated by a single element. In this chapter, we will construct the Cayley automaton semigroups arising from finite monogenic semigroups. We will consider separately the cases where the semigroups do and do not have a non-trivial subgroup. The case of the infinite monogenic semigroup is deferred to Chapter 7.

Throughout this chapter the semigroup S will have the presentation

$$S = \langle x | x^r = x^{n+r} \rangle$$

where $n, r \in \mathbb{N}$ (so $S = \{x, x^2, \ldots, x^{n+r-1}\}$). The value r is referred to as the *index* of the semigroup and n is the *period*. In this chapter, $\alpha = \alpha_1\alpha_2\ldots$ will be an element of S^ω.

If a word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ (where $a_i \in \{1, 2, \ldots, r+n-1\}$) acts on α then we will denote the output by $\beta = \beta_1\beta_2\ldots \in S^\omega$. Since S is commutative, each β_i can be written as $x^{e_i}\gamma_i$ where e_i is a sum of the indices $a_1, a_2, \ldots, a_m$ and γ_i is a product of the terms $\alpha_1, \alpha_2, \ldots, \alpha_i$.

Lemma 4.1. *Let* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \alpha = \beta$. *Then* $\beta_k = x^{e_k}\gamma_k$ *where*

$$e_k = \binom{k-1}{0}a_1 + \binom{k}{1}a_2 + \ldots + \binom{k+m-2}{m-1}a_m$$

and γ_k *is a product of* $\alpha_1, \alpha_2, \ldots, \alpha_k$.

Proof. We will act on the sequence α one generator at a time. First consider $\overline{x^{a_m}}$. We obtain

$$\overline{x^{a_m}} \cdot \alpha = (x^{a_m}\alpha_1)(x^{a_m}\alpha_1\alpha_2)(x^{a_m}\alpha_1\alpha_2\alpha_3)\ldots.$$

Now consider $\overline{x^{a_{m-1}}} \cdot \overline{x^{a_m}} \cdot \alpha = \overline{x^{a_{m-1}}} \cdot (x^{a_m}\alpha_1)(x^{a_m}\alpha_1\alpha_2)(x^{a_m}\alpha_1\alpha_2\alpha_3)\ldots$. As the output we obtain

$$\begin{aligned}
&(x^{a_{m-1}}x^{a_m}\alpha_1)(x^{a_{m-1}}x^{a_m}\alpha_1x^{a_m}\alpha_1\alpha_2)(x^{a_{m-1}}x^{a_m}\alpha_1x^{a_m}\alpha_1\alpha_2x^{a_m}\alpha_1\alpha_2\alpha_3)\ldots\\
=&(x^{a_{m-1}+a_m}\alpha_1)(x^{a_{m-1}+(1+1)a_m}\alpha_1^2\alpha_2)(x^{a_{m-1}+(1+1+1)a_m}\alpha_1^3\alpha_2^2\alpha_3)\ldots\\
=&(x^{a_{m-1}+a_m}\alpha_1)(x^{a_{m-1}+2a_m}\alpha_1^2\alpha_2)(x^{a_{m-1}+3a_m}\alpha_1^3\alpha_2^2\alpha_3)\ldots.
\end{aligned}$$

Now introduce the next generator and consider $\overline{x^{a_{m-2}}} \cdot \overline{x^{a_{m-1}}} \cdot \overline{x^{a_m}} \cdot \alpha$ which we write as

$$\overline{x^{a_{m-2}}} \cdot (x^{a_{m-1}+a_m}\alpha_1)(x^{a_{m-1}+2a_m}\alpha_1^2\alpha_2)(x^{a_{m-1}+3a_m}\alpha_1^3\alpha_2^2\alpha_3)\ldots.$$

We obtain as the output $\nu_1\nu_2\nu_3\ldots$ where

$$\begin{aligned}\nu_1 &= x^{a_{m-2}}x^{a_{m-1}+a_m}\alpha_1\\ &= x^{a_{m-2}+a_{m-1}+a_m}\alpha_1\end{aligned}$$

and

$$\begin{aligned}\nu_2 &= x^{a_{m-2}}x^{a_{m-1}+a_m}\alpha_1 x^{a_{m-1}+2a_m}\alpha_1^2\alpha_2\\ &= x^{a_{m-2}+(1+1)a_{m-1}+(1+2)a_m}\alpha_1^3\alpha_2\\ &= x^{a_{m-2}+2a_{m-1}+3a_m}\alpha_1^3\alpha_2\end{aligned}$$

and

$$\begin{aligned}\nu_3 &= x^{a_{m-2}}x^{a_{m-1}+a_m}\alpha_1 x^{a_{m-1}+2a_m}\alpha_1^2\alpha_2 x^{a_{m-1}+3a_m}\alpha_1^3\alpha_2^2\alpha_3\\ &= x^{a_{m-2}+(1+1+1)a_{m-1}+(1+2+3)a_m}\alpha_1^6\alpha_2^3\alpha_3\\ &= x^{a_{m-2}+3a_{m-1}+6a_m}\alpha_1^6\alpha_2^3\alpha_3.\end{aligned}$$

Let us now consider $\overline{x^{a_{m-3}}} \cdot \overline{x^{a_{m-2}}} \cdot \overline{x^{a_{m-1}}} \cdot \overline{x^{a_m}} \cdot \alpha$ which we write as

$\overline{x^{a_{m-3}}} \cdot \nu_1\nu_2\nu_3 \ldots$. As the output we obtain $\xi_1\xi_2\xi_3\ldots$ where

$$\begin{aligned}
\xi_1 &= x^{a_{m-3}}\nu_1 \\
&= x^{a_{m-3}}x^{a_{m-2}+a_{m-1}+a_m}\alpha_1 \\
&= x^{a_{m-3}+a_{m-2}+a_{m-1}+a_m}\alpha_1
\end{aligned}$$

and

$$\begin{aligned}
\xi_2 &= x^{a_{m-3}}\nu_1\nu_2 \\
&= x^{a_{m-3}}x^{a_{m-2}+a_{m-1}+a_m}\alpha_1 x^{a_{m-2}+2a_{m-1}+3a_m}\alpha_1^3\alpha_2 \\
&= x^{a_{m-3}+(1+1)a_{m-2}+(1+2)a_{m-1}+(1+3)a_m}\alpha_1^4\alpha_2 \\
&= x^{a_{m-3}+2a_{m-2}+3a_{m-1}+4a_m}\alpha_1^4\alpha_2
\end{aligned}$$

and

$$\begin{aligned}
\xi_3 &= x^{a_{m-3}}\nu_1\nu_2\nu_3 \\
&= x^{a_{m-3}}x^{a_{m-2}+a_{m-1}+a_m}\alpha_1 x^{a_{m-2}+2a_{m-1}+3a_m}\alpha_1^3\alpha_2 x^{a_{m-2}+3a_{m-1}+6a_m}\alpha_1^6\alpha_2^3\alpha_3 \\
&= x^{a_{m-3}+(1+1+1)a_{m-2}+(1+2+3)a_{m-1}+(1+3+6)a_m}\alpha_1^{10}\alpha_2^4\alpha_3 \\
&= x^{a_{m-3}+3a_{m-2}+6a_{m-1}+10a_m}\alpha_1^{10}\alpha_2^4\alpha_3.
\end{aligned}$$

Continuing in this way will eventually yield, after all generators have been considered, $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \alpha = \beta_1\beta_2\beta_3\ldots$ where

$$\beta_1 = x^{a_1+a_2+a_3+\ldots+a_m}\gamma_1,$$

$$\beta_2 = x^{a_1+(1+1)a_2+(1+1+1)a_3+\ldots+(1+1+\ldots+1)a_m}\gamma_2,$$

$$\beta_3 = x^{a_1+(1+2)a_2+(1+2+3)a_3+\ldots+(1+2+\ldots+m)a_m}\gamma_3.$$

and the γ_i are products of $\alpha_1, \ldots, \alpha_i$.

Hence we have

$$\begin{array}{lllll}
e_1 = a_1 + & a_2 + & a_3 + \ldots + & & a_m \\
e_2 = a_1 + & (1+1)a_2 + & (1+1+1)a_3 + \ldots + & & (1+1+\ldots+1)a_m \\
e_3 = a_1 + & (1+2)a_2 + & (1+2+3)a_3 + \ldots + & & (1+2+\ldots+m)a_m \\
\quad\vdots & \vdots & \vdots & \vdots & \\
e_k = a_1 + & c_2a_2 + & c_3a_3 + \ldots + & & c_ma_m
\end{array}$$

where $c_2 = 1 + (k-1) = k$, $c_3 = 1 + (k-1) + \frac{k(k-1)}{2} = \frac{k(k+1)}{2}$ and $c_m = 1 + (k-1) + \frac{k(k-1)}{2} + \ldots + \frac{(k-1)k\ldots(k+m-4)}{(m-2)!} = \frac{k(k+1)\ldots(k+m-2)}{(m-1)!}$.

Reading down the columns above we observe that the figurate (or q-topic) numbers appear (see [12, Chapter 1] for more details on q-topic numbers). The b^{th} q-topic number is denoted by $P_q(b)$ and in general they are defined recursively by $P_0(b) = 1$ for all $b \geq 1$ and $P_q(b) = \sum_{i=1}^{b} P_{q-1}(i)$ (so, for clarity, the 0-topic numbers are $1, 1, 1, 1, \ldots$, the 1-topic numbers are $1, 2, 3, 4, \ldots$, the 2-topic (or triangular) numbers are $1, 3, 6, 10, \ldots$, the 3-topic (or tetrahedral) numbers are $1, 4, 10, 20, \ldots$ and so on).

This gives us $P_q(b) = \binom{b+q-1}{q}$ (see [12, p.7]) and so we may rewrite the above as

$$\begin{aligned}
e_1 &= \binom{0}{0}a_1 &&+ \binom{1}{1}a_2 + \binom{2}{2}a_3 &&+ \ldots + \binom{m-1}{m-1}a_m \\
e_2 &= \binom{1}{0}a_1 &&+ \binom{2}{1}a_2 + \binom{3}{2}a_3 &&+ \ldots + \binom{m}{m-1}a_m \\
e_3 &= \binom{2}{0}a_1 &&+ \binom{3}{1}a_2 + \binom{4}{2}a_3 &&+ \ldots + \binom{m+1}{m-1}a_m \\
& &&\vdots \qquad \vdots &&\vdots \quad \vdots \\
e_k &= \binom{k-1}{0}a_1 &&+ \binom{k}{1}a_2 + \binom{k+1}{2}a_3 &&+ \ldots + \binom{k+m-2}{m-1}a_m
\end{aligned}$$

□

The q-topic numbers are related to Pascal's Triangle. The first five rows of Pascal's Triangle are shown below:

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

and we observe that this can also be written as

$$\begin{array}{ccccccccc} & & & & P_0(1) & & & & \\ & & & P_0(2) & & P_1(1) & & & \\ & & P_0(3) & & P_1(2) & & P_2(1) & & \\ & P_0(4) & & P_1(3) & & P_2(2) & & P_3(1) & \\ P_0(5) & & P_1(4) & & P_2(3) & & P_3(2) & & P_4(1) \end{array}$$

(see [11, Section 4.2] for details). Note also that the q-topic numbers satisfy $P_q(b) = P_q(b-1)+P_{q-1}(b)$. We will return to the connection between Pascal's Triangle and the q-topic numbers later.

4.1 Non-trivial Subgroups

We move on now to consider the cases where the period n of the semigroup $S = \langle x | x^r = x^{n+r} \rangle$ is at least two. First we note that the cyclic group of order n is denoted C_n.

Lemma 4.2. *The free semigroup F_n of rank n is an ideal in $\Sigma(\mathcal{C}(S))$.*

Proof. As a subgroup of S we have $\{x^r, x^{r+1}, \ldots, x^{r+n-1}\} \cong C_n$. By Proposition 3.22 $F_n \cong \langle \overline{x^r}, \overline{x^{r+1}}, \ldots, \overline{x^{r+n-1}} \rangle \leq \Sigma(\mathcal{C}(S))$. Let $s \in C_n$ and $t \notin C_n$. Since $st \in C_n$ there exists $u \in C_n$ such that $st = ts = us = su$. This follows from the fact that C_n is an ideal in S and that S is commutative.

Assume that $st^n = su^n$ for some $n \in \mathbb{N}$ (note that the case $n = 1$ is established above). Then by induction we have

$$st^{n+1} = (st^n)t = (su^n)t = (st)u^n = (su)u^n = su^{n+1}.$$

Hence $st^n = su^n$ for all $n \in \mathbb{N}$.

Hence

$$\overline{s} \cdot \overline{t} \cdot \alpha = (st\alpha_1)(st^2\alpha_1^2\alpha_2)\ldots = (su\alpha_1)(su^2\alpha_1^2\alpha_2)\ldots = \overline{s} \cdot \overline{u} \cdot \alpha$$

and so $\overline{s} \cdot \overline{t} = \overline{s} \cdot \overline{u}$.

Now consider $(\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}) \cdot (\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}})$ where $a_i \in \{r, r+1, \ldots, r+n-1\}$ and $b_j \in \{1, 2, \ldots, r+n-1\}$ with $b_1 \leq r-1$. Hence $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in F_n$. Using the result in the preceding paragraph, we can write $\overline{x^{a_m}} \cdot \overline{x^{b_1}} = \overline{x^{a_m}} \cdot \overline{x^{c_1}}$ where $c_1 \in \{r, r+1, \ldots, r+n-1\}$.

Applying this repeatedly gives us

$$\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}} = \overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \overline{x^{c_1}} \cdot \overline{x^{c_2}} \cdot \ldots \cdot \overline{x^{c_k}}$$

where $c_i \in \{r, r+1, \ldots, r+n-1\}$. Hence F_n is a left ideal.

By a symmetric argument, F_n is also a right ideal and is therefore a two-sided ideal. $\square$

Lemma 4.3. *$\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in F_n$ if and only if $\sum_{i=1}^{m} a_i \geq r-1$. Consequently, any element $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in F_n$ can be written uniquely as $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$*

where $b_i \in \{r, r+1, \ldots, r+n-1\}$ *and* $a_i \equiv b_i \mod n$.

Proof. Let $a_i \in \{1, 2, \ldots, r+n-1\}$. Then there exists a unique $b_i \in \{r, r+1, \ldots, r+n-1\}$ such that $a_i \equiv b_i \mod n$. By acting on a sequence α with the words $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$ we obtain the following:

$$\begin{aligned}\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \alpha =& (x^{e_1}\gamma_1)(x^{e_2}\gamma_2)(x^{e_3}\gamma_3)\ldots \\ \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}} \cdot \alpha =& (x^{f_1}\gamma_1)(x^{f_2}\gamma_2)(x^{f_3}\gamma_3)\ldots\end{aligned}$$

where e_i and f_j are as in the notation used in Lemma 4.1. Since the γ_i terms depend only on α and m the same terms appear in both output sequences.

Hence $e_i \equiv f_i \mod n$ for all i and provided that $e_1 = \sum_{i=1}^{m} a_i \geq r-1$ we have $x^{e_i}\gamma_i = x^{f_i}\gamma_i$ and the outputs are equal. If $e_1 < r-1$ then it is possible to have $x^{e_1}\gamma_i \in S \setminus C_n$ and $x^{f_1}\gamma_1 \in C_n$ which would contradict equality of the outputs. Hence $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}} \in F_n$.

Conversely, if $\sum_{i=1}^{m} a_i < r-1$ then $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot x = x^{\left(\sum_{i=1}^{m} a_i\right)+1}$ and $\sum_{i=1}^{m} a_i + 1 \leq r-1$. Hence this can not be an element in the ideal as $x^{\left(\sum_{i=1}^{m} a_i\right)+1} \in S \setminus C_n$. $\square$

We also have the following corollary:

Corollary 4.4. $\Sigma(\mathcal{C}(S))$ *is a small extension of* F_n.

Proof. Recall that a semigroup U is a *small extension* of V if $|U \setminus V| < \infty$.

The statement of Lemma 4.3 is equivalent to saying that $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \notin F_n$ if and only if $\sum_{i=1}^{m} a_i < r - 1$. Given that $a_i \in \{1, 2, \ldots, r + n - 1\}$ there are only finitely many such sums. $\square$

Many properties of semigroups are preserved when passing to a small extension, such as finite generation [8], finite presentability [31] and automaticity [20]. Hence we have the following:

Corollary 4.5. *$\Sigma(\mathcal{C}(S))$ is finitely generated, finitely presented and automatic.*

Proposition 4.6. *$\Sigma(\mathcal{C}(S))/F_n$ is nilpotent of class $r - 1$.*

Proof. We have that $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \notin F_n$ if and only if $\sum_{i=1}^{m} a_i < r - 1$. A word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_{r-1}}}$ of length $r-1$ must satisfy $\sum_{i=1}^{m} a_i \geq r - 1$ since $a_i \geq 1$ for each i and hence lies in F_n. Hence $\Sigma(\mathcal{C}(S))/F_n$ is nilpotent of class at most $r - 1$. The word $\underbrace{\overline{x} \cdot \overline{x} \cdot \ldots \cdot \overline{x}}_{r-2}$ satisfies $\sum_{i=1}^{m} a_i = r - 2$ and so does not lie in F_n. Hence $\Sigma(\mathcal{C}(S))/F_n$ is nilpotent of class equal to $r - 1$. $\square$

Having established that there are only finitely many words not in the ideal F_n we move now towards identifying when two words are equal. For the remainder of this section we will assume that the words $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ are such that $\sum_{i=1}^{m} a_i < r - 1$ and $\sum_{j=1}^{k} b_j < r - 1$.

Lemma 4.7. *If* $\sum_{i=1}^{m} a_i \neq \sum_{j=1}^{k} b_j$ *then* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$.

Proof. Consider both words acting on the sequence x. Then

$$\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot x = x^{\left(\sum_{i=1}^{m} a_i\right)+1} \neq x^{\left(\sum_{j=1}^{k} b_j\right)+1} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}} \cdot x$$

and hence

$$\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}.$$

□

Lemma 4.8. *If $m \neq k$ then $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$.*

Proof. Assume that $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$. Let p be such that $\sum_{i=1}^{m} a_i + p \geq r-1$ and $\sum_{j=1}^{k} b_j + p \geq r-1$. Consider the words $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \overline{x^{p}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}} \cdot \overline{x^{p}}$. These words lie in F_n by Lemma 4.3 and so can be written uniquely as $\overline{x^{c_1}} \cdot \overline{x^{c_2}} \cdot \ldots \cdot \overline{x^{c_m}} \cdot \overline{x^{p_1}}$ and $\overline{x^{d_1}} \cdot \overline{x^{d_2}} \cdot \ldots \cdot \overline{x^{d_k}} \cdot \overline{x^{p_1}}$ where $a_i \equiv c_i \bmod n$, $b_i \equiv d_i \bmod n$, $p \equiv p_1 \bmod n$ and $c_i, d_i, p_1 \in \{r, r+1, \ldots, r+n-1\}$.

Hence $\overline{x^{c_1}} \cdot \overline{x^{c_2}} \cdot \ldots \cdot \overline{x^{c_m}} \cdot \overline{x^{p_1}} = \overline{x^{d_1}} \cdot \overline{x^{d_2}} \cdot \ldots \cdot \overline{x^{d_k}} \cdot \overline{x^{p_1}} \in F_n$ which can only hold if $m = k$. □

Thus far we have established two necessary, but not sufficient, conditions for equality of words. Namely, $k = m$ and $\sum_{i=1}^{m} a_i = \sum_{j=1}^{k} b_j$.

If $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$ both act on the same sequence α then we will denote the outputs obtained by $(x^{e_{a,1}}\gamma_1)(x^{e_{a,2}}\gamma_2)\ldots$ and $(x^{e_{b,1}}\gamma_1)(x^{e_{b,2}}\gamma_2)\ldots$ respectively.

Recall from Lemma 4.1 that

$$\begin{aligned} e_{a,t} &= \tbinom{t-1}{0}a_1 + \tbinom{t}{1}a_2 \quad + \ldots + \tbinom{t+m-2}{m-1}a_m \\ &= P_0(t)a_1 + P_1(t)a_2 + \ldots + P_{m-1}(t)a_m \end{aligned}$$

and

$$\begin{aligned} e_{b,t} &= \tbinom{t-1}{0}b_1 + \tbinom{t}{1}b_2 \quad + \ldots + \tbinom{t+m-2}{m-1}b_m \\ &= P_0(t)b_1 + P_1(t)b_2 + \ldots + P_{m-1}(t)b_m. \end{aligned}$$

Let us define

$$\begin{aligned} E(m,t) &= e_{a,t} - e_{b,t} \\ &= \tbinom{t-1}{0}X_1 \ + \tbinom{t}{1}X_2 \quad + \ldots + \tbinom{t+m-2}{m-1}X_m \\ &= P_0(t)X_1 \ + P_1(t)X_2 + \ldots + P_{m-1}(t)X_m \end{aligned}$$

where $X_i = a_i - b_i$.

Observe that

$$\begin{aligned} E(m,1) = 0 &\iff (a_1 - b_1) + (a_2 - b_2) + \ldots + (a_m - b_m) = 0 \\ &\iff a_1 + a_2 + \ldots a_m = b_1 + b_2 + \ldots + b_m \\ &\iff \sum_{i=1}^{m} a_i = \sum_{i=1}^{m} b_i. \end{aligned}$$

Lemma 4.9. *If two words are equal then* $E(m,t) \equiv 0 \mod n$ *for all* t.

Proof. Suppose that $E(m,i) \not\equiv 0 \mod n$ for some i. So $e_{a,i} \not\equiv e_{b,i} \mod n$. Write $\gamma_i = x^v$ for some v. We have that $e_{a,i} + v \not\equiv e_{b,i} + v \mod n$. Therefore $x^{e_{a,i}}\gamma_i = x^{e_{a,i}+v} \neq x^{e_{b,i}+v} = x^{e_{b,i}}\gamma_i$. □

Lemma 4.10. *If* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ *and* $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$ *are equal then there exists* j *such that* $x^{e_{a,j}}\gamma_j, x^{e_{b,j}}\gamma_j \in C_n$ *but* $x^{e_{a,j-1}}\gamma_{j-1}, x^{e_{b,j-1}}\gamma_{j-1} \notin C_n$*.*

Proof. If there does not exist such a j then there must exist g such that (without loss of generality) $x^{e_{a,g}}\gamma_g \in C_n$ but $x^{e_{b,g}}\gamma_g \notin C_n$ which contradicts the equality of the words. $\square$

If $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$ then we have $E(m,1) = 0$ and $E(m,t) \equiv 0 \mod n$ for all t. Hence there must exist f such that $E(m,i) = 0$ for all $i < f$ and $E(m,f) \equiv 0 \mod n$ but $E(m,f) \neq 0$. Note that we must have $f \leq m$ otherwise we would have m equations in $X_1, \ldots, X_m$ which would force $a_i = b_i$ for all i.

Lemma 4.11. *If* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$ *then* $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f \in C_n$*.*

Proof. Suppose that $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f \notin C_n$. Write $\gamma_f = x^v$ for some v. Then $x^{e_{a,f}+v} = x^{e_{b,f}+v} \implies e_{a,f} = e_{b,f} \implies E(m,f) = 0$ which contradicts the value of f. $\square$

Lemma 4.12. *There exist* $t_1 < t_2$ *such that* $E(m,t_1) = E(m,t_2)$*.*

Proof. A typical $E(m,t)$ has the form

$$E(m,t) = P_0(t)X_1 + P_1(t)X_2 + \ldots + P_{m-1}(t)X_m.$$

Notice that the X_i terms are not dependent on t. By considering each $P_i(t)$ modulo n (and noting that $P_0(t) = 1$ for all t) there are at most n^{m-1} different such $E(m, t)$. Hence there must exist t_1, t_2 such that $E(m, t_1) = E(m, t_2)$. $\square$

Since the coefficients of the X_i terms are defined by the recurrence relation $P_q(b) = P_q(b-1) + P_{q-1}(b)$ with $P_0(b) = 1$, once we have $E(m, 1)$ the remaining $E(m, t)$ are completely determined. Once we find the values t_1 and t_2 as per Lemma 4.12 all of the subsequent $E(m, t)$ are determined by $E(m, t_2 + k) = E(m, t_1 + (k \mod (t_2 - t_1)))$.

Collating the above results, we can state exactly when two words are equal:

Theorem 4.13. *Let $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ be words in $\Sigma(\mathcal{C}(S))$ such that $\sum_{i=1}^{m} a_i, \sum_{j=1}^{k} b_j < r-1$. Then the words are equal if and only if the following hold:*

1. *$k = m$,*
2. *There exists $f \in \{1, \ldots, m\}$ such that*
   (a) *$E(m, i) = 0$ for $i < f$,*
   (b) *$E(m, j) \neq 0$ but $E(m, j) \equiv 0 \mod n$ for $j \geq f$,*
   (c) *$x^{e_{a,f}}\gamma_f, x^{e_{b,f}}\gamma_f \in C_n$.*

Proof. The forwards implication holds by Lemmas 4.8, 4.9 and 4.11. It remains to establish the reverse implication.

Suppose first that $k = m$. Then $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \alpha = (x^{e_{a,1}}\gamma_1)(x^{e_{a,2}}\gamma_2)\ldots$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}} \cdot \alpha = (x^{e_{b,1}}\delta_1)(x^{e_{b,2}}\delta_2)\ldots$.

Since γ_i and δ_i depend only on m and α we conclude that $\gamma_i = \delta_i$ for all i. Thus we may write $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}} \cdot \alpha = (x^{e_{b,1}}\gamma_1)(x^{e_{b,2}}\gamma_2)\ldots$.

By condition 2a, $E(m, i) = 0$ for $i < f$ and so $e_{a,i} = e_{b,i}$ for $i = 1, 2, \ldots, f-1$ and so the first $f - 1$ terms of the outputs are equal.

Condition 2b ensures that $e_{a,j} \equiv e_{b,j} \mod n$ for $j \geq f$. By condition 2c we have $x^{e_{a,f}}\gamma_f, x^{e_{b,f}}\gamma_f \in C_n$. Write $\gamma_f = x^v$ for some v. Hence $x^{e_{a,f}+v}, x^{e_{b,f}+v} \in C_n$ and since $e_{a,f} + v \equiv e_{b,f} + v \mod n$ we conclude $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f$. All the terms $x^{e_{a,j}}\gamma_j, x^{e_{b,j}}\gamma_j$ where $j > f$ are also in C_n and we obtain equality for each j by the same reasoning. $\square$

We now seek to improve the conditions given in Theorem 4.13. In particular, we seek a condition that is easier to check than condition 2b in Theorem 4.13. We begin by considering the cases when the period of the semigroup is prime (and so the subgroup in S is C_p, the cyclic group of order p). We do this by first returning to the connection between the q-topic numbers and Pascal's Triangle.

Lemma 4.14 (Lucas's Theorem [14, Theorem 1])**.** *For $n, m \in \mathbb{N} \cup \{0\}$ and a prime p we have*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod p$$

where

$$m = m_k p^k + m_{k-1} p^{k-1} + \ldots + m_1 p + m_0$$

and

$$n = n_k p^k + n_{k-1} p^{k-1} + \ldots + n_1 p + n_0$$

are the base p expansions of m and n and $\binom{m_i}{n_i} = 0$ if $m_i < n_i$.

In [24], Long considers Pascal's Triangle modulo a prime p. He defines $\nabla^d_{s,t}$ to be the triangle of entries in Pascal's Triangle with corners $\binom{sp^d}{tp^d+1}$, $\binom{sp^d}{tp^d+p^d-1}$ and $\binom{sp^d+p^d-2}{tp^d+p^d-1}$ where $0 \leq t < s$ and $d \geq 1$. All entries are taken modulo p. Thus every entry in $\nabla^d_{s,t}$ has the form $\binom{sp^d+y}{tp^d+z}$ where $0 \leq y < z \leq p^d - 1$.

Lemma 4.15. *For all $d \geq 0$, all entries $\binom{sp^d+y}{tp^d+z} \in \nabla^d_{s,t}$ are congruent to 0 modulo p.*

Proof. By Lemma 4.14 $\binom{sp^d+y}{tp^d+z} \equiv \binom{s}{t}\binom{y}{z} \equiv 0 \mod p$ since $y < z$. □

As an illustration, let us fix $p = 2$ and consider $\nabla^2_{1,0}$ which is highlighted in bold. This has corners $\binom{4}{1}$, $\binom{4}{3}$ and $\binom{6}{3}$.

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 0 & & 1 & & & & \\
 & & & 1 & & 1 & & 1 & & 1 & & & \\
 & & 1 & & \mathbf{0} & & \mathbf{0} & & \mathbf{0} & & 1 & & \\
 & 1 & & 1 & & \mathbf{0} & & \mathbf{0} & & 1 & & 1 & \\
1 & & 0 & & 1 & & \mathbf{0} & & 1 & & 0 & & 1
\end{array}
$$

Lemma 4.16. *Let p be a prime. Then $E(m,t) \equiv 0 \mod p$ for all t if and only if $X_i = a_i - b_i \equiv 0 \mod p$ for all $i \in \{1,\ldots,m\}$.*

Proof. The reverse implication is trivial.

For the forward implication, find d such that $p^{d-1} < m \le p^d$ and consider $\nabla^d_{1,0}$. This has corners $\binom{p^d}{1}, \binom{p^d}{p^d-1}$ and $\binom{2p^d-2}{p^d-1}$. With the exception of the entries on the outermost diagonals, $\nabla^d_{1,0}$ spans the width of Pascal's Triangle along its top. The coefficients of the X_i $(i \ge 2)$ terms in $E(m,p^d)$ correspond to the first $m-1$ terms on the diagonal edge of $\nabla^d_{1,0}$, namely $\binom{p^d}{1}, \ldots, \binom{p^d+m-2}{p^d-1}$.

By Lemma 4.15 we have $E(m,p^d) = \binom{p^d-1}{0}X_1 + \underbrace{0 + \ldots + 0}_{m-1 \text{ times}} \equiv 0 \mod p$ which forces $X_1 \equiv 0 \mod p$ and hence $a_1 \equiv b_1 \mod p$.

We have $E(m,p^d-1) = \binom{p^d-2}{0}X_1 + \binom{p^d-1}{1}X_2 + \underbrace{0 + \ldots + 0}_{m-2 \text{ times}} \equiv 0 \mod p$ which forces $X_2 \equiv 0 \mod p$ and hence $a_2 \equiv b_2 \mod p$.

By continuing in this fashion, when we consider $E(m, p^d - j)$ we will have already shown that $X_1, X_2, \ldots, X_j \equiv 0 \mod p$. The coefficient of X_{j+1} can never be zero as this would contradict $P_j(p^d - j) = P_j(p^d - j + 1) - P_{j-1}(p^d - j + 1)$ as we know $P_j(p^d - j + 1) \equiv 0$ and $P_{j-1}(p^d - j + 1) \not\equiv 0$. This then forces $X_j \equiv 0 \mod p$ for all j. $\square$

We now have a modified version of Theorem 4.13 in the case of a prime modulus:

Theorem 4.17. *Let $S = \langle x | x^r = x^{r+p} \rangle$ where p is prime. Let $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ be words in $\Sigma(\mathcal{C}(S))$ such that $\sum_{i=1}^{m} a_i, \sum_{j=1}^{k} b_j < r - 1$. Then the words are equal if and only if the following hold:*

1. $k = m$,
2. $a_i \equiv b_i \mod p$ *for all* i,
3. *There exists a maximal* $f \in \{1, \ldots, m\}$ *such that*
   (a) $E(m, i) = 0$ *for* $i < f$,
   (b) $x^{e_{a,f}} \gamma_f, x^{e_{b,f}} \gamma_f \in C_p$.

Note that the condition in Theorem 4.13 where we required $E(m, j) \equiv 0 \mod p$ for $j \geq f$ is subsumed by condition 2 above.

Having considered prime moduli, we now extend the arguments to an arbitrary modulus n. We show the existence of l such that

$$\binom{l}{1}, \binom{l+1}{2}, \ldots, \binom{l+m-2}{m-1} \equiv 0 \mod n.$$

This will give us $E(m,l) = \binom{l-1}{0}X_1 + \underbrace{0 + \ldots + 0}_{m-1 \text{ times}} \equiv 0 \mod n$ which forces $X_1 \equiv 0 \mod n$. Working back up the diagonals of Pascal's Triangle, similar to in the prime modulus case, we will always force $X_{j+1} \equiv 0 \mod n$ at the $(l-j)^{th}$ congruence. This gives $a_i \equiv b_i \mod n$ for all i.

We require $\binom{l}{1} = l \equiv 0 \mod n$ and so $l = qn$ for some q. Notice that

$$\binom{l+i}{i+1} = \frac{l(l+1)(l+2)\ldots(l+i)}{(i+1)!} = \frac{qn(l+1)(l+2)\ldots(l+i)}{(i+1)!}$$

and so if $q = \operatorname{lcm}(2!, 3!, \ldots, (m-1)!) = (m-1)!$ then $\binom{l+i}{i+1} \equiv 0 \mod n$ for all $i \in \{0, 1, \ldots, m-2\}$. This gives us the required congruence.

We can now state a further amended version of Theorem 4.13:

Theorem 4.18. *Let $S = \langle x | x^r = x^{r+n} \rangle$. Let $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ be words in $\Sigma(\mathcal{C}(S))$ such that $\sum_{i=1}^{m} a_i, \sum_{j=1}^{k} b_j < r-1$. Then the words are equal if and only if the following hold:*

1. *$k = m$,*
2. *$a_i \equiv b_i \mod n$ for all i,*
3. *There exists a maximal $f \in \{1, \ldots, m\}$ such that*
   (a) *$E(m,i) = 0$ for $i < f$,*

(b) $x^{e_{a,f}}\gamma_f, x^{e_{b,f}}\gamma_f \in C_n$.

Having completely determined the elements of $\Sigma(\mathcal{C}(S)) \setminus F_n$ in Theorem 4.18 we now put some bounds on the size of $\Sigma(\mathcal{C}(S)) \setminus F_n$.

Theorem 4.19. *Let* $S = \langle x | x^r = x^{r+n} \rangle$. *Then*

$$r - 2 \leq |\Sigma(\mathcal{C}(S)) \setminus F_n| \leq 2^{r-2} - 1.$$

Proof. The set $\Sigma(\mathcal{C}(S)) \setminus F_n$ must at least contain $\{\overline{x}, \overline{x^2}, \ldots, \overline{x^{r-2}}\}$ and so $r - 2 \leq |\Sigma(\mathcal{C}(S)) \setminus F_n|$.

A word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in \Sigma(\mathcal{C}(S)) \setminus F_n$ must satisfy $\sum_{i=1}^{m} a_i < r - 1$ by Lemma 4.3. Therefore, by considering all ordered partitions of the integers $1, 2, \ldots, r-2$ (that is, ways to express an integer as a sum of smaller integers where the order of the terms matters) we obtain an upper bound on $|\Sigma(\mathcal{C}(S)) \setminus F_n|$ (note that we must consider ordered partitions and not simply partitions as in general $\Sigma(\mathcal{C}(S))$ is not commutative).

A positive integer k has 2^{k-1} ordered partitions. Hence the total number of ordered partitions to consider is $2^0 + 2^1 + \ldots + 2^{r-3} = 2^{r-2} - 1$. $\square$

We will see later in Example 4.26 that the upper bound can be attained.

4.2 Trivial Subgroups

We now consider the cases where the semigroup S has a presentation

$$S = \langle x | x^r = x^{r+1} \rangle$$

and hence the subgroup is trivial. The semigroup is therefore aperiodic and by Theorem 3.5 $\Sigma(\mathcal{C}(S))$ is finite. Note also that S is nilpotent of class r and so by Proposition 3.18 we see $\Sigma(\mathcal{C}(S))$ is nilpotent of class $r-1$.

First notice that $x^r a = x^r = x^{r-1}a$ for all $a \in S$ and so by Theorem 3.6 we conclude that $\overline{x^r} = \overline{x^{r-1}}$.

Lemma 4.20. *Let* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in \Sigma(\mathcal{C}(S))$. *Then* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{r-1}}$ *if and only if* $\displaystyle\sum_{i=1}^{m} a_i \geq r-1$.

Proof. If $\sum_{i=1}^{m} a_i \geq r-1$ then

$$\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \alpha = (x^{\sum_{i=1}^{m} a_i}\alpha_1)(x^{\sum_{i=1}^{m} ia_i}\alpha_1^m\alpha_2)\ldots = (x^r)^\omega = \overline{x^{r-1}} \cdot \alpha$$

and so $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{r-1}}$.

If $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{r-1}}$ then by equating the first terms of the outputs we obtain $x^{\sum_{i=1}^{m} a_i}\alpha_1 = x^{r-1}\alpha_1 = x^r$. Hence $x^{\sum_{i=1}^{m} a_i}\alpha_1 = x^q$ where q is at least $\sum_{i=1}^{m} a_i + 1 \geq r$ and so $\sum_{i=1}^{m} a_i \geq r-1$. $\square$

Lemma 4.21. *Let* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in \Sigma(\mathcal{C}(S))$. *Then* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{r-2}}$

if and only if $\sum_{i=1}^{m} a_i = r - 2$.

Proof. If $\sum_{i=1}^{m} a_i = r - 2$ then

$$\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \cdot \alpha = (x^{\sum_{i=1}^{m} a_i}\alpha_1)(x^{\sum_{i=1}^{m} ia_i}\alpha_1^m\alpha_2)\ldots = (x^{r-2}\alpha_1)(x^r)^\omega = \overline{x^{r-2}} \cdot \alpha$$

and so $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{r-2}}$.

If $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{r-2}}$ then by equating the first terms in the output we obtain $x^{\sum_{i=1}^{m} a_i}\alpha_1 = x^{r-2}\alpha_1$ and so for equality with all values of α_1 (and in particular $\alpha_1 = x$) this forces $\sum_{i=1}^{m} a_i = r - 2$. $\square$

As a consequence of Lemmas 4.20 or 4.21 it is possible for words of different lengths to be equal in $\Sigma(\mathcal{C}(S))$. Observe that this is in stark contrast to the non-trivial subgroup case in Section 4.1 where to have equality of words we required the words to have the same length.

This behaviour can also happen when the sums of the indices in the words are less than $r - 2$. Consider $S = \langle x | x^9 = x^{10} \rangle$. Then

$$\overline{x^2} \cdot \overline{x^3} \cdot \alpha = (x^5\alpha_1)(x^9)^\omega = \overline{x^3} \cdot \overline{x} \cdot \overline{x} \cdot \alpha.$$

For equality of words $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ where $k \neq m$ and $\sum_{i=1}^{m} a_i, \sum_{j=1}^{k} b_j < r - 2$ we still require the condition from Lemma 4.7 that

$\sum\limits_{i=1}^{m} a_i = \sum\limits_{j=1}^{k} b_j$. We now classify exactly when words of different lengths are equal.

Lemma 4.22. *Let $k \neq m$ and $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}, \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ be such that $\sum\limits_{i=1}^{m} a_i = \sum\limits_{j=1}^{k} b_j < r-2$. Then $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ if and only if $x^{e_{a,2}}\gamma_2 = x^{e_{b,2}}\gamma_2 = x^r$.*

Proof. The reverse implication is trivial.

For the forwards implication, assume that $x^{e_{a,2}}\gamma_2 \neq x^r$ and $x^{e_{b,2}}\gamma_2 \neq x^r$. After acting on a sequence α, we obtain $x^{e_{a,2}}\gamma_2 = x^{e_{a,2}}\alpha_1^m\alpha_2$ and $x^{e_{b,2}}\gamma_2 = x^{e_{b,2}}\alpha_1^k\alpha_2$ where $e_{a,2} = \sum\limits_{i=1}^{m} ia_i$ and $e_{b,2} = \sum\limits_{j=1}^{k} jb_j$.

If $\sum\limits_{i=1}^{m} ia_i = \sum\limits_{j=1}^{k} jb_j$ then since $m \neq k$, $\alpha_1^m \neq \alpha_1^k$ and so $x^{e_{a,2}}\gamma_2 \neq x^{e_{b,2}}\gamma_2$ which gives $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$.

Now assume without loss of generality that $\sum\limits_{i=1}^{m} ia_i = \sum\limits_{j=1}^{k} jb_j + p$ for some $p > 0$. If $k = m + s$ for some $s > 0$ then acting on the sequence $xxx\ldots$ and equating $x^{e_{a,2}}\gamma_2$ with $x^{e_{b,2}}\gamma_2$ we obtain $x^{c_1} = x^{c_2}$ where

$$c_1 = \Big(\sum_{j=1}^{k} jb_j\Big) + p + m + 1$$

and

$$c_2 = \Big(\sum_{j=1}^{k} jb_j\Big) + m + s + 1$$

which forces $p = s$. Conversely, by acting on an arbitrary sequence α and setting $x^{e_{a,2}}\gamma_2 = x^{e_{b,2}}\gamma_2$ we obtain

$$x^c x^p \alpha_1^m \alpha_2 = x^c \alpha_1^m \alpha_1^p \alpha_2$$

(where $c = \sum_{j=1}^{k} jb_j$) which forces $x^p = \alpha_1^p$ and hence $x = \alpha_1$.

Hence by taking $\alpha_1 = x^2$ we can show that $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$. In the cases when $p \neq s$ we show $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ by choosing $\alpha_1 = x$.

If $m = k + y$ for some $y > 0$ then acting on a sequence α and setting $x^{e_{a,2}}\gamma_2 = x^{e_{b,2}}\gamma_2$ we obtain

$$x^c \alpha_1^k \alpha_2 x^p \alpha_1^y = x^c \alpha_1^k \alpha_2$$

(where $c = \sum_{j=1}^{k} jb_j$) which forces $x^p \alpha_1^y$ to be equal to the empty word which is a contradiction and hence $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \neq \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$.

Acting on the sequence $xxx\ldots$ now verifies that $x^{e_{a,2}}\gamma_2 = x^{e_{b,2}}\gamma_2 = x^r$. □

Having considered the case when two words have different lengths, we look now at what happens when they have the same length.

Lemma 4.23. $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$ *if and only if there exists* f *such that* $E(m, i) = 0$ *for* $i < f$ *and* $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f = x^r$.

Proof. Suppose that $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$. Then since x^r

is the zero element of S, there must exist f such that $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f = x^r$ but $x^{e_{a,f-1}}\gamma_{f-1} = x^{e_{b,f-1}}\gamma_{f-1} \neq x^r$. The only way to have the equalities $x^{e_{a,i}}\gamma_i = x^{e_{b,i}}\gamma_i$ when $i < f$ is to have $e_{a,i} = e_{b,i}$ and hence $E(m,i) = 0$ for $i < f$.

Conversely, suppose we have $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = (x^{e_{a,1}}\gamma_1)(x^{e_{a,2}}\gamma_2)\ldots$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}} = (x^{e_{b,1}}\gamma_1)(x^{e_{b,2}}\gamma_2)\ldots$. For $i < f$ we have $E(m,i) = 0$ and so $e_{a,i} = e_{b,i}$ and hence $x^{e_{a,i}}\gamma_i = x^{e_{b,i}}\gamma_i$ for $i < f$. Since $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f = x^r$ and x^r is the zero element of S we conclude that $x^{e_{a,j}}\gamma_j = x^{e_{b,j}}\gamma_j$ for $j \geq f$. Hence $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_m}}$. □

Collating Lemmas 4.22 and 4.23 we obtain the following classification:

Theorem 4.24. *Let* $S = \langle x | x^r = x^{r+1} \rangle$, $\sum_{i=1}^{m} a_i, \sum_{j=1}^{k} b_j < r - 2$. *Then* $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} = \overline{x^{b_1}} \cdot \overline{x^{b_2}} \cdot \ldots \cdot \overline{x^{b_k}}$ *if and only if, for* $k = m$*, there exists* f *such that* $E(m,i) = 0$ *for* $i < f$ *and* $x^{e_{a,f}}\gamma_f = x^{e_{b,f}}\gamma_f = x^r$*, and, for* $k \neq m$*,* $\sum_{i=1}^{m} a_i = \sum_{j=1}^{k} b_j$ *and* $x^{e_{a,2}}\gamma_2 = x^{e_{b,2}}\gamma_2 = x^r$*.*

Similarly to Theorem 4.19 we seek to place upper and lower bounds on $|\Sigma(\mathcal{C}(S))|$ now that we have determined all the elements by Theorem 4.24

Theorem 4.25. *Let* $S = \langle x | x^r = x^{r+1} \rangle$*. Then* $r - 1 \leq |\Sigma(\mathcal{C}(S))| \leq 2^{r-3} + 1$*.*

Proof. The semigroup $\Sigma(\mathcal{C}(S))$ must at least contain $\{\overline{x}, \overline{x^2}, \ldots, \overline{x^{r-1}}\}$ and so $r - 1 \leq |\Sigma(\mathcal{C}(S))|$.

A word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \in \Sigma(\mathcal{C}(S))$ which is not equal to either $\overline{x^{r-2}}$ or $\overline{x^{r-1}}$ must satisfy $\sum_{i=1}^{m} a_i < r-2$ by Lemmas 4.20 and 4.21. Therefore we consider all ordered integer partitions of $1, 2, \ldots, r-3$. There are $2^{r-3} - 1$ such partitions. $\square$

4.3 Examples

We conclude this chapter by illustrating Theorems 4.17 and 4.24 with some examples.

Example 4.26. Let $S = \langle x | x^5 = x^9 \rangle$. Then by Lemma 4.2 we have that, $F_4 = \langle \overline{x^5}, \overline{x^6}, \overline{x^7}, \overline{x^8} \rangle \leq \Sigma(\mathcal{C}(S))$. By Lemma 4.3 a word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_3}} \notin F_4$ if and only if $\sum_{i=1}^{m} a_i < 4$. Hence the words outside of F_4 are: $\overline{x}, \overline{x^2}, \overline{x^3}$, $\overline{x} \cdot \overline{x}, \overline{x} \cdot \overline{x^2}, \overline{x^2} \cdot \overline{x}$ and $\overline{x} \cdot \overline{x} \cdot \overline{x}$. Notice that no pair of these words satisfy all the conditions of Theorem 4.17 and hence they are all distinct. Thus $\Sigma(\mathcal{C}(S)) = \{\overline{x}, \overline{x^2}, \overline{x^3}, \overline{x} \cdot \overline{x}, \overline{x} \cdot \overline{x^2}, \overline{x^2} \cdot \overline{x}, \overline{x} \cdot \overline{x} \cdot \overline{x}\} \cup F_4$.

By Theorem 4.19, we have $3 \leq |\Sigma(\mathcal{C}(S)) \setminus F_4| \leq 7$ and so the upper bound on $|\Sigma(\mathcal{C}(S)) \setminus F_4|$ is attained.

Example 4.27. Let $S = \langle x | x^{19} = x^{23} \rangle$. Then by Lemma 4.3 a word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}} \notin F_4$ if and only if $\sum_{i=1}^{m} a_i < 18$. Consider the words $\overline{x^{a_1}} \cdot \overline{x^{a_2}} = \overline{x^4} \cdot \overline{x^8}$ and $\overline{x^{b_1}} \cdot \overline{x^{b_2}} = \overline{x^8} \cdot \overline{x^4} \in \Sigma(\mathcal{C}(S)) \setminus F_4$. Clearly the words have the same length and $8 \equiv 4 \mod 4$ so the first two conditions of Theorem

4.17 are satisfied. Notice

$$E(2,1) = 12 - 12 = 0$$

and

$$E(2,2) = 20 - 16 = 4 \equiv 0 \mod 4.$$

Hence the value of f that we seek for condition 3 is $f = 2$. We have

$$x^{e_{a,2}}\gamma_2 = x^{20}\alpha_1^2\alpha_2 = x^{20}x^q$$

and

$$x^{e_{b,2}}\gamma_2 = x^{16}\alpha_1^2\alpha_2 = x^{16}x^q$$

where $x^q = \alpha_1^2\alpha_2$ and hence $q \geq 3$. Thus

$$x^{16}x^q = x^{19}x^{q-3} = x^{23}x^{q-3} = x^{20}x^q$$

and so $x^{e_{a,2}}\gamma_2 = x^{e_{b,2}}\gamma_2 \in C_4$ and condition 4 is satisfied. Hence $\overline{x^4} \cdot \overline{x^8} = \overline{x^8} \cdot \overline{x^4} \in \Sigma(\mathcal{C}(S))$.

Example 4.28. Let $S = \langle x | x^7 = x^8 \rangle$. Then $\Sigma(\mathcal{C}(S))$ is generated by $\{\overline{x}, \overline{x^2}, \overline{x^3}, \overline{x^4}, \overline{x^5}, \overline{x^6}\}$, all of which are distinct elements in $\Sigma(\mathcal{C}(S))$ by Theorem 3.6. A word $\overline{x^{a_1}} \cdot \overline{x^{a_2}} \cdot \ldots \cdot \overline{x^{a_m}}$ of length greater than one must satisfy $\sum_{i=1}^{m} a_i < 5$ by Lemmas 4.20 and 4.21 in order to be distinct from a generator. We split into the cases where $\sum_{i=1}^{m} a_i = 2, 3, 4$.

In the case where $\sum_{i=1}^{m} a_i = 2$ there are two possible words. We act on a sequence α with both of them and compare the outputs:

$$\begin{aligned}\overline{x^2} \cdot \alpha =&(x^2\alpha_1)(x^2\alpha_1\alpha_2)\dots \\ \overline{x} \cdot \overline{x} \cdot \alpha =&(x^2\alpha_1)(x^3\alpha_1^2\alpha_2)\dots.\end{aligned}$$

Since the lengths of these words are different, in order to have equality we would require $x^2\alpha_1\alpha_2 = x^3\alpha_1^2\alpha_2 = x^7$ by Theorem 4.24. However, this does not hold if we choose $\alpha_1 = \alpha_2 = x$ and so we conclude that $\overline{x^2} \neq \overline{x} \cdot \overline{x}$.

In the case where $\sum_{i=1}^{m} a_i = 3$ there are four possible words. Again, we act on a sequence α and compare the outputs:

$$\begin{aligned}\overline{x^3} \cdot \alpha =&(x^3\alpha_1)(x^3\alpha_1\alpha_2)\dots \\ \overline{x} \cdot \overline{x^2} \cdot \alpha =&(x^3\alpha_1)(x^5\alpha_1^2\alpha_2)\dots = (x^3\alpha_1)(x^7)^\omega \\ \overline{x^2} \cdot \overline{x} \cdot \alpha =&(x^3\alpha_1)(x^4\alpha_1^2\alpha_2)\dots = (x^3\alpha_1)(x^7)^\omega \\ \overline{x} \cdot \overline{x} \cdot \overline{x} \cdot \alpha =&(x^3\alpha_1)(x^6\alpha_1^3\alpha_2)\dots = (x^3\alpha_1)(x^7)^\omega\end{aligned}$$

and we conclude by Theorem 4.24 that $\overline{x} \cdot \overline{x^2} = \overline{x^2} \cdot \overline{x} = \overline{x} \cdot \overline{x} \cdot \overline{x}$. Note that we can show $\overline{x^3}$ is distinct from the other words by choosing $\alpha_1 = \alpha_2 = x$.

In the case where $\sum_{i=1}^{m} a_i = 4$ there are eight possible words. Again, we act on a sequence α and compare the outputs:

$$
\begin{aligned}
\overline{x^4} \cdot \alpha &= (x^4\alpha_1)(x^4\alpha_1\alpha_2)\dots \\
\overline{x^2} \cdot \overline{x^2} \cdot \alpha &= (x^4\alpha_1)(x^6\alpha_1^2\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots \\
\overline{x} \cdot \overline{x^3} \cdot \alpha &= (x^4\alpha_1)(x^7\alpha_1^2\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots \\
\overline{x^3} \cdot \overline{x} \cdot \alpha &= (x^4\alpha_1)(x^5\alpha_1^2\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots \\
\overline{x^2} \cdot \overline{x} \cdot \overline{x} \cdot \alpha &= (x^4\alpha_1)(x^7\alpha_1^3\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots \\
\overline{x} \cdot \overline{x^2} \cdot \overline{x} \cdot \alpha &= (x^4\alpha_1)(x^8\alpha_1^3\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots \\
\overline{x} \cdot \overline{x} \cdot \overline{x^2} \cdot \alpha &= (x^4\alpha_1)(x^9\alpha_1^3\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots \\
\overline{x} \cdot \overline{x} \cdot \overline{x} \cdot \overline{x} \cdot \alpha &= (x^4\alpha_1)(x^{10}\alpha_1^4\alpha_2)\dots &= (x^4\alpha_1)(x^7)^\omega\dots
\end{aligned}
$$

and hence by Theorem 4.24, $\overline{x^2} \cdot \overline{x^2} = \overline{x} \cdot \overline{x^3} = \overline{x^3} \cdot \overline{x} = \overline{x^2} \cdot \overline{x} \cdot \overline{x} = \overline{x} \cdot \overline{x^2} \cdot \overline{x} = \overline{x} \cdot \overline{x} \cdot \overline{x^2} = \overline{x} \cdot \overline{x} \cdot \overline{x} \cdot \overline{x}$. Again, we show $\overline{x^4}$ is distinct from the others by choosing $\alpha_1 = \alpha_2 = x$.

Therefore $\Sigma(\mathcal{C}(S)) = \{\overline{x}, \overline{x^2}, \overline{x^3}, \overline{x^4}, \overline{x^5}, \overline{x^6}, \overline{x} \cdot \overline{x}, \overline{x} \cdot \overline{x^2}, \overline{x^2} \cdot \overline{x^2}\}$.

Chapter 5

Self-Automaton Semigroups

With expansion-like constructions, such as the Cayley automaton semigroup construction, it is often natural to consider the objects which are invariant under the construction. In this chapter, we will investigate such semigroups, termed *self-automaton semigroups*. This viewpoint is adopted by Cain in [7, Section 6.4] where he gives as examples of self-automaton semigroups semilattices and $I \times I$ rectangular bands with an identity. This led him to pose the following:

Open Problem 5.1. Classify the finite self-automaton semigroups. The class of such semigroups might consist of precisely those finite bands in which every $\mathcal{D}$-class is square (that is, $I \times I$ for some I) and every topmost $\mathcal{D}$-class is a singleton.

Initially, the need for square $\mathcal{D}$-classes may appear surprising. However, further consideration of the problem suggests that this may have arisen as a consequence of Cain's choice (and also the choice of Maltcev in [25]) to act on sequences from the right with states of the automata, as opposed to the convention adopted by other authors (such as Mintz in [28] and Silva and Steinberg in [32]) of acting from the left. As the left action approach seems more natural to us, we will translate the notion of being self-automaton, as defined by Cain, into this alternative setting.

It should be noted here that the results of acting from the left rather than the right go far beyond a simple anti-isomorphism. By acting on the left, a wider and more interesting class of self-automaton semigroups is obtained than by acting on the right. Indeed, the examples presented by Cain in [7] can be interpreted fully in the framework of left actions.

Section 5.1 will introduce self-automaton semigroups and consider the initial links between these semigroups and their left-regular representations. Motivated by Open Problem 5.1 we consider bands in Section 5.2 where we show that a band is self-automaton if and only if its left-regular representation is faithful. This suggests a rephrasing of Cain's original question in terms of left actions, which may go as follows:

Question 5.2. Does the class of self-automaton semigroups consist precisely of those bands which have a faithful left-regular representation?

The majority of this chapter will be aimed at answering this question. In trying to do so, positive results are proved for the classes of regular semigroups and monoids, but, in general, the question has a negative answer. An example of a non-band self-automaton semigroup is constructed in Section 5.3 but this is not an answer to Open Problem 5.1 due to a lack of self-duality in the semigroup.

In Section 5.4 we present Cain's original notion in terms of left actions and exhibit an example to answer Open Problem 5.1 in the negative. Further properties of self-automaton semigroups are discussed in Section 5.5. Finally, in Section 5.6 we consider the semigroups that arise as a result of constructing automata from left Cayley graphs and describe fully the link between left and right graphs and left and right actions.

The material in Sections 5.1 to 5.5 can be found in [27].

5.1 Definitions

We begin by making the following definition:

Definition 5.3. Let S be a finite semigroup. Then S is *self-automaton* if the map $S \to \Sigma(\mathcal{C}(S))$ which maps $s \mapsto \overline{s}$ is an isomorphism.

Notice that the map $s \mapsto \overline{s}$ is always a surjection onto the set $\{\overline{s} : s \in S\}$ which generates $\Sigma(\mathcal{C}(S))$ and so to prove that it is an isomorphism it will suffice to show that it is a monomorphism. Below we discuss injectivity of the map $s \mapsto \overline{s}$ before returning later to a discussion of when the map is a homomorphism, which requires more careful consideration.

Before continuing, let us consider an example of a self-automaton semigroup.

Example 5.4. Let $L_n = \{x_1, x_2, \ldots, x_n\}$ be a left-zero semigroup (i.e. $x_i x_j = x_i$ for all $i, j \in \{1, \ldots, n\}$). Notice that for $i \neq j$ we have

$$\overline{x_i} \cdot x_i = x_i \neq x_j = \overline{x_j} \cdot x_i$$

and hence $\overline{x_i} \neq \overline{x_j}$ showing that the map $x_i \mapsto \overline{x_i}$ is injective.

For any sequence $\alpha \in L_n^*$ we have $\overline{x_i} \cdot \alpha = (x_i)^k$ where $|\alpha| = k$. Now we have

$$\overline{x_i} \cdot \overline{x_j} \cdot \alpha = \overline{x_i} \cdot (x_j)^k = (x_i)^k = \overline{x_i} \cdot \alpha = \overline{x_i x_j} \cdot \alpha$$

and hence the map $x_i \mapsto \overline{x_i}$ is a homomorphism. Hence we conclude that L_n is self-automaton.

Motivated by Example 5.4 we now move towards establishing when the map $s \mapsto \overline{s}$ is injective in general.

Definition 5.5. Let S be a finite semigroup. For each $a \in S$ define the map $\lambda_a : S \to S$ by $\lambda_a(x) = ax$ where $x \in S$. Then $\lambda_a \in \mathcal{T}_S$ (the full transformation semigroup on S) and so there is a map $\lambda : S \to \mathcal{T}_S$ given by $\lambda(a) = \lambda_a$. The map λ is the *left-regular representation* of S and is said to be *faithful* if λ is injective.

Lemma 5.6. *Let S be a finite semigroup. The map $s \mapsto \overline{s}$ is injective if and only if the left-regular representation of S is faithful.*

Proof. ($\Rightarrow$) Let $x, y \in S$. If $x \neq y$ then $\overline{x} \neq \overline{y}$ and so by Theorem 3.6 there exists $a \in S$ such that $xa \neq ya$. Hence

$$x \neq y \implies \exists a : xa \neq ya \implies \lambda_x \neq \lambda_y \implies \lambda(x) \neq \lambda(y)$$

and the representation is faithful.

($\Leftarrow$) Since λ is injective we have, for $x, y \in S$,

$$x \neq y \implies \lambda(x) \neq \lambda(y) \implies \lambda_x \neq \lambda_y \implies \exists a : xa \neq ya \implies \overline{x} \neq \overline{y}$$

and hence $s \mapsto \overline{s}$ is injective. $\square$

Having established when $s \mapsto \overline{s}$ is injective, it remains to determine when it is a homomorphism.

The original definition of being self-automaton, as stated in [7], is simply that $S \cong \Sigma(\mathcal{C}(S))$. At this point, we may pause to consider why we have chosen to instead define the concept of being self-automaton in terms of a particular isomorphism, rather than a direct analogue of the original definition.

The original definition is somewhat loose. There is no explicit isomorphism to work with, thus making it difficult to determine where to start when attempting to find examples of self-automaton semigroups. We chose to consider the "canonical" map $s \mapsto \overline{s}$ initially as having a concrete map allowed us to find several initial examples.

Currently, no examples of an isomorphism $\phi : S \to \Sigma(\mathcal{C}(S))$ have been found where ϕ is not the map $s \mapsto \overline{s}$ (we do not consider examples such as $s \mapsto \overline{\theta(s)}$ where θ is an automorphism of S to be examples of a different isomorphism). Further inspection of the map $s \mapsto \overline{s}$ reveals the following:

Lemma 5.7. *Let S be a finite semigroup such that $S \cong \Sigma(\mathcal{C}(S))$. If the map $s \mapsto \overline{s}$ is an injection then it is an isomorphism.*

Proof. Since $S \cong \Sigma(\mathcal{C}(S))$ and $s \mapsto \overline{s}$ is injective we have that $\Sigma(\mathcal{C}(S)) = \{\overline{s} : s \in S\}$. Let $s, t \in S$. Then there must exist $u \in S$ such that $\overline{s} \cdot \overline{t} = \overline{u}$. By acting on the sequence consisting of a single symbol $a \in S$ we obtain

$$sta = \overline{s} \cdot \overline{t} \cdot a = \overline{u} \cdot a = ua$$

and by Theorem 3.6 we conclude that $\overline{u} = \overline{st}$. Hence the map $s \mapsto \overline{s}$ is an isomorphism. $\square$

An immediate consequence of Lemma 5.7 is that if an example of a semigroup S satisfying $S \cong \Sigma(\mathcal{C}(S))$ but not via $s \mapsto \overline{s}$ exists then it can not have a faithful left-regular representation. Interestingly, there exist examples of semigroups S without faithful left-regular representations satisfying $|S| = |\Sigma(\mathcal{C}(S))|$ but $S \ncong \Sigma(\mathcal{C}(S))$ (such an example is given by the zero-union of a nilpotent monogenic semigroup and a right-zero semigroup of the appropriate size). However, an example where $S \cong \Sigma(\mathcal{C}(S))$ will not be found in this way as if T is a nilpotent semigroup of class n then $\Sigma(\mathcal{C}(T))$ is nilpotent of class $n - 1$ (as per Proposition 3.18).

Given the relative ease with which we can work with Definition 5.3 and the lack of examples of semigroups S satisfying $S \cong \Sigma(\mathcal{C}(S))$ but not via the map $s \mapsto \overline{s}$, it may be the case that the more restricted Definition 5.3 is the correct definition to use, which we record below:

Question 5.8. *Let S be a semigroup such that $S \cong \Sigma(\mathcal{C}(S))$. Then is the map $s \mapsto \overline{s}$ necessarily an isomorphism?*

5.2 Bands

Having already seen Example 5.4, we show now that the class of bands provides a plentiful source of self-automaton semigroups in the left action setting.

Lemma 5.9. *Let B be a finite band. Then the map $b \mapsto \overline{b}$ is a homomorphism.*

Proof. First notice that for any band B and elements $\beta_1, \beta_2, \ldots, \beta_n \in B$ and for $i \leq j \leq n$ we have $\beta_1 \ldots \beta_i \beta_1 \ldots \beta_j = \beta_1 \ldots \beta_j$.

Let $\alpha = \alpha_1 \alpha_2 \ldots \alpha_n \in B^*$. Let $s, t \in B$. We have that

$$\begin{aligned}
\overline{s} \cdot \overline{t} \cdot \alpha &= \overline{s} \cdot (t\alpha_1)(t\alpha_1\alpha_2) \ldots (t\alpha_1\alpha_2 \ldots \alpha_n) \\
&= (st\alpha_1)(st\alpha_1 t\alpha_1\alpha_2) \ldots (st\alpha_1 t\alpha_1\alpha_2 \ldots t\alpha_1 \ldots \alpha_n) \\
&= (st\alpha_1)(st\alpha_1\alpha_2) \ldots (st\alpha_1\alpha_2 \ldots \alpha_n) \\
&= \overline{st} \cdot \alpha.
\end{aligned}$$

Hence $s \mapsto \overline{s}$ is a homomorphism. $\square$

By considering Lemma 5.9 together with Lemma 5.6 we immediately obtain the following:

Theorem 5.10. *A finite band is self-automaton if and only if its left-regular representation is faithful.*

With this result, and considering Question 5.2, we prove the following:

Theorem 5.11. *Let S be a finite semigroup with relative left and right identities (that is, for all $s \in S$ there exist $e, f \in S$ such that $se = fs = s$). Then S is self-automaton if and only if S is a band with a faithful left-regular representation.*

Proof. ($\Rightarrow$) Let $s \in S$ and let $e, f \in S$ be such that $se = fs = s$. Let $\alpha_1, \alpha_2 \in S$. We must have

$$(s\alpha_1)(s\alpha_1 e\alpha_1\alpha_2) = (s\alpha_1)(s\alpha_1 s\alpha_1\alpha_2)$$

since

$$\overline{s} \cdot \overline{e} \cdot \alpha_1\alpha_2 = \overline{se} \cdot \alpha_1\alpha_2 = \overline{s} \cdot \alpha_1\alpha_2 = \overline{fs} \cdot \alpha_1\alpha_2 = \overline{f} \cdot \overline{s} \cdot \alpha_1\alpha_2$$

and hence $s\alpha_1 e\alpha_1\alpha_2 = s\alpha_1 s\alpha_1\alpha_2$ for all $\alpha_1, \alpha_2 \in S$. By taking $\alpha_1 = \alpha_2 = e$ we see that $s^2 = s$ and hence S is a band.

Since S is self-automaton, the map $s \mapsto \overline{s}$ is injective and so by Lemma 5.6 the left-regular representation of S is faithful.

($\Leftarrow$) This follows from Lemmas 5.6 and 5.9. $\square$

We immediately deduce positive answers to Question 5.2 in the following cases:

Theorem 5.12. *A finite monoid is self-automaton if and only if it is a band.*

Theorem 5.13. *A finite regular semigroup is self-automaton if and only if it is a band with a faithful left-regular representation.*

5.3 Non-Band Examples

Theorems 5.12 and 5.13 show that Question 5.2 has a positive answer in the cases of monoids and regular semigroups. However, we go on to show that the answer in general is negative. Question 5.2 will be discussed further in Chapter 8.

First we prove a result (which is a generalisation of Lemma 5.9) that we will use in Example 5.15.

Lemma 5.14. *Let S be a finite semigroup. If S^2 is a band then the map $s \mapsto \overline{s}$ is a homomorphism.*

Proof. First recall that $S^2 = \{xy : x, y \in S\}$.

Let $s, t \in S$ and let $\alpha \in S^*$. Then

$$\begin{aligned}\overline{s} \cdot \overline{t} \cdot \alpha &= (st\alpha_1)(st\alpha_1 t\alpha_1\alpha_2)\ldots(st\alpha_1 t\alpha_1\alpha_2\ldots t\alpha_1\ldots\alpha_n) \\ &= (st\alpha_1)(st\alpha_1\alpha_2)\ldots(st\alpha_1\ldots\alpha_n) \text{ as each } t\alpha_1\ldots\alpha_i \text{ is an idempotent} \\ &= \overline{st} \cdot \alpha.\end{aligned}$$

Hence $s \mapsto \overline{s}$ is a homomorphism. □

Example 5.15. Let S be the semigroup defined by the following Cayley Table:

	a	b	c	d
a	b	b	b	c
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

We first verify associativity. A three-element product is determined by the leftmost term unless this is a and the second or third term is d. Suppose that in a three-element product the first term is a and the second is d. Let $x \in \{a, b, c, d\}$. Then $(ad)x = c = a(dx)$. Now suppose that the first term is a and the third is d. Now if $x \in \{a, b, c\}$ then $(ax)d = b = a(xd)$ and if $x = d$ then $(ax)d = c = a(xd)$ and the multiplication is associative.

Clearly the left-regular representation of S is faithful and so by Lemma 5.6 $s \mapsto \overline{s}$ is injective. Observe that $S^2 = \{b, c, d\} \cong L_3$, a three-element left-zero semigroup. Hence by Lemma 5.14 $s \mapsto \overline{s}$ is an isomorphism.

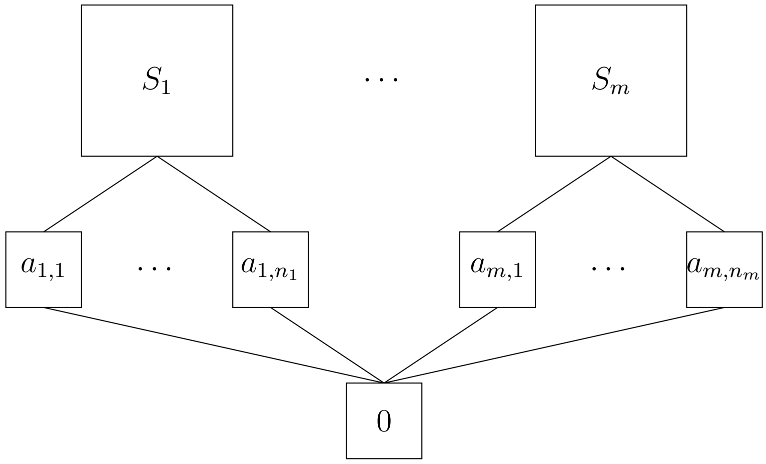
Notice that in Example 5.15, $a^2 \neq a$ and hence S is not a band. This is the first counterexample to Question 5.2.

Next, we exhibit examples of semigroups which satisfy $S = S^2$ and are self-automaton, but which are not bands.

Example 5.16. Let $S_1, \ldots, S_m$ be finite self-automaton semigroups and define $T = S_1 \cup \ldots \cup S_m \cup \{a_{1,1}, \ldots, a_{1,n_1}, a_{2,1}, \ldots a_{2,n_2}, \ldots, a_{m,1}, \ldots, a_{m,n_m}, 0\}$ where the product in T extends the products in each S_i and we set $a_{i,j}s_i = a_{i,j}$ for all $j \in \{1, \ldots, n_i\}$, $s_i \in S_i$ and all other products to 0.

In a product of three terms in T, if all three terms are from the same S_i then associativity of this product is inherited from S_i. For all other possibilities, the only way to obtain a non-zero product of three terms is a product of the form $a_{i,j}s_1s_2$ where $s_1, s_2 \in S_i$. Observe that $(a_{i,j}s_1)s_2 = a_{i,j}s_2 = a_{i,j} = a_{i,j}s_3 = a_{i,j}(s_1s_2)$ (where $s_3 = s_1s_2$). Hence the multiplication in T is associative.

To better illustrate the construction of T, we have the following egg-box diagram:



Let $s_{i_1}, s_{i_2} \in S_i$. Consider the sequence $\alpha = X_1X_2\dots X_kZB_1B_2\dots$ where $X_1,\dots,X_k \in S_i$, $Z \in T \setminus S_i$ and $B_j \in T$. Then

$$\begin{aligned}
\overline{s_{i_1}} \cdot \overline{s_{i_2}} \cdot \alpha &= (\overline{s_{i_1}} \cdot \overline{s_{i_2}} \cdot X_1X_2\dots X_k)0^\omega \\
&= (\overline{s_{i_1}s_{i_2}} \cdot X_1X_2\dots X_k)0^\omega \text{ since } S_i \text{ is self-automaton} \\
&= \overline{s_{i_1}s_{i_2}} \cdot \alpha.
\end{aligned}$$

Notice that by taking the string $X_1X_2\dots X_k$ to be empty we have accounted for acting on any sequence over T which is not a sequence of elements entirely from S_i. If β is a sequence of elements entirely from S_i then it follows from the fact that S_i is self-automaton that $\overline{s_{i_1}} \cdot \overline{s_{i_2}} \cdot \beta = \overline{s_{i_1}s_{i_2}} \cdot \beta$. Hence all the products in each S_i hold in $\Sigma(\mathcal{C}(T))$ and so S_i embeds in $\Sigma(\mathcal{C}(T))$.

We also have that

$$\begin{aligned}\overline{a_{i,j}} \cdot \overline{s_{i_1}} \cdot \alpha &= \overline{a_{i,j}} \cdot (\overline{s_{i_1}} \cdot X_1 X_2 \ldots X_k) 0^\omega \\ &= (a_{i,j})^k 0^\omega \\ &= \overline{a_{i,j}} \cdot \alpha.\end{aligned}$$

Again, by taking the string $X_1 X_2 \ldots X_k$ to be empty we have accounted for acting on all sequences over T that are not sequences of elements entirely from S_i. If β is a sequence of elements entirely from S_i then $\overline{a_{i,j}} \cdot \overline{s_{i_1}} \cdot \beta = (a_{i,j})^\omega = \overline{a_{i,j}} \cdot \beta$. Hence $\overline{a_{i,j}} \cdot \overline{s_{i_1}} = \overline{a_{i,j}}$ for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n_i\}$ and we conclude that all of these products also hold in $\Sigma(\mathcal{C}(T))$.

Every other product in T is of the form $xy = 0$ and so these products will also hold in $\Sigma(\mathcal{C}(T))$. Hence all products from T hold in $\Sigma(\mathcal{C}(T))$ and so the map $s \mapsto \overline{s}$ is a homomorphism. Using Lemma 5.6, we show below that the map is also injective.

For $s_1, s_2 \in S_i$ with $s_1 \neq s_2$ there exists $a \in S_i$ such that $s_1 a \neq s_2 a$ (since S_i is self-automaton) and hence $\overline{s_1} \neq \overline{s_2}$. For $s_i \in S_i$ and $s_j \in S_j$ ($S_i \neq S_j$) then $s_j s_i = 0 \neq s_i s_i \in S_i$ and hence $\overline{s_i} \neq \overline{s_j}$. If $a_{i,j} \neq a_{k,l}$ then there exists $b \in S$ such that $a_{i,j} b \neq a_{k,l} b$ (we can choose $b \in S_i$). Note also that $s_i s_i \neq a_{k,l} s_i$ for all i, k, l and hence $\overline{s_i} \neq \overline{a_{k,l}}$. Finally observe that for all $x \neq 0$ there exists $y \in S$ such that $xy \neq 0$ and so $\overline{x} \neq \overline{0}$ for all $x \neq 0$.

Hence the map is an isomorphism.

5.4 Comparisons with Cain's Construction

As indicated earlier, we have defined states to act on the left of sequences, in contrast to the approach taken by Cain who views states as acting from the right. The aim of this section is to address the similarities and differences between the two approaches and show how the two are related, before resolving a question stated in the introduction to this chapter.

In line with [7] we make the following definition:

Definition 5.17. Let S be a finite semigroup. Define $\Pi(\mathcal{C}(S))$ to be the semigroup generated by $\{\overline{s} : s \in S\}$ by acting on sequences from the right. That is, for a sequence $\alpha = \alpha_1\alpha_2 \dots \alpha_n$ and states $\overline{s}, \overline{t}$, we have

$$\alpha \cdot \overline{s} = (s\alpha_1)(s\alpha_1\alpha_2) \dots (s\alpha_1\alpha_2 \dots \alpha_n)$$

and

$$\alpha \cdot (\overline{s} \cdot \overline{t}) = (\alpha \cdot \overline{s}) \cdot \overline{t}.$$

Recall that a map ϕ is an *anti-homomorphism* if, for $x, y \in S$ we have $\phi(xy) = \phi(y)\phi(x)$.

Theorem 5.18. *Let S be a finite semigroup and $x_1, \dots, x_n \in S$. The map $\phi : \Sigma(\mathcal{C}(S)) \to \Pi(\mathcal{C}(S))$ which maps $\overline{x_1} \cdot \dots \cdot \overline{x_n} \mapsto \overline{x_n} \cdot \dots \cdot \overline{x_1}$ is an anti-isomorphism.*

Proof. In $\Pi(\mathcal{C}(S))$ we have $\phi(\overline{x_1} \cdot \dots \cdot \overline{x_n}) = \overline{x_n} \cdot \dots \cdot \overline{x_1} = \phi(\overline{x_n}) \cdot \dots \cdot \phi(\overline{x_1})$. Hence

ϕ is an anti-homomorphism. The generating sets $\{\overline{s} : s \in S\}$ for $\Sigma(\mathcal{C}(S))$ and $\Pi(\mathcal{C}(S))$ are in bijection so we conclude that ϕ is an anti-isomorphism. $\square$

By this result, we have that $\Sigma(\mathcal{C}(S))$ and $\Pi(\mathcal{C}(S))$ are dual copies of each other. Hence, to obtain information about $\Pi(\mathcal{C}(S))$ it will suffice to determine $\Sigma(\mathcal{C}(S))$ and then take the dual. Given the way that the action is defined, it is perhaps more natural to work with $\Sigma(\mathcal{C}(S))$ and this is the reason for using left actions rather than right actions.

In Cain's setting of right actions, our main question becomes the following: when is the map $S \to \Pi(\mathcal{C}(S))$ defined by $s \mapsto \overline{s}$ an *anti-isomorphism*? Cain's notion of being self-automaton means that $S \cong \Pi(\mathcal{C}(S))$ and so we make the following definition:

Definition 5.19. A finite semigroup is said to be *C-self-automaton* if and only if $S \cong \Pi(\mathcal{C}(S))$.

In the following theorem, we express being C-self-automaton in terms of our setting.

Recall that a semigroup is said to be *self-dual* if it is anti-isomorphic to itself.

Theorem 5.20. *Let $s \mapsto \overline{s}$ be an anti-isomorphism $S \to \Pi(\mathcal{C}(S))$. Then S is C-self-automaton if and only if S is self-dual and self-automaton.*

Proof. If the map $s \mapsto \overline{s}$ is also an isomorphism $S \to \Pi(\mathcal{C}(S))$ then S is commutative and is hence self-dual. By Theorem 5.18 S is self-automaton.

If $s \mapsto \overline{s}$ is an anti-isomorphism $S \to \Pi(\mathcal{C}(S))$ but not an isomorphism then again by Theorem 5.18 S is self-automaton. Suppose that $\phi : \Pi(\mathcal{C}(S)) \to S$ is an isomorphism. Define the map $\psi : S \to S$ by $\psi(x) = \phi(\overline{x})$ for all $x \in S$. It is clear that ψ is a bijection.

For $x, y \in S$ we have

$$\psi(xy) = \phi(\overline{xy}) = \phi(\overline{y} \cdot \overline{x}) = \phi(\overline{y})\phi(\overline{x}) = \psi(y)\psi(x).$$

Hence ψ is an anti-isomorphism $S \to S$ and S is self-dual.

Conversely, it is clear by Theorem 5.18 that if S is self-automaton and self-dual then $S \cong \Pi(\mathcal{C}(S))$. $\square$

The remainder of this section will address Open Problem 5.1, although in light of Definition 5.3, “self-automaton”should be interpreted as C-self-automaton in Open Problem 5.1.

Lemma 5.21. *Let S be a self-automaton semigroup. If $a, x \in S$ are such that $xa = a$ then $a^2 = a$.*

Proof. Assume that S is self-automaton. Consider $\overline{x} \cdot \overline{x}$ and $\overline{x^2}$ acting on a sequence $\alpha_1\alpha_2$ and equate the second outputs to obtain $x(x\alpha_1)^2\alpha_2 = x^2\alpha_1\alpha_2$. Setting $\alpha_1 = a$ gives $a^2\alpha_2 = a\alpha_2$ for all $\alpha_2 \in S$ and we conclude by Theorem 3.6 that $a^2 = a$. $\square$

We immediately deduce the following as a corollary of Lemma 5.21.

Lemma 5.22. *Let S be a self-automaton semigroup and $a \in S$ be such that $a^2 \neq a$. Then the $\mathcal{L}$-class of a is trivial.*

Proof. We know from Lemma 5.21 that if S is self-automaton and $a^2 \neq a$ then there does not exist $x \in S$ such that $xa = a$. Now suppose that $a\mathcal{L}y$ for some $y \in S$. So there exist $u, v \in S^1$ such that $ua = y$ and $vy = a$. This gives us $vua = a$ which is a contradiction unless $vu = 1$. If $v \neq 1$ and $u \neq 1$ then $vu \neq 1$ as $1 \notin S$. If $v = 1$ and $u \neq 1$ then we have $ua = a$ which is a contradiction (similarly, if $v \neq 1$ and $u = 1$ we obtain $va = a$). Therefore we must have $v = u = 1$ and hence $a = y$ and L_a is trivial. □

Lemma 5.23. *Let S be a self-dual, self-automaton semigroup and let $a, x \in S$. If $ax = a$ then a is an idempotent.*

Proof. Let $\phi : S \to S$ be an anti-isomorphism. Then we have that $\phi(x)\phi(a) = \phi(a)$ and by Lemma 5.21 $\phi(a)$ is an idempotent. Hence a is also an idempotent. □

This means that in self-dual self-automaton semigroups, no non-idempotent elements can be stabilised by multiplication on either side.

Lemma 5.24. *Let S be a self-dual, self-automaton semigroup and let $z = xy$ where either x or y is a regular element of S. Then $z^2 = z$.*

Proof. If x is regular then write $x = qx$ for some $q \in S$. Then

$$z = xy = qxy = qz$$

and by Lemma 5.21 $z^2 = z$.

If y is regular then write $y = yp$ for some $p \in S$. Then

$$z = xy = xyp = zp$$

and by Lemma 5.23 $z^2 = z$. $\square$

Theorem 5.25. *Let S be a self-automaton and self-dual semigroup. If $S^2 = S$ then S is a band.*

Proof. Let $a \in S$ and suppose that $a^2 \neq a$. Then by Theorem 5.13 we know a is not a regular element. We can choose a such that a is in a maximal $\mathcal{D}$-class with respect to the non-regular elements of S. Write $a = bc$ for some $b, c \in S$. By Lemma 5.24 neither b nor c can be regular elements of S.

Since S is self-dual, by Lemma 5.22 $D_a = \{a\}$. If $b = a$ or $c = a$ then we have either $a = ac$ or $a = ba$ which would be a contradiction by Lemma 5.21 or Lemma 5.23. Hence $b \neq a$ and $c \neq a$.

This gives us at least 2 non-regular elements in S. Since $a = bc$ we have $D_b > D_a$ which is a contradiction as D_a was assumed to be maximal with respect to the non-regular elements of S. Hence $a^2 = a$ and S is a band. $\square$

So we have established that in the case when $S^2 = S$ and $s \mapsto \overline{s}$ is an anti-isomorphism it is necessary for S to be a band in order to have $S \cong \Pi(\mathcal{C}(S))$. Combining this with Theorem 5.20 we obtain the following:

Corollary 5.26. *The only semigroups satisfying $S^2 = S$ and $S \cong \Pi(\mathcal{C}(S))$ (where $s \mapsto \overline{s}$ is an anti-isomorphism) are the self-dual bands with faithful left-regular representations.*

If, however, we could find an example of a self-dual semigroup satisfying $S \neq S^2$ and fulfilling the conditions of Lemmas 5.6 and 5.14, we would have a counterexample to Open Problem 5.1. After a discussion of these conditions with Benjamin Steinberg, he suggested the following [33]:

Example 5.27. Let $X = \{1, 2, 3, 4, 5\}$ and $X' = \{1', 2', 3', 4', 5'\}$. Let $a, b : X \to X$ be the functions given by

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 3 & 4 & 5 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 4 & 4 & 5 \end{pmatrix}.$$

Let $T = \langle a, b \rangle$ where a, b act on the *right* of X. We have that

$$a \neq a^2 = a^3$$
$$b^2 = b$$

and

$$ba = b.$$

This gives $T = \{a, a^2, b, ab, a^2b\}$.

Note $T \neq T^2 = \{a^2, b, ab, a^2b\}$ which is a band.

Now let $a', b' : X' \to X'$ be given by

$$a' = \begin{pmatrix} 1' & 2' & 3' & 4' & 5' \\ 2' & 3' & 3' & 4' & 5' \end{pmatrix}, \quad b' = \begin{pmatrix} 1' & 2' & 3' & 4' & 5' \\ 4' & 5' & 4' & 4' & 5' \end{pmatrix}.$$

Let $T' = \langle a', b' \rangle$ where a', b' act on the *left* of X'. We have that

$$a' \neq (a')^2 = (a')^3$$
$$(b')^2 = b'$$

and

$$a'b' = b'.$$

This gives $T' = \{a', (a')^2, b', b'a', b'(a')^2\}$.

Note $T' \neq (T')^2 = \{(a')^2, b', b'a', b'(a')^2\}$ which is a band.

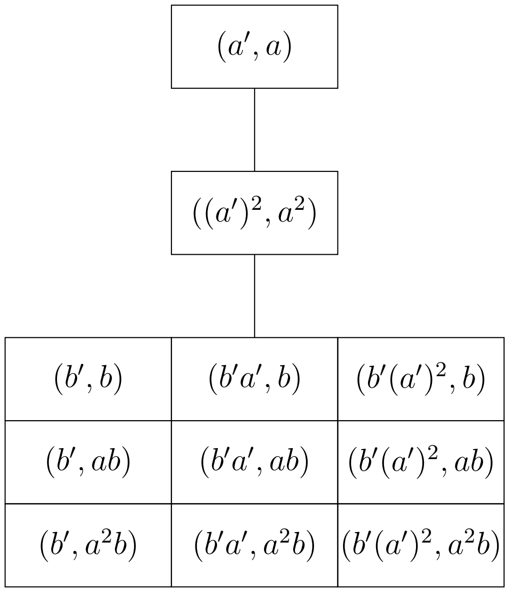
Note that T and T' are dual to each other.

Now let $\widehat{T} = \langle (a', a), (b', b) \rangle \leq T' \times T$. It is easily shown that $|\widehat{T}| = 11$ and that

$$\widehat{T} = \{(a', a), (b', b), ((a')^2, a^2), (b', ab), (b'a', b), (b', a^2b), (b'a', ab),$$
$$(b'(a')^2, b), (b'a', a^2b), (b'(a')^2, ab), (b'(a')^2, a^2b)\}.$$

Observe that $(\widehat{T})^2 = \widehat{T} \setminus \{(a', a)\}$ and $(\widehat{T})^2$ is a band.

The egg-box diagram of $\widehat{T}$ is:



Observe that $\widehat{T}$ is self-dual under that map that fixes $(a', a), ((a')^2, a^2)$, and the diagonal of the bottom $\mathcal{D}$-class, and flips all other elements over the main diagonal.

The left-regular representation of $\widehat{T}$ is not faithful - notice that $\overline{(b'a', t)} = \overline{(b'(a')^2, t)}$ for $t \in \{b, ab, a^2b\}$.

To remedy this, let $R = X' \times X$, a 5×5 rectangular band. Let $S = \widehat{T} \cup R$ with multiplication defined by retaining products from $\widehat{T}$ and R and setting

$$(u, v)(i, j) = (u(i), j)$$

and

$$(i, j)(u, v) = (i, jv)$$

for $u \in T', v \in T, i \in X', j \in X$. Note that $(u(i), j)$ and (i, jv) are elements of R.

It is easily checked that this multiplication is associative.

Observe that R is the minimal ideal of S and note that $S^2 \neq S$, S^2 is a band and S is self-dual. It remains to verify that S has a faithful left-regular representation.

Observe:

$$(b'a', b)(1, 2) = (5, 2) \neq (4, 2) = (b'(a')^2)(1, 2)$$

and hence $\overline{(b'a', b)} \neq \overline{(b'(a')^2, b)}$.

Similarly, $\overline{(b'a', ab)} \neq \overline{(b'(a')^2, ab)}$ and $\overline{(b'a', a^2b)} \neq \overline{(b'(a')^2, a^2b)}$.

If $i \neq k$ then (i, j) and (k, l) do not act the same on the left of R so $\overline{(i, j)} \neq \overline{(k, l)}$.

If $\{j, k\} \neq \{2, 3\}$ then $(i, j)(a', a) = (i, ja) \neq (i, ka) = (i, k)(a', a)$ and so $\overline{(i, j)} \neq \overline{(i, k)}$.

Also, $(i, 2)(b', b) = (i, 5) \neq (i, 4) = (i, 3)(b', b)$.

Hence the left-regular representation of S is faithful. Observe that $|S| = 36$.

We have shown that S satisfies the following:

1. $S \neq S^2$ and hence S is not a band,

2. S^2 is a band and so by Lemma 5.14 $s \mapsto \overline{s}$ is a homomorphism,

3. S has a faithful left-regular representation,

4. S is self-dual.

Conditions 2 and 3 show us that S is self-automaton. Condition 4 shows that, by Theorem 5.18, $S \cong \Pi(\mathcal{C}(S))$. Since S is not a band, this is clearly a counterexample to Open Problem 5.1.

5.5 Other Properties of Self-Automaton Semigroups

We now establish some properties of self-automaton semigroups in general.

Lemma 5.28. *Let S be a finite semigroup such that $s \mapsto \overline{s}$ is a homomorphism. Let $f : S \to T$ be an epimorphism of semigroups. Then the map $t \mapsto \bar{t}$ is also a homomorphism $T \to \Sigma(\mathcal{C}(T))$.*

Proof. As the map $s \mapsto \overline{s}$ is a homomorphism, notice that, for $x, y \in S$ and $\alpha = \alpha_1\alpha_2 \dots \alpha_n \in S^*$ we have $\overline{x} \cdot \overline{y} \cdot \alpha = \overline{xy} \cdot \alpha$ and hence

$$(xy\alpha_1) \dots (xy\alpha_1 y\alpha_1\alpha_2 \dots y\alpha_1\alpha_2 \dots \alpha_n) = (xy\alpha_1) \dots (xy\alpha_1\alpha_2 \dots \alpha_n)$$

Hence $xy\alpha_1 y\alpha_1\alpha_2 \dots y\alpha_1\alpha_2 \dots \alpha_n = xy\alpha_1\alpha_2 \dots \alpha_n$ for all n.

Let $\beta = \beta_1\beta_2 \ldots \beta_n \in T^*$ where $\beta_i = f(\alpha_i)$ for some $\alpha_i \in S$. Then, for $x, y \in S$,

$$\begin{aligned}
\overline{f(x)} \cdot \overline{f(y)} \cdot \beta &= (f(x)f(y)\beta_1) \ldots (f(x)f(y)\beta_1 f(y)\beta_1\beta_2 \ldots f(y)\beta_1 \ldots \beta_n) \\
&= (f(xy\alpha_1)) \ldots (f(xy\alpha_1 y\alpha_1\alpha_2 \ldots y\alpha_1 \ldots \alpha_n)) \\
&= (f(xy\alpha_1)) \ldots (f(xy\alpha_1\alpha_2 \ldots \alpha_n)) \\
&= (f(xy)\beta_1) \ldots (f(xy)\beta_1\beta_2 \ldots \beta_n) \\
&= \overline{f(xy)} \cdot \beta \\
&= \overline{f(x)f(y)} \cdot \beta.
\end{aligned}$$

Hence $t \mapsto \bar{t}$ is a homomorphism. □

In particular, if $s \mapsto \overline{s}$ is a homomorphism then it is in fact an epimorphism (since the set $\{\overline{s} : s \in S\}$ generates $\Sigma(\mathcal{C}(S))$) and this property is passed to $\Sigma(\mathcal{C}(S))$. This leads to the following result:

Theorem 5.29. *Let S be such that $s \mapsto \overline{s}$ is a homomorphism. Then $\Sigma(\mathcal{C}(S))$ is isomorphic to the image of the left-regular representation of S.*

Proof. Let $L = \{\lambda_a : x \mapsto ax : a \in S\}$ be the image of the left-regular representation of S and define $\phi : L \to \Sigma(\mathcal{C}(S))$ by $\phi(\lambda_a) = \overline{a}$. It is clear that ϕ is a surjective map. To establish injectivity we have

$$\phi(\lambda_a) = \phi(\lambda_b) \implies \overline{a} = \overline{b} \implies ax = bx \text{ for all } x \in S \implies \lambda_a = \lambda_b$$

and hence ϕ is injective. Therefore ϕ is a bijection.

We also have $\phi(\lambda_a)\phi(\lambda_b) = \overline{a} \cdot \overline{b} = \overline{ab} = \phi(\lambda_{ab}) = \phi(\lambda_a\lambda_b)$ and hence ϕ is a homomorphism and $L \cong \Sigma(\mathcal{C}(S))$. $\square$

In the case when S is a band, we can go a little further than Theorem 5.29.

Theorem 5.30. *Let S be a band. Then $\Sigma(\mathcal{C}(S))$ is self-automaton.*

Proof. It suffices to show that $\Sigma(\mathcal{C}(S))$ has a faithful left-regular representation, since by Lemma 5.28 we know that the map $\overline{s} \mapsto \overline{(\overline{s})}$ is a homomorphism for all $\overline{s} \in \Sigma(\mathcal{C}(S))$.

Let $a, b \in S$ be such that $\overline{a} \neq \overline{b}$. Then by Lemma 5.6 there exists $x \in S$ such that $ax \neq bx$. It now follows by using Lemma 5.9 that

$$axx \neq bxx \implies \overline{ax} \neq \overline{bx} \implies \overline{a} \cdot \overline{x} \neq \overline{b} \cdot \overline{x}$$

and hence the left-regular representation is faithful. $\square$

However, it is not possible to replace the hypothesis that S is a band with the assumption that the map $s \mapsto \overline{s}$ is a homomorphism in Theorem 5.30, as we now show by means of an example:

Example 5.31. Let S be the semigroup defined by the following Cayley Table:

	a	b	c	d
a	a	b	c	a
b	a	b	c	a
c	a	b	c	b
d	a	b	c	a

It was shown in Example 3.25 that the multiplication in S is associative and that $\Sigma(\mathcal{C}(S)) \cong R_2$, a fact which we will re-establish using the theory of this chapter.

Observe that $S^2 = \{a, b, c\} \cong R_3$, a three-element right-zero semigroup and so by Lemma 5.14 the map $s \mapsto \overline{s}$ is a homomorphism. Note also that $\overline{a} = \overline{b} = \overline{d}$ by Theorem 3.6.

It now follows that $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{y}$ where $x, y \in \{a, c\}$ and hence $\Sigma(\mathcal{C}(S)) \cong R_2$ which does not have a faithful left-regular representation so is not self-automaton. In fact, $\Sigma(\mathcal{C}(R_2)) \cong \{1\}$.

It is also worth noting that self-automaton semigroups are closed under taking direct products.

Theorem 5.32. *S, T are self-automaton semigroups if and only if $S \times T$ is also self-automaton.*

Proof. Recall Proposition 3.24 which states that for finite semigroups S and T, $\Sigma(\mathcal{C}(S \times T)) \leq \Sigma(\mathcal{C}(S)) \times \Sigma(\mathcal{C}(T))$ and $\overline{(s,t)}$ can be written as $(\overline{s}, \overline{t})$ as

$\Sigma(\mathcal{C}(S \times T))$ is isomorphic to the subsemigroup of $\Sigma(\mathcal{C}(S)) \times \Sigma(\mathcal{C}(T))$ where the words in each component have the same length.

($\Rightarrow$) Let S, T be self-automaton semigroups. Define $\phi : S \times T \to \Sigma(\mathcal{C}(S \times T))$ by $\phi((s,t)) = \overline{(s,t)}$. This map is clearly a surjection to the generating set $\{\overline{(s,t)} : s \in S, t \in T\}$. If $\overline{(s,t)} = \overline{(u,v)}$ then by Lemma 5.6

$$
\begin{aligned}
&(s,t)(\alpha,\beta) = (u,v)(\alpha,\beta) \text{ for all } \alpha \in S, \beta \in T \\
&\Rightarrow (s\alpha, t\beta) = (u\alpha, v\beta) \\
&\Rightarrow s\alpha = u\alpha, t\beta = v\beta \\
&\Rightarrow s = u \text{ and } t = v \text{ since } S, T \text{ are self-automaton} \\
&\Rightarrow (s,t) = (u,v)
\end{aligned}
$$

and the map is injective.

We also have that

$$
\begin{aligned}
\overline{(s,t)} \cdot \overline{(u,v)} &= (\overline{s}, \overline{t}) \cdot (\overline{u}, \overline{v}) \\
&= (\overline{s} \cdot \overline{u}, \overline{t} \cdot \overline{v}) \\
&= (\overline{su}, \overline{tv}) \text{ since } S \text{ and } T \text{ are self-automaton} \\
&= \overline{(su, tv)} \\
&= \overline{(s,t)(u,v)}
\end{aligned}
$$

and hence ϕ is an isomorphism.

($\Leftarrow$) Assume that $S \times T$ is self-automaton. Then

$$\overline{(s,t)} \cdot \overline{(u,v)} = \overline{(s,t)(u,v)} = \overline{(su,tv)}.$$

Hence by equating the outputs of $\overline{(s,t)} \cdot \overline{(u,v)} \cdot \gamma$ and $\overline{(su,tv)} \cdot \gamma$ (where $\gamma = (\alpha_1, \beta_1)(\alpha_2, \beta_2)\ldots$ and $\alpha_i \in S, \beta_j \in T$) we obtain

$$su\alpha_1 u\alpha_1\alpha_2 \ldots u\alpha_1 \ldots \alpha_n = su\alpha_1 \ldots \alpha_n$$

and

$$tv\beta_1 v\beta_1\beta_2 \ldots v\beta_1 \ldots \beta_n = tv\beta_1 \ldots \beta_n$$

for all n. This forces $\overline{s} \cdot \overline{u} \cdot \alpha = \overline{su} \cdot \alpha$ and $\overline{t} \cdot \overline{v} \cdot \beta = \overline{tv} \cdot \beta$ (where $\alpha = \alpha_1\alpha_2\ldots$ and $\beta = \beta_1\beta_2\ldots$). Hence the maps $s \mapsto \overline{s}$ and $t \mapsto \overline{t}$ are homomorphisms.

If $s_1 \neq s_2$ then $\overline{(s_1,t)} \neq \overline{(s_2,t)}$ for all $t \in T$. Hence by Lemma 5.6 there exists $(a,b) \in S \times T$ such that

$$(s_1,t)(a,b) \neq (s_2,t)(a,b) \Rightarrow (s_1a, tb) \neq (s_2a, tb) \Rightarrow s_1a \neq s_2a \Rightarrow \overline{s_1} \neq \overline{s_2}$$

and hence $s \mapsto \overline{s}$ is injective. Similarly, $t \mapsto \overline{t}$ is injective.

It now follows that $s \mapsto \overline{s}$ and $t \mapsto \overline{t}$ are isomorphisms. $\square$

5.6 Constructions on the Left Cayley Graph

In Section 5.4 we considered what happened to the Cayley automaton semigroup when we acted from the right with states of the automaton instead of from the left. In this spirit, we now consider what happens to the Cayley automaton semigroup if we had instead constructed the automaton from the left Cayley graph of the semigroup rather than the right Cayley graph. The four possible cases of left and right actions with left and right graphs will be considered and we will see how all four are connected.

In [25, Section 8], Maltcev also considers an alternative construction of an automaton. He defines the “dual Cayley automaton”to be the automaton constructed from the right Cayley graph with a transition function δ defined by $\delta(s,t) = (st, ts)$. We note that this is a different construction from what is defined below.

Let $\mathcal{C}^L(S)$ be the automaton arising from the left Cayley graph of S where we take all of S as the generating set. Therefore $\mathcal{C}^L(S) = (S, S, \delta)$ where $\delta(s,t) = (ts, ts)$. A typical edge in $\mathcal{C}^L(S)$ has the form:

$$s \xrightarrow{t|ts} ts$$

Since we have started with the left Cayley graph, it is perhaps more natural to first consider the case of right actions. The semigroup generated by $\mathcal{C}^L(S)$ using right actions will be denoted by $\Pi(\mathcal{C}^L(S))$.

For the left Cayley graph cases, the analogous result to Theorem 3.6 is that $\overline{x} = \overline{y} \iff ax = ay$ for all $a \in S$. Hence for a sequence $\alpha = \alpha_1\alpha_2 \dots \alpha_n$ we have

$$\alpha \cdot \overline{x} = (\alpha_1 x)(\alpha_2\alpha_1 x) \dots (\alpha_n\alpha_{n-1} \dots \alpha_1 x).$$

Theorem 5.33. $\Pi(\mathcal{C}^L(S)) \cong \Pi(\mathcal{C}(S^{op}))$.

Proof. Recall the definition of $\Pi(\mathcal{C}(S))$ from Definition 5.17. The dual of a semigroup S is denoted by S^{op} and is anti-isomorphic to S.

Define the anti-isomorphism $\phi : S \to S^{op}$ by $\phi(x) = x$ for all $x \in S$.

Define the map $\psi : \Pi(\mathcal{C}^L(S)) \to \Pi(\mathcal{C}(S^{op}))$ by $\psi(\overline{x_1} \cdot \dots \cdot \overline{x_n}) = \overline{x_1} \cdot \dots \cdot \overline{x_n}$.

Note that for all $s, t \in S$ we have

$$\begin{aligned} \overline{s} = \overline{t} \in \Pi(\mathcal{C}^L(S)) &\iff as = at \text{ for all } a \in S \\ &\iff sa = ta \text{ for all } a \in S^{op} \\ &\iff \overline{s} = \overline{t} \in \Pi(\mathcal{C}(S^{op})). \end{aligned}$$

Hence the generating sets $\{\overline{s} : s \in S\}$ for $\Pi(\mathcal{C}^L(S))$ and $\{\overline{s} : s \in S^{op}\}$ for $\Pi(\mathcal{C}(S^{op}))$ are in bijection.

Let $\alpha = \alpha_1\alpha_2 \dots \alpha_n$. In $\Pi(\mathcal{C}^L(S))$ we have

$$\alpha \cdot \overline{x} \cdot \overline{y} = (\alpha_1 xy)(\alpha_2\alpha_1 x\alpha_1 xy) \dots (\alpha_n\alpha_{n-1} \dots \alpha_1 x\alpha_{n-1} \dots \alpha_1 x \dots \alpha_1 xy)$$

and in $\Pi(\mathcal{C}(S^{op}))$ we have

$$\begin{aligned}
\alpha \cdot \overline{x} \cdot \overline{y} =& (yx\alpha_1)(yx\alpha_1 x\alpha_1\alpha_2)\dots(yx\alpha_1 x\alpha_1\alpha_2\dots x\alpha_1\dots\alpha_n) \\
=& (\phi(\alpha_1 xy))(\phi(\alpha_2\alpha_1 x\alpha_1 xy))\dots(\phi(\alpha_n\dots\alpha_1 x\dots\alpha_2\alpha_1 x\dots\alpha_1 xy))
\end{aligned}$$

and hence $\Pi(\mathcal{C}^L(S)) \cong \Pi(\mathcal{C}(S^{op}))$.

Alternatively, we could have noticed that the anti-isomorphism $\phi : S \to S^{op}$ defined by $\phi(s) = s$ induces an isomorphism between the automata $\mathcal{C}^L(S)$ and $\mathcal{C}(S^{op})$.

A typical edge in $\mathcal{C}(S^{op})$ can be written as

$$\phi(s) \xrightarrow{\phi(t)|\phi(ts)} \phi(ts)$$

and since $\phi(s) = s$ this is just the edge from s to ts in $\mathcal{C}^L(S)$. Therefore we are acting from the right with isomorphic automata and hence
$\Pi(\mathcal{C}^L(S)) \cong \Pi(\mathcal{C}(S^{op}))$. $\square$

Had we instead generated a semigroup from $\mathcal{C}^L(S)$ with left actions we would denote this by $\Sigma(\mathcal{C}^L(S))$. Using Theorem 5.18 we obtain

$$\begin{aligned}
\Pi(\mathcal{C}^L(S)) \cong \Pi(\mathcal{C}(S^{op})) \iff& \Pi(\mathcal{C}^L(S))^{op} \cong \Pi(\mathcal{C}(S^{op}))^{op} \\
\iff& \Sigma(\mathcal{C}^L(S)) = \Sigma(\mathcal{C}(S^{op}))
\end{aligned}$$

since $\Sigma(\mathcal{C}^L(S))$ is anti-isomorphic to $\Pi(\mathcal{C}^L(S))$ via the map $\overline{x_1} \cdot \ldots \cdot \overline{x_n} \mapsto \overline{x_n} \cdot \ldots \cdot \overline{x_1}$ as per the case for $\Sigma(\mathcal{C}(S))$ and $\Pi(\mathcal{C}(S))$ in Theorem 5.18. The connection between all four semigroups is summed up in the following diagram:

$$\begin{tikzcd}
 & \text{Left Cayley Graph} & \text{Right Cayley Graph} \\
\text{Left Action} & \Sigma(\mathcal{C}^L(S)) \arrow[r, leftrightarrow, "S \leftrightarrow S^{op}"] \arrow[d, leftrightarrow, "\text{Dual}"'] & \Sigma(\mathcal{C}(S)) \arrow[d, leftrightarrow, "\text{Dual}"] \\
\text{Right Action} & \Pi(\mathcal{C}^L(S)) \arrow[r, leftrightarrow, "S \leftrightarrow S^{op}"'] & \Pi(\mathcal{C}(S))
\end{tikzcd}$$

Chapter 6

Cayley Chains of Finite Semigroups

In Section 5.5 we began to consider iterations of the Cayley automaton construction. We saw in Theorem 5.29 that if a semigroup S is such that $s \mapsto \overline{s}$ is a homomorphism then $\Sigma(\mathcal{C}(S))$ is isomorphic to the left-regular representation of S. Theorem 5.30 showed that in the case of bands, $\Sigma(\mathcal{C}(S))$ is actually self-automaton. However, we saw in Example 5.31 that there exist semigroups satisfying $s \mapsto \overline{s}$ is a homomorphism but $\Sigma(\mathcal{C}(S))$ is not self-automaton. In doing so, we constructed the chain of semigroups

$$S \to \Sigma(\mathcal{C}(S)) = R_2 \to \Sigma(\mathcal{C}(R_2)) = \{1\}.$$

Chains such as this one will be the focus of study in this chapter.

6.1 Definitions and Finite Chains

Definition 6.1. Let $S = S_0$ be a finite semigroup. For $i \geq 1$ define $S_i = \Sigma(\mathcal{C}(S_{i-1}))$. The *Cayley chain* of S is the sequence of semigroups $S_0, S_1, S_2, \ldots$. If there exist minimal n and r (with $n \leq r$) such that $S_n \cong S_{r+1}$ then we will say that the chain has length $r+1$, denoted $\Delta(S) = r+1$.

We shall restrict ourselves to aperiodic semigroups to ensure that S_i is finite for all i (see Theorem 3.5).

Proposition 6.2. *A semigroup S satisfies $S \cong \Sigma(\mathcal{C}(S))$ if and only if $\Delta(S) = 1$.*

Proposition 6.3. *Let S be an n-nilpotent semigroup. Then $\Delta(S) = n$.*

Recall Proposition 3.18 which states that if S is n-nilpotent then $\Sigma(\mathcal{C}(S))$ is $(n-1)$-nilpotent. Hence there exist Cayley chains of any arbitrary finite length.

6.2 Infinite Chains

Maltcev poses the following question:

Question 6.4 ([25, Question 23])**.** *Is it true that for every finite aperiodic semigroup S there exists $n \geq 1$ such that $S_{n-1} = S_n$?*

By means of an example, we show now that this question has a negative answer.

Example 6.5. Let $S = Z_2^1 = S_0$ be a two-element null semigroup with an identity adjoined. Then S has the following Cayley table:

	a	b	c
a	a	a	a
b	a	a	b
c	a	b	c

Note that by Corollary 3.11 the element $\overline{a} \in \Sigma(\mathcal{C}(S))$ is the zero element.

Let $\alpha = \alpha_1\alpha_2 \ldots \in S^\omega$. We will act on α with various words in $\Sigma(\mathcal{C}(S))$ to determine the Cayley table of $\Sigma(\mathcal{C}(S))$. First notice that by Theorem 3.6 the elements $\overline{a}, \overline{b}$ and $\overline{c}$ are all distinct.

We have

$$\begin{aligned}\overline{b} \cdot \alpha =& (b\alpha_1)(b\alpha_1\alpha_2)\ldots \\ \overline{c} \cdot \overline{b} \cdot \alpha =& (b\alpha_1)(b\alpha_1 b\alpha_1\alpha_2)\ldots\end{aligned}$$

and since $(b\alpha_1)^2\alpha_2 = a$ for all $\alpha_1 \in S$, if we choose $\alpha_1 = \alpha_2 = c$ we obtain

$$b\alpha_1 b\alpha_1\alpha_2 = (bc)^2c = a \neq b = bc^2 = b\alpha_1\alpha_2$$

and hence $\overline{c} \cdot \overline{b} \neq \overline{b}$ as the words do not act the same on sequences of the form $cc\alpha_3\alpha_4\ldots$. Note that since $cb = b$ the only possible word of length one that

$\overline{c} \cdot \overline{b}$ could possibly be equal to is $\overline{b}$.

We also have

$$\begin{aligned} \overline{c} \cdot \alpha =& (c\alpha_1)(c\alpha_1\alpha_2)\dots \\ \overline{c} \cdot \overline{c} \cdot \alpha =& (c\alpha_1)(c\alpha_1 c\alpha_1\alpha_2)\dots \end{aligned}$$

and by choosing $\alpha_1 = b$ and $\alpha_2 = c$ we have

$$c\alpha_1 c\alpha_1\alpha_2 = (cb)^2 c = a \neq b = cbc = c\alpha_1\alpha_2$$

and hence $\overline{c} \cdot \overline{c} \neq \overline{c}$.

So far we have shown $S_1 \supseteq \{\overline{a}, \overline{b}, \overline{c}, \overline{c} \cdot \overline{b}, \overline{c} \cdot \overline{c}\}$. We now show that in fact these are all the elements of S_1.

If we have the relation $x_1 x_2 \dots x_m = a \in S$ then we must have $\overline{x_1} \cdot \overline{x_2} \cdot \dots \cdot \overline{x_m} = \overline{a} \in \Sigma(\mathcal{C}(S))$. Hence the only other word of length two to consider is $\overline{b} \cdot \overline{c}$ as all other words of length two are equal to $\overline{a}$.

The only possible equality to check is $\overline{b} \cdot \overline{c} = \overline{b}$. A sequence $\alpha \in S^\omega$ can be written as either $\alpha = (c)^\omega$ or $\alpha = (c)^n X \alpha_{n+2}\alpha_{n+3}\dots$ where $n \geq 0$, $X \in \{a, b\}$ and $\alpha_i \in S$. In the case where $\alpha = (c)^\omega$ we have

$$\overline{b} \cdot \alpha = (b)^\omega = \overline{b} \cdot \overline{c} \cdot \alpha$$

and in the case $\alpha = (c)^n X \alpha_{n+2}\alpha_{n+3}\dots$ we have

$$\overline{b} \cdot \alpha = (b)^n (a)^\omega = \overline{b} \cdot \overline{c} \cdot \alpha$$

and hence $\overline{b} \cdot \overline{c} = \overline{b}$.

Consider also the words $\overline{c} \cdot \overline{c}$ and $\overline{c} \cdot \overline{c} \cdot \overline{c}$. Similarly to above, we can write a sequence α as $\alpha = (c)^\omega$, $\alpha = (c)^n (a)\alpha_{n+2}\alpha_{n+3}\dots$ or $\alpha = (c)^n (b)\alpha_{n+2}\alpha_{n+3}\dots$. We now have the following cases:

for $\alpha = (c)^\omega$ we have

$$\overline{c} \cdot \overline{c} \cdot \alpha = (c)^\omega = \overline{c} \cdot \overline{c} \cdot \overline{c} \cdot \alpha,$$

for $\alpha = (c)^n (a)\alpha_{n+2}\alpha_{n+3}\dots$ we have

$$\overline{c} \cdot \overline{c} \cdot \alpha = (c)^n (a)^\omega = \overline{c} \cdot \overline{c} \cdot \overline{c} \cdot \alpha$$

and finally, for $\alpha = (c)^n (b)\alpha_{n+2}\alpha_{n+3}\dots$ we have

$$\overline{c} \cdot \overline{c} \cdot \alpha = (c)^n (b)(a)^\omega = \overline{c} \cdot \overline{c} \cdot \overline{c} \cdot \alpha$$

and hence $\overline{c} \cdot \overline{c} = \overline{c} \cdot \overline{c} \cdot \overline{c}$.

Finally we consider the words $\overline{c} \cdot \overline{b}$ and $\overline{c} \cdot \overline{c} \cdot \overline{b}$. We now observe that a sequence

α has one of three forms: $\alpha = a\alpha_2\alpha_3\ldots$, $\alpha = b\alpha_2\alpha_3\ldots$ or $\alpha = c\alpha_2\alpha_3\ldots$. We examine each case in turn. Firstly, when $\alpha = a\alpha_2\alpha_3\ldots$ we obtain

$$\overline{c} \cdot \overline{b} \cdot \alpha = (a)^\omega = \overline{c} \cdot \overline{c} \cdot \overline{b} \cdot \alpha.$$

For $\alpha = b\alpha_2\alpha_3\ldots$ we get

$$\overline{c} \cdot \overline{b} \cdot \alpha = (a)^\omega = \overline{c} \cdot \overline{c} \cdot \overline{b} \cdot \alpha$$

and finally, for $\alpha = c\alpha_2\alpha_3\ldots$ we have

$$\overline{c} \cdot \overline{b} \cdot \alpha = (b)(a)^\omega = \overline{c} \cdot \overline{c} \cdot \overline{b} \cdot \alpha$$

so $\overline{c} \cdot \overline{b} = \overline{c} \cdot \overline{c} \cdot \overline{b}$.

We now have enough information to complete the Cayley table for S_1:

	$\overline{a}$	$\overline{b}$	$\overline{c}$	$\overline{c} \cdot \overline{b}$	$\overline{c} \cdot \overline{c}$
$\overline{a}$	$\overline{a}$	$\overline{a}$	$\overline{a}$	$\overline{a}$	$\overline{a}$
$\overline{b}$	$\overline{a}$	$\overline{a}$	$\overline{b}$	$\overline{a}$	$\overline{b}$
$\overline{c}$	$\overline{a}$	$\overline{c} \cdot \overline{b}$	$\overline{c} \cdot \overline{c}$	$\overline{c} \cdot \overline{b}$	$\overline{c} \cdot \overline{c}$
$\overline{c} \cdot \overline{b}$	$\overline{a}$	$\overline{a}$	$\overline{c} \cdot \overline{b}$	$\overline{a}$	$\overline{c} \cdot \overline{b}$
$\overline{c} \cdot \overline{c}$	$\overline{a}$	$\overline{c} \cdot \overline{b}$	$\overline{c} \cdot \overline{c}$	$\overline{c} \cdot \overline{b}$	$\overline{c} \cdot \overline{c}$

and we will relabel the elements of S_1 for the purpose of clarity as follows:

$$\begin{aligned} \overline{a} &\mapsto 0 \\ \overline{b} &\mapsto q \\ \overline{c} &\mapsto r \\ \overline{c} \cdot \overline{b} &\mapsto s \\ \overline{c} \cdot \overline{c} &\mapsto t. \end{aligned}$$

This gives rise to the following modified Cayley table:

	0	q	r	s	t
0	0	0	0	0	0
q	0	0	q	0	q
r	0	s	t	s	t
s	0	0	s	0	s
t	0	s	t	s	t

We now explicitly calculate $S_2 = \Sigma(\mathcal{C}(S_1))$. This is, strictly speaking, unnecessary, as we will see how S_1 forms the basis of an inductive argument for constructing the Cayley chain of S. However, it is included to better illustrate the structure of the semigroups in the Cayley chain.

First notice that $\overline{r} = \overline{t}$ and that $\alpha_i r = \alpha_i t$ and $\alpha_i q = \alpha_i s$ for all $\alpha_i \in S_1$. So we can partition S_1 into three subsets: $\{0\}, \{q, s\}$ and $\{r, t\}$ and the elements in each subset act the same on the right of S_1. Hence we only need to consider actions on sequences over $\{0, q, r\}$.

Consider the words $\overline{q}$ and $\overline{q} \cdot \overline{r}$. Note also that $r^k = t$ for $k \geq 2$. A sequence α over $\{0, q, r\}$ either has the form $\alpha = (r)^n 0 \alpha_{n+2} \alpha_{n+3} \ldots$, $\alpha = (r)^n q \alpha_{n+2} \alpha_{n+3} \ldots$ or $\alpha = (r)^\omega$ where $n \geq 0$. We observe the following: for $\alpha = (r)^n 0 \alpha_{n+2} \alpha_{n+3} \ldots$ and $\alpha = (r)^n q \alpha_{n+2} \alpha_{n+3} \ldots$ we have

$$\overline{q} \cdot \alpha = (q)^n (0)^\omega,$$

and for $\alpha = (r)^\omega$ we have

$$\overline{q} \cdot \alpha = (q)^\omega$$

and hence $\overline{q} = \overline{q} \cdot \overline{r}$.

We have that $\overline{r} \cdot \overline{q} \cdot \alpha = (s\alpha_1)(0)^\omega = \overline{r} \cdot \overline{s} \cdot \alpha = \overline{r} \cdot \overline{r} \cdot \overline{q} \cdot \alpha$ and hence $\overline{r} \cdot \overline{q} = \overline{r} \cdot \overline{s} = \overline{r} \cdot \overline{r} \cdot \overline{q}$.

By choosing $\alpha_1 = q$ we see $\overline{r} \cdot \overline{r} \neq \overline{t}$.

Now consider the words $\overline{s} \cdot \overline{r}$ and $\overline{s}$. If $\alpha = (r)^n 0 \alpha_{n+2} \alpha_{n+3} \ldots$ or $(r)^n q \alpha_{n+2} \alpha_{n+3} \ldots$ then we obtain

$$\overline{s} \cdot \overline{r} \cdot \alpha = (s)^n (0)^\omega.$$

If $\alpha = (r)^\omega$ we get

$$\overline{s} \cdot \overline{r} \cdot \alpha = (s)^\omega$$

and hence $\overline{s} \cdot \overline{r} = \overline{s}$.

Finally, we consider the words $\overline{r} \cdot \overline{r}$ and $\overline{r} \cdot \overline{r} \cdot \overline{r}$. If $\alpha = (r)^n 0 \alpha_{n+2} \alpha_{n+3} \ldots$ we obtain

$$\overline{r} \cdot \overline{r} \cdot \alpha = (t)^n(0)^\omega = \overline{r} \cdot \overline{r} \cdot \overline{r} \cdot \alpha.$$

If $\alpha = (r)^n q \alpha_{n+2}\alpha_{n+3} \ldots$ then we obtain

$$\overline{r} \cdot \overline{r} \cdot \alpha = (t)^n(s)(0)^\omega = \overline{r} \cdot \overline{r} \cdot \overline{r} \cdot \alpha.$$

If $\alpha = (r)^\omega$ we get

$$\overline{r} \cdot \overline{r} \cdot \alpha = (t)^\omega = \overline{r} \cdot \overline{r} \cdot \overline{r} \cdot \alpha.$$

Hence $\overline{r} \cdot \overline{r} = \overline{r} \cdot \overline{r} \cdot \overline{r}$.

We can now complete the Cayley table for S_2:

	$\overline{0}$	$\overline{q}$	$\overline{r}$	$\overline{s}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{r}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{q}$	$\overline{0}$	$\overline{0}$	$\overline{q}$	$\overline{0}$	$\overline{0}$	$\overline{q}$
$\overline{r}$	$\overline{0}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{r}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{r}$
$\overline{s}$	$\overline{0}$	$\overline{0}$	$\overline{s}$	$\overline{0}$	$\overline{0}$	$\overline{s}$
$\overline{r} \cdot \overline{q}$	$\overline{0}$	$\overline{0}$	$\overline{r} \cdot \overline{q}$	$\overline{0}$	$\overline{0}$	$\overline{r} \cdot \overline{q}$
$\overline{r} \cdot \overline{r}$	$\overline{0}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{r}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{q}$	$\overline{r} \cdot \overline{r}$

Let us rename the elements of S_2 as follows:

$$\begin{aligned}
\overline{0} &\mapsto 0\\
\overline{q} &\mapsto y\\
\overline{r} &\mapsto z\\
\overline{s} &\mapsto x_1\\
\overline{r}\cdot\overline{q} &\mapsto zy\\
\overline{r}\cdot\overline{r} &\mapsto z^2.
\end{aligned}$$

We see that S_2 is a member of the family of semigroups with the following general Cayley table:

	0	y	z	x_1	x_2	$\cdots$	x_i	zy	z^2
0	0	0	0	0	0	$\cdots$	0	0	0
y	0	0	y	0	0	$\cdots$	0	0	y
z	0	zy	z^2	zy	zy	$\cdots$	zy	zy	z^2
x_1	0	0	x_1	0	0	$\cdots$	0	0	x_1
x_2	0	0	x_2	0	0	$\cdots$	0	0	x_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
x_i	0	0	x_i	0	0	$\cdots$	0	0	x_i
zy	0	0	zy	0	0	$\cdots$	0	0	zy
z^2	0	zy	z^2	zy	zy	$\cdots$	zy	zy	z^2

If the set of elements $\{x_1, \ldots, x_i\}$ were empty then S_1 would be the first member of this family. We now show, that for $i \geq 0$, $|S_{i+1}| = i + 5$ and that

S_{i+1} is in this family of semigroups.

We proceed by induction on i and note that the calculations above establish the base case $i = 0$. So for an arbitrary i, let S_{i+1} have the required form.

First note that $\overline{z} = \overline{z^2}$ and that we may partition S_{i+1} into three subsets according to elements acting the same on the right of S_{i+1}: $\{0\}$,
$\{y, x_1, \ldots, x_i, zy\}$ and $\{z, z^2\}$. Hence it will suffice to act on sequences α over $\{0, y, z\}$.

By choosing $\alpha_1 = y$ and $\alpha_2 = z$ we obtain

$$\overline{z} \cdot yz = (zy)(zy) \neq (zy)(0) = \overline{z} \cdot \overline{z} \cdot yz$$

and hence $\overline{z} \neq \overline{z} \cdot \overline{z}$.

Similarly, by choosing $\alpha_1 = \alpha_2 = z$ we see

$$\overline{zy} \cdot zz = (zy)(zy) \neq (zy)(0) = \overline{z} \cdot \overline{y} \cdot zz$$

and hence $\overline{zy} \neq \overline{z} \cdot \overline{y}$.

Now observe that an arbitrary infinite sequence α over $\{0, y, z\}$ can be written as $(z)^n 0 \alpha_{n+2} \alpha_{n+3} \ldots$, $(z)^n y \alpha_{n+2} \alpha_{n+3} \ldots$ or $(z)^\omega$ where $n \geq 0$. Now consider the words $\overline{z} \cdot \overline{z}$ and $\overline{z} \cdot \overline{z} \cdot \overline{z}$. For $\alpha = (z)^n 0 \alpha_{n+2} \alpha_{n+3} \ldots$ we obtain

$$\overline{z} \cdot \overline{z} \cdot \alpha = (z^2)^n (0)^\omega = \overline{z} \cdot \overline{z} \cdot \overline{z} \cdot \alpha.$$

If we have $\alpha = (z)^n y \alpha_{n+2} \alpha_{n+3} \dots$ we obtain

$$\overline{z} \cdot \overline{z} \cdot \alpha = (z^2)^n (zy)(0)^\omega = \overline{z} \cdot \overline{z} \cdot \overline{z} \cdot \alpha.$$

Finally, for $\alpha = (z)^\omega$ we obtain

$$\overline{z} \cdot \overline{z} \cdot \alpha = (z^2)^\omega = \overline{z} \cdot \overline{z} \cdot \overline{z} \cdot \alpha$$

and hence $\overline{z} \cdot \overline{z} = \overline{z} \cdot \overline{z} \cdot \overline{z}$.

We have established so far that $S_{i+2} = \Sigma(\mathcal{C}(S_{i+1}))$ contains the elements $\{\overline{0}, \overline{y}, \overline{z}, \overline{x_1} \dots, \overline{x_i}, \overline{zy}, \overline{z} \cdot \overline{y}, \overline{z} \cdot \overline{z}\}$ and aim to show that it contains no more.

In the cases where $\alpha = (z)^n 0 \alpha_{n+2} \alpha_{n+3} \dots$ or $(z)^n y \alpha_{n+2} \alpha_{n+3} \dots$ observe that

$$\overline{x_j} \cdot \overline{z} \cdot \alpha = (x_j)^n (0)^\omega = \overline{x_j} \cdot \alpha$$

and

$$\overline{y} \cdot \overline{z} \cdot \alpha = (y)^n (0)^\omega = \overline{y} \cdot \alpha$$

and

$$\overline{zy} \cdot \overline{z} \cdot \alpha = (zy)^n (0)^\omega = \overline{zy} \cdot \alpha.$$

For the case $\alpha = (z)^\omega$ we obtain

$$\overline{x_j} \cdot \overline{z} \cdot \alpha = (x_j)^\omega = \overline{x_j} \cdot \alpha$$

and

$$\overline{y} \cdot \overline{z} \cdot \alpha = (y)^\omega = \overline{y} \cdot \alpha$$

and

$$\overline{zy} \cdot \overline{z} \cdot \alpha = (zy)^\omega = \overline{zy} \cdot \alpha$$

and hence $\overline{x_j} \cdot \overline{z} = \overline{x_j}$, $\overline{y} \cdot \overline{z} = \overline{y}$ and $\overline{zy} \cdot \overline{z} = \overline{zy}$.

We now consider α in the form $\alpha = y\alpha_2\alpha_3\ldots$. We obtain

$$\overline{z} \cdot \overline{x_j} \cdot \alpha = (0)^\omega = \overline{z} \cdot \overline{z} \cdot \overline{x_j} \cdot \alpha = \overline{z} \cdot \overline{y} \cdot \alpha = \overline{z} \cdot \overline{z} \cdot \overline{y} \cdot \alpha.$$

In the cases where $\alpha = z\alpha_2\alpha_3\ldots$ we obtain

$$\overline{z} \cdot \overline{x_j} \cdot \alpha = (zy)(0)^\omega = \overline{z} \cdot \overline{z} \cdot \overline{x_j} \cdot \alpha = \overline{z} \cdot \overline{y} \cdot \alpha = \overline{z} \cdot \overline{z} \cdot \overline{y} \cdot \alpha$$

and hence

$$\overline{z} \cdot \overline{x_j} = \overline{z} \cdot \overline{z} \cdot \overline{x_j} = \overline{z} \cdot \overline{y} = \overline{z} \cdot \overline{z} \cdot \overline{y}.$$

We can now complete the Cayley table for S_{i+2}:

	$\overline{0}$	$\overline{y}$	$\overline{z}$	$\overline{x_1}$	$\overline{x_2}$	$\cdots$	$\overline{x_i}$	$\overline{zy}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{z}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{y}$	$\overline{0}$	$\overline{0}$	$\overline{y}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{z}$	$\overline{0}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{z}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{y}$	$\cdots$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{z}$
$\overline{x_1}$	$\overline{0}$	$\overline{0}$	$\overline{x_1}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{x_1}$
$\overline{x_2}$	$\overline{0}$	$\overline{0}$	$\overline{x_2}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{x_2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\overline{x_i}$	$\overline{0}$	$\overline{0}$	$\overline{x_i}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{x_i}$
$\overline{zy}$	$\overline{0}$	$\overline{0}$	$\overline{zy}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{zy}$
$\overline{z}\cdot\overline{y}$	$\overline{0}$	$\overline{0}$	$\overline{z}\cdot\overline{y}$	$\overline{0}$	$\overline{0}$	$\cdots$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{z}\cdot\overline{y}$
$\overline{z}\cdot\overline{z}$	$\overline{0}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{z}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{y}$	$\cdots$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{y}$	$\overline{z}\cdot\overline{z}$

This has the required form, perhaps made clearer by renaming the elements as follows: $\overline{0} \mapsto 0, \overline{y} \mapsto Y, \overline{z} \mapsto Z, \overline{x_j} \mapsto X_j$ (for $j \leq i$), $\overline{zy} \mapsto X_{i+1}, \overline{z}\cdot\overline{y} \mapsto ZY$ and $\overline{z}\cdot\overline{z} \mapsto Z^2$. This gives, as a rewritten Cayley table for S_{i+2}:

	0	Y	Z	X_1	X_2	$\cdots$	X_i	X_{i+1}	ZY	Z^2
0	0	0	0	0	0	$\cdots$	0	0	0	0
Y	0	0	Y	0	0	$\cdots$	0	0	0	Y
Z	0	ZY	Z^2	ZY	ZY	$\cdots$	ZY	ZY	ZY	Z^2
X_1	0	0	X_1	0	0	$\cdots$	0	0	0	X_1
X_2	0	0	X_2	0	0	$\cdots$	0	0	0	X_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
X_i	0	0	X_i	0	0	$\cdots$	0	0	0	X_i
X_{i+1}	0	0	X_{i+1}	0	0	$\cdots$	0	0	0	X_{i+1}
ZY	0	0	ZY	0	0	$\cdots$	0	0	0	ZY
Z^2	0	ZY	Z^2	ZY	ZY	$\cdots$	ZY	ZY	ZY	Z^2

Notice also that $|S_{i+2}| = i + 6 = (i + 1) + 5$.

This shows that the Cayley chain of S is infinite.

Consider now the aperiodic semigroups of order less than three (that is, the trivial semigroup, the two-element left- and right-zero semigroups, the two-element null semigroup and the two-element semilattice). These semigroups all satisfy $\Delta(S) \leq 2$ and so by means of the preceding example we note the following:

Remark 6.6. Example 6.5 is a minimal example of an aperiodic semigroup with an infinite Cayley chain.

6.3 Cayley Chains of Subsemigroups

In this section we will consider how the length of the Cayley chain for a semigroup T is related to the length of the chain for a subsemigroup S. We will also consider zero-unions of semigroups and consider how adjoining zeros and identities to a semigroup impacts on the length of the chain.

Proposition 6.7. *Let T_1, T_2 be semigroups and let $S = T_1 \cup_0 T_2$. Then $\Delta(S) = \max(\Delta(T_1), \Delta(T_2))$.*

Proof. This follows from Proposition 3.8 which states that
$\Sigma(\mathcal{C}(T_1 \cup_0 T_2)) = \Sigma(\mathcal{C}(T_1)) \cup_0 \Sigma(\mathcal{C}(T_2))$. □

In particular, $\Delta(S) < \infty$ if and only if $\Delta(T_1) < \infty$ and $\Delta(T_2) < \infty$.

In the cases where $\Delta(T) < \infty$ it is possible for a subsemigroup $S < T$ to have either $\Delta(S) < \Delta(T)$ or $\Delta(S) > \Delta(T)$. Equality is also possible. We illustrate these three possibilities by examples.

Example 6.8. Let T be a semigroup where $\Delta(T) > 1$ (recall that such semigroups exist by Proposition 6.3) and let $S = \{1\}$ be a trivial subsemigroup of T. Then $\Delta(T) > \Delta(S) = 1$.

Example 6.9. Let $T = (R_n \times L_m)^1$ for some $n \geq 2, m \geq 1$ and let $S = R_n$. Then $\Delta(S) = 2 > 1 = \Delta(T)$ (see Example 3.13 and Theorem 5.10).

Example 6.10. Let $T = L_{n+1}$ and $S = L_n$ where $n \geq 1$. Then $\Delta(S) = 1 = \Delta(T)$.

We also show by means of an example that in the cases where $\Delta(T) = \infty$ there can exist non-trivial subsemigroups S such that $\Delta(S) < \infty$.

Example 6.11. Let $T = Z_2^1$ (see Example 6.5) and $S = Z_2$. Then $\Delta(Z_2^1) = \infty > 2 = \Delta(Z_2)$.

We have shown that if T has a finite Cayley chain then the Cayley chain of a subsemigroup S can be longer, shorter or equal in length. We show now that it is not possible for the Cayley chain of S to be infinite.

Theorem 6.12. *Let $S \leq T$ and $\Delta(T) = n$. Then there exists k, r such that $S_k = S_{k+r}$.*

Proof. Recall by Proposition 3.21 that since $S \leq T$ we have that $\Sigma(\mathcal{C}(S))$ divides $\Sigma(\mathcal{C}(T))$ - that is, there exists a semigroup U such that $\Sigma(\mathcal{C}(T)) \geq U \twoheadrightarrow \Sigma(\mathcal{C}(S))$. Also, by Proposition 3.23, if $S \twoheadrightarrow T$ then $\Sigma(\mathcal{C}(S)) \twoheadrightarrow \Sigma(\mathcal{C}(T))$.

Consider the Cayley chains of T and S. We show by induction that S_i divides T_i for all $i \geq 0$. Since $S_0 \leq T_0$ the base case holds so assume that the statement is true for some arbitrary i.

Since S_i divides T_i there exists U_i such that $T_i \geq U_i \twoheadrightarrow S_i$. It now follows that there exists U_{i+1} such that $T_{i+1} \geq U_{i+1} \twoheadrightarrow \Sigma(\mathcal{C}(U_i)) \twoheadrightarrow S_{i+1}$ and hence the statement is true for all i.

Since each T_i $(0 \leq i \leq n-1)$ is finite there can exist only finitely many divisors. Hence there exist k, r such that $S_k = S_{k+r}$. $\square$

In the case where T_n is self-automaton (recall from Definition 5.3 that this means the map $t \mapsto \bar{t}$ is an isomorphism $T_n \to \Sigma(\mathcal{C}(T_n))$) we can improve on Theorem 6.12:

Theorem 6.13. *Let $S \leq T$ and $\Delta(T) = n + 1$. If T_n is self-automaton then there exists k such that $S_k = S_{k+1}$.*

Proof. Since T_n is self-automaton, it has the property that $t \mapsto \bar{t}$ is a homomorphism $T_n \to T_{n+1} = T_n$. Let U be a subsemigroup of T and let $u_1, u_2 \in U$. We have that $\overline{u_1} \cdot \overline{u_2} \cdot \alpha = \overline{u_1 u_2} \cdot \alpha$ for all $\alpha \in T^*$ since T is self-automaton. Since $U^* \subseteq T^*$ it follows that $\overline{u_1} \cdot \overline{u_2} \cdot \alpha = \overline{u_1 u_2} \cdot \alpha$ for all $\alpha \in U^*$ and hence the map $u \mapsto \overline{u}$ is a homomorphism $U \to \Sigma(\mathcal{C}(U))$. We now apply Lemma 5.28 to see that for S, a homomorphic image of U, the map $s \mapsto \overline{s}$ is a homomorphism $S \to \Sigma(\mathcal{C}(S))$.

Hence if S_k is a divisor of T_n then the map $s \mapsto \overline{s}$ is a homomorphism $S_k \to S_{k+1}$ and $|S_k| \geq |S_{k+1}|$. If $|S_k| = |S_{k+1}|$ then the map $s \mapsto \overline{s}$ is in fact an isomorphism as it is an epimorphism between sets of the same size. Hence there exists k such that $S_k = S_{k+1}$. $\square$

Corollary 6.14. *Let $S \leq T$. Then $|S_i| \leq |T_i|$ for all i.*

Proof. By Theorem 6.12 we know that S_i divides T_i and hence there exists U_i such that $T_i \geq U_i \twoheadrightarrow S_i$. Consequently $|T_i| \geq |U_i| \geq |S_i|$. $\square$

We also consider now the adjunction of zeros and identities to a semigroup S.

Proposition 6.15. *Let S be a semigroup and $T = S^0$. Then $T_i = (S_i)^0$.*

Proof. This follows from Proposition 3.7 which states that $\Sigma(\mathcal{C}(S^0)) \cong [\Sigma(\mathcal{C}(S))]^0$. In particular, if $\Delta(S) = n$ then $\Delta(T) = n$. □

Adjoining an identity does not behave in a similarly nice way. In Example 6.11 we saw that $\Delta(Z_2) = 2$ but $\Delta(Z_2^1) = \infty$. The length of a a chain can also stay the same after an identity has been adjoined - for example, $\Delta(L_n) = 1 = \Delta(L_n^1)$ - but it can also be reduced - $\Delta(R_n) = 2 > 1 = \Delta(R_n^1)$.

Throughout this chapter, we have not seen an example of a finite aperiodic semigroup satisfying $S_n = S_{n+r}$ where $r \geq 2$. This leads us to ask the following, which will be discussed further in Chapter 8.

Question 6.16. *Does there exist a finite aperiodic semigroup S with $S_n = S_{n+r}$ where $n \geq 0$ and $r \geq 2$?*

Chapter 7

Cayley Automaton Semigroups of Infinite Semigroups

In this chapter we will move away from finite semigroups and consider the construction of a Cayley automaton semigroup from an infinite semigroup. Rather than building an automaton from a Cayley graph, we will instead think of each element s in the semigroup S as giving rise to a transformation $\overline{s} : S^* \to S^*$ and the Cayley automaton semigroup is simply the subsemigroup of the endomorphism monoid of the $|S|$-ary rooted tree generated by $\{\overline{s} : s \in S\}$, as per Section 3.1.

We will consider the case of cancellative semigroups, where we will reprove and extend Theorem 3.4 regarding the Cayley automaton semigroups of finite groups before going on to make some basic statements about Cayley automaton semigroups of general infinite semigroups. Finally, we will construct the Cayley automaton semigroup arising from the Bicyclic Monoid.

7.1 Cancellative Semigroups

Lemma 7.1. *Let S be a right-cancellative semigroup. Then $\Sigma(\mathcal{C}(S))$ is also right-cancellative.*

Proof. Recall that a semigroup is right-cancellative if $xa = ya \implies x = y$ for all $x, y, a \in S$.

Let $x \neq y$ be elements of S and let $a \in S$ be arbitrary. If $\overline{x} \cdot \overline{a} = \overline{y} \cdot \overline{a}$ then the actions of the words agree on all sequences α. In particular, for the sequence $\alpha = \alpha_1$, where α_1 is arbitrary, we obtain

$$\overline{x} \cdot \overline{a} \cdot \alpha_1 = (xa\alpha_1) = (ya\alpha_1) = \overline{y} \cdot \overline{a} \cdot \alpha_1$$

and hence $xa\alpha_1 = ya\alpha_1$. By the right-cancellativity of S we get $x = y$ and hence $\overline{x} = \overline{y}$. Thus $\Sigma(\mathcal{C}(S))$ is right-cancellative. □

Lemma 7.2. *Let S be a left-cancellative semigroup. Then $\Sigma(\mathcal{C}(S))$ is also left-cancellative.*

Proof. Recall that a semigroup is left-cancellative if $ax = ay \implies x = y$ for all $x, y, a \in S$.

Similarly to the proof of Lemma 7.1, let us assume that, for $x, y, a \in S$ we have $\overline{a} \cdot \overline{x} = \overline{y} \cdot \overline{a}$. By acting on the sequence $\alpha = \alpha_1$ for some $\alpha_1 \in S$ we obtain

$$\overline{a} \cdot \overline{x} \cdot \alpha_1 = (ax\alpha_1) = (ay\alpha_1) = \overline{a} \cdot \overline{y} \cdot \alpha_1$$

and hence $ax\alpha_1 = ay\alpha_1$. By the left-cancellativity of S we have
$x\alpha_1 = y\alpha_1$ and now by Theorem 3.6 we conclude $\overline{x} = \overline{y}$. Hence $\Sigma(\mathcal{C}(S))$ is left-cancellative. □

Combining Lemmas 7.1 and 7.2 we immediately obtain the following:

Theorem 7.3. *Let S be a cancellative semigroup. Then $\Sigma(\mathcal{C}(S))$ is cancellative.*

Recall that a semigroup is cancellative if it is both left- and right-cancellative.

We now show that for a cancellative semigroup S there are no relations between pairs of words of equal length in $\Sigma(\mathcal{C}(S))$.

Lemma 7.4. *Let S be a cancellative semigroup, $k \geq 1$ and $x_i, y_j \in S$ for $i, j \in \{1, 2, \ldots, k\}$. Then $\overline{x_k} \cdot \overline{x_{k-1}} \cdot \ldots \cdot \overline{x_1} = \overline{y_k} \cdot \overline{y_{k-1}} \cdot \ldots \cdot \overline{y_1}$ if and only if $x_i = y_i$ for all $i \in \{1, 2, \ldots, k\}$.*

Proof. Let $\alpha = \alpha_1\alpha_2\ldots$ be a sequence in S^* such that $|\alpha| \geq k$. First considering $\overline{x_k} \cdot \overline{x_{k-1}} \cdot \ldots \cdot \overline{x_1}$, we act on α one generator at a time and consider the outputs. We obtain the following:

$$\begin{aligned}
\overline{x_1}\cdot\alpha &= (x_1\alpha_1)(x_1\alpha_1\alpha_2)\dots &&= (A_{1,1})(A_{1,2})\dots\\
\overline{x_2}\cdot\overline{x_1}\cdot\alpha &= (x_2A_{1,1})(x_2A_{1,1}A_{1,2})\dots &&= (A_{2,1})(A_{2,2})\dots\\
\overline{x_3}\cdot\overline{x_2}\cdot\overline{x_1}\cdot\alpha &= (x_3A_{2,1})(x_3A_{2,1}A_{2,2})\dots &&= (A_{3,1})(A_{3,2})\dots\\
&\vdots &&\vdots\\
\overline{x_k}\cdot\overline{x_{k-1}}\cdot\ldots\cdot\overline{x_1}\cdot\alpha &= (x_kA_{k-1,1})(x_kA_{k-1,1}A_{k-1,2})\dots &&= (A_{k,1})(A_{k,2})\dots
\end{aligned}$$

where $A_{1,j} = x_1\alpha_1\alpha_2\dots\alpha_j$ and $A_{i,j} = x_iA_{i-1,1}A_{i-1,2}\dots A_{i-1,j}$ for $i \geq 2$.

Similarly, considering $\overline{y_k}\cdot\overline{y_{k-1}}\cdot\ldots\cdot\overline{y_1}$ and acting on α one generator at a time, we obtain

$$\begin{aligned}
\overline{y_1}\cdot\alpha &= (y_1\alpha_1)(y_1\alpha_1\alpha_2)\dots &&= (B_{1,1})(B_{1,2})\dots\\
\overline{y_2}\cdot\overline{y_1}\cdot\alpha &= (y_2B_{1,1})(y_2B_{1,1}B_{1,2})\dots &&= (B_{2,1})(B_{2,2})\dots\\
\overline{y_3}\cdot\overline{y_2}\cdot\overline{y_1}\cdot\alpha &= (y_3B_{2,1})(y_3B_{2,1}B_{2,2})\dots &&= (B_{3,1})(B_{3,2})\dots\\
&\vdots &&\vdots\\
\overline{y_k}\cdot\overline{y_{k-1}}\cdot\ldots\cdot\overline{y_1}\cdot\alpha &= (y_kB_{k-1,1})(y_kB_{k-1,1}B_{k-1,2})\dots &&= (B_{k,1})(B_{k,2})\dots
\end{aligned}$$

where $B_{1,j} = y_1\alpha_1\alpha_2\dots\alpha_j$ and $B_{i,j} = y_iB_{i-1,1}B_{i-1,2}\dots B_{i-1,j}$ for $i \geq 2$.

Assume that $\overline{x_k}\cdot\overline{x_{k-1}}\cdot\ldots\cdot\overline{x_1} = \overline{y_k}\cdot\overline{y_{k-1}}\cdot\ldots\cdot\overline{y_1}$. Then

$$A_{k,1} = x_kA_{k-1,1} = y_kB_{k-1,1} = B_{k,1}.$$

Since $A_{k,2} = B_{k,2}$ we obtain

$$x_k A_{k-1,1} A_{k-1,2} = y_k B_{k-1,1} B_{k-1,2}$$

and by the cancellativity of S we conclude that $A_{k-1,2} = B_{k-1,2}$. Similarly, $A_{k,3} = B_{k,3}$ gives $x_k A_{k-1,1} A_{k-1,2} A_{k-1,3} = y_k B_{k-1,1} B_{k-1,2} B_{k-1,3}$ and again by the cancellativity of S we conclude $A_{k-1,3} = B_{k-1,3}$. Continuing in this fashion will yield $A_{k-1,j} = B_{k-1,j}$ for $j \geq 2$.

More generally, if

$$\begin{aligned} x_i A_{i-1,1} A_{i-1,2} \ldots A_{i-1,j} &= A_{i,j} \\ &= B_{i,j} \\ &= y_i B_{i-1,1} B_{i-1,2} \ldots B_{i-1,j} \end{aligned}$$

and

$$\begin{aligned} x_i A_{i-1,1} A_{i-1,2} \ldots A_{i-1,j} A_{i-1,j+1} &= A_{i,j+1} \\ &= B_{i,j+1} \\ &= y_i B_{i-1,1} B_{i-1,2} \ldots B_{i-1,j} B_{i-1,j+1} \end{aligned}$$

then by the cancellativity of S we obtain $A_{i-1,j+1} = B_{i-1,j+1}$. Thus once we know $A_{i,j} = B_{i,j}$ it follows that $A_{i-1,v} = B_{i-1,v}$ for $v \geq j+1$.

This will yield $x_1\alpha_1\alpha_2\ldots\alpha_k = A_{1,k} = B_{1,k} = y_1\alpha_1\alpha_2\ldots\alpha_k$ and hence $x_1 = y_1$ by the cancellativity of S and $A_{1,j} = B_{1,j}$ for all j.

Since we also have $x_2A_{1,1}A_{1,2}\ldots A_{1,k} = A_{2,k} = B_{2,k} = y_2B_{1,1}B_{1,2}\ldots B_{1,k}$ we see that $x_2 = y_2$ by the cancellativity of S. Indeed, since $A_{i,k} = B_{i,k}$ for all $i \in \{1,\ldots,k\}$, continuing in this way gives $x_i = y_i$ for all i.

The converse of the statement is clear. $\square$

Having considered relations between pairs of words of equal length, we look now at relations between pairs of words of different lengths. We do this by means of a more general lemma:

Lemma 7.5 ([32, Lemma 2.7])**.** *Let X be an alphabet with at least 2 elements and suppose that $\equiv$ is a congruence on X^* such that, for $u, v \in X^*$ we have*

$$u \equiv v, |u| = |v| \implies u = v.$$

Then $\equiv$ is the trivial congruence.

Proof. Let $u \equiv v$ and assume without loss of generality that $|u| < |v|$. Let $a \neq b \in X$. Then we have that $uav \equiv vau$ and $ubv \equiv vbu$. These all have equal length, and it follows from our hypothesis that $uav = vau$. However, since $|u| < |v|$ we have that ua is a prefix of v. Similarly, since $ubv = vbu$, we have that ub is a prefix of v. This contradicts $a \neq b$. $\square$

Note also that Lemma 7.5 can be found in [15, Proposition 3.1.12].

Since every semigroup is a quotient of a free semigroup on some set X by some congruence (see [21, Section 1.6] for details), Lemma 7.5 shows that if there are no relations between words of equal length then there are in fact no relations between any pairs of words. So to show that $\Sigma(\mathcal{C}(S))$ is free for a semigroup S (where $|S| > 1$), it suffices to show that $\overline{x_1} \cdot \ldots \cdot \overline{x_n} = \overline{y_1} \cdot \ldots \cdot \overline{y_n} \implies x_i = y_i$ for all i.

By combining Lemmas 7.4 and 7.5 we have shown the following:

Theorem 7.6. *Let S be a non-trivial cancellative semigroup. Then $\Sigma(\mathcal{C}(S))$ is free of rank equal to the cardinality of S.*

In Chapter 4 we considered the Cayley automaton semigroups arising from finite monogenic semigroups. The case of the infinite monogenic semigroup was deferred to this chapter. Since the infinite monogenic semigroup $\mathbb{N}$ is cancellative, we obtain the following:

Corollary 7.7. $\Sigma(\mathcal{C}(\mathbb{N}))$ *is free of countable rank.*

Since every group is a cancellative semigroup (indeed, the classes of finite cancellative semigroups and finite groups coincide), and at no point did the proofs of Lemmas 7.4 and 7.5 actually depend on the semigroup being infinite, we have reproved Theorem 3.4 and extended it to the case of infinite groups. We now state the extended version for completeness:

Theorem 7.8. *Let G be a non-trivial group (either finite or infinite). Then $\Sigma(\mathcal{C}(G))$ is free of rank equal to the cardinality of G.*

7.2 General Infinite Semigroups

We now look at infinite semigroups in general, considering the connection between the semigroup S and a particular quotient. We will also see some properties of Cayley automaton semigroups arising from monoids before constructing some examples.

Let S be an infinite semigroup. Define a relation $\sim$ on S by $x \sim y$ if and only if $xa = ya$ for all $a \in S$. By Theorem 3.6 we have that $x \sim y$ if and only if $\overline{x} = \overline{y} \in \Sigma(\mathcal{C}(S))$.

Lemma 7.9. *The relation $\sim$ is a congruence on S.*

Proof. Clearly $\overline{x} = \overline{x}$ for all $x \in S$ and so $\sim$ is a reflexive relation. We have $\overline{x} = \overline{y} \implies \overline{y} = \overline{x}$ and hence $\sim$ is symmetric. Finally, if $\overline{x} = \overline{y}$ and $\overline{y} = \overline{z}$ then $\overline{x} = \overline{z}$ and $\sim$ is transitive. Thus $\sim$ is an equivalence relation on S.

Now suppose that $x \sim y$ and let $t \in S$ be arbitrary. Since $xa = ya$ for all $a \in S$ it follows that $x(ta) = y(ta)$ for all $a \in S$ and so $(xt)a = (yt)a$. Hence $xt \sim yt$. We also have $txa = tya$ for all $a \in S$ and so $tx \sim ty$. Hence $\sim$ is a congruence on S. $\square$

Under the congruence $\sim$, the congruence class of $x \in S$ is

$$[x] = \{y \in S : xa = ya \ \forall a \in S\} = \{y \in S : \overline{x} = \overline{y} \in \Sigma(\mathcal{C}(S))\}.$$

For infinite semigroups S, we will use the congruence $\sim$ to explore finite generation of $\Sigma(\mathcal{C}(S))$.

Lemma 7.10. *If $S/\sim$ is finite then $\Sigma(\mathcal{C}(S))$ is finitely generated.*

Proof. Suppose that there are n equivalence classes and suppose that a set of representatives for these classes is $\{x_{i_1}, x_{i_2}, \ldots, x_{i_n}\}$. Let $y \in S$ be arbitrary. Then $[y] = [x_{i_k}]$ for some $k \in \{1, \ldots, n\}$ and so $\overline{y} = \overline{x_{i_k}}$. Hence $\Sigma(\mathcal{C}(S))$ is finitely generated by $\{\overline{x_{i_1}}, \overline{x_{i_2}}, \ldots, \overline{x_{i_n}}\}$. $\square$

If, in addition, we know that each $\overline{x}$ is an indecomposable element in $\Sigma(\mathcal{C}(S))$ then the converse to Lemma 7.10 also holds.

Recall that an element $x \in S$ is indecomposable if $x \in S \setminus S^2$.

Lemma 7.11. *Let S be a semigroup such that each $\overline{x}$ is an indecomposable element in $\Sigma(\mathcal{C}(S))$. If $\Sigma(\mathcal{C}(S))$ is finitely generated then $S/\sim$ is finite.*

Proof. We always have that $\Sigma(\mathcal{C}(S)) \setminus (\Sigma(\mathcal{C}(S)))^2 \subseteq \{\overline{x} : x \in S\}$. However, since we are assuming that each $\overline{x}$ is indecomposable
(so $\overline{x} \in \Sigma(\mathcal{C}(S)) \setminus (\Sigma(\mathcal{C}(S)))^2$) we must have

$$\Sigma(\mathcal{C}(S)) \setminus (\Sigma(\mathcal{C}(S))^2) = \{\overline{x} : x \in S\}.$$

Suppose that $\Sigma(\mathcal{C}(S))$ is finitely generated by $\{\overline{x_{i_1}}, \overline{x_{i_2}}, \ldots, \overline{x_{i_n}}\}$. Then for all $y \in S$, $\overline{y} = \overline{x_{i_k}}$ for some k. Hence $[y] = [x_{i_k}]$ and so $S/\sim$ is finite. $\square$

It is not always the case that $\Sigma(\mathcal{C}(S)) \setminus (\Sigma(\mathcal{C}(S))^2) = \{\overline{x} : x \in S\}$, as we show now by means of an example:

Example 7.12. Consider the semigroup defined by the following Cayley table:

	0	x	y	t_1	t_2	$\dots$
0	0	0	0	0	0	$\dots$
x	0	x	0	0	0	$\dots$
y	0	0	y	0	0	$\dots$
t_1	0	0	0	0	0	$\dots$
t_2	0	0	0	0	0	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Since $\overline{t_i} = \overline{0}$ for all i we have that $\Sigma(\mathcal{C}(S)) = \langle \overline{x}, \overline{y}, \overline{0} \rangle$. However, $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x} = \overline{0}$ so in fact $\Sigma(\mathcal{C}(S)) = \langle \overline{x}, \overline{y} \rangle$ and $\overline{0}$ is decomposable. Hence $\Sigma(\mathcal{C}(S)) \setminus (\Sigma(\mathcal{C}(S))^2) \neq \{\overline{x} : x \in S\}$.

Lemma 7.13. *If $S/\!\sim$ is uncountable then $\Sigma(\mathcal{C}(S))$ is not finitely generated.*

Proof. Suppose that $S/\!\sim = \{[x_i]\}_{i \in I}$ is uncountable. Then $\Sigma(\mathcal{C}(S)) = \langle \{\overline{x_i} : x_i \in S\} \rangle$ where $\overline{x_j} \neq \overline{x_k}$ for $j \neq k$. Now assume that $\Sigma(\mathcal{C}(S))$ is finitely generated. Then $\Sigma(\mathcal{C}(S))$ is countable which is a contradiction as $\Sigma(\mathcal{C}(S))$ contains an uncountable generating set. Hence $\Sigma(\mathcal{C}(S))$ is not finitely generated. $\square$

Lemma 7.14. *If $\Sigma(\mathcal{C}(S))$ is finitely generated then $S/\!\sim$ is also finitely generated.*

Proof. Suppose that $\Sigma(\mathcal{C}(S)) = \langle \overline{x_1}, \dots, \overline{x_m} \rangle$ where $\overline{x_i} \neq \overline{x_j}$ and $|S/{\sim}| = \infty$ (otherwise there is nothing to prove). We have $[x_i] \neq [x_j]$ for $i \neq j$ and $\{[x_1] \dots, [x_m]\} \subseteq S/{\sim}$. For an arbitrary $y \in S$ we have

$$\begin{aligned}
&\overline{y} = \overline{x_{i_1}} \cdot \overline{x_{i_2}} \dots \cdot \overline{x_{i_k}} \\
&\Longrightarrow y\alpha_1 = x_{i_1} x_{i_2} \dots x_{i_k} \alpha_1 \text{ for all } \alpha_1 \in S \\
&\Longrightarrow [y] = [x_{i_1} x_{i_2} \dots x_{i_k}] \\
&\Longrightarrow [y] = [x_{i_1}][x_{i_2}] \dots [x_{i_k}]
\end{aligned}$$

and hence $S/{\sim} = \langle [x_1], \dots, [x_m] \rangle$. $\square$

Lemma 7.15. *Let $S = \{x_i\}_{i \in I}$. If $\Sigma(\mathcal{C}(S))$ is finitely generated then there exists a finite subset of $\{\overline{x_i} : x_i \in S\}$ that is a generating set for $\Sigma(\mathcal{C}(S))$.*

Proof. Let $A = \{\overline{x_{i_1}}, \dots, \overline{x_{i_k}}\}$ and suppose that $\Sigma(\mathcal{C}(S))$ is generated by $A \cup \{\overline{y_1} \cdot \overline{y_2} \cdot \dots \cdot \overline{y_m}\}$ where $\overline{y_j} \in \{\overline{x_i} : x_i \in S\}$. Then $\Sigma(\mathcal{C}(S))$ is generated by $A \cup \{\overline{y_1}, \overline{y_2}, \dots, \overline{y_m}\}$ which is a finite subset of $\{\overline{x_i} : x_i \in S\}$. $\square$

In some cases we have $\Sigma(\mathcal{C}(S)) \cong \Sigma(\mathcal{C}(S/{\sim}))$ whilst $S \ncong S/{\sim}$, which we show now by means of an example.

Example 7.16. Let $S = G \times Z$ be the direct product of an infinite group $G = \{g_1, g_2, \dots\}$ and an infinite null semigroup $Z = \{0, z_1, z_2, \dots\}$. Then by Theorem 3.6 we have $\overline{(g_i, z_j)} = \overline{(g_i, z_k)} = \overline{(g_i, 0)}$ for all i, j, k and so $\Sigma(\mathcal{C}(S)) = \langle \overline{(g_1, 0)}, \overline{(g_2, 0)}, \overline{(g_3, 0)}, \dots \rangle \cong F$, a free semigroup of rank equal to the cardinality of G since $\{(g_1, 0), (g_2, 0), (g_3, 0) \ldots\} \cong G$.

Again by Theorem 3.6 we have $S/\!\sim\, = \{[(g_1, 0)], [(g_2, 0)], [(g_3, 0)] \ldots\} \cong G$. Hence $\Sigma(\mathcal{C}(S/\!\sim)) \cong F$.

We can also have $\Sigma(\mathcal{C}(S)) \ncong \Sigma(\mathcal{C}(S/\!\sim))$ when $S \ncong S/\!\sim$.

Example 7.17. Let S be the semigroup defined by the following Cayley table:

	1	2	3	4	5	6	0	x_1	x_2	x_3	
1	0	0	0	0	0	0	0	0	0	0	$\ldots$
2	0	3	0	5	0	0	0	0	0	0	$\ldots$
3	0	0	0	0	0	0	0	0	0	0	$\ldots$
4	0	3	0	0	0	1	0	0	0	0	$\ldots$
5	0	0	0	0	0	0	0	0	0	0	$\ldots$
6	0	5	0	3	0	0	0	0	0	0	$\ldots$
0	0	0	0	0	0	0	0	0	0	0	$\ldots$
x_1	0	0	0	0	0	0	0	0	0	0	$\ldots$
x_2	0	0	0	0	0	0	0	0	0	0	$\ldots$
x_3	0	0	0	0	0	0	0	0	0	0	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Note that S is 3-nilpotent (and hence is associative) and so
$\Sigma(\mathcal{C}(S)) = \langle \overline{0}, \overline{2}, \overline{4}, \overline{6} \rangle$ is 2-nilpotent by Proposition 3.18.

Now consider $S/\!\sim\, = \{[0], [2], [4], [6]\}$. Then $S/\!\sim$ is 2-nilpotent and so

$\Sigma(\mathcal{C}(S/{\sim})) \cong \{1\}$. Hence $\Sigma(\mathcal{C}(S)) \ncong \Sigma(\mathcal{C}(S/{\sim}))$.

Lemma 7.18. *Let $x \in S$ be an element of infinite order (so $\langle x \rangle \cong \mathbb{N}$). Then $\overline{x}$ has infinite order in $\Sigma(\mathcal{C}(S))$.*

Proof. Assume that $\overline{x}$ has finite order. Then there exist positive integers n, k such that $\underbrace{\overline{x} \cdot \ldots \cdot \overline{x}}_{n \text{ times}} = \underbrace{\overline{x} \cdot \ldots \cdot \overline{x}}_{k \text{ times}}$. Acting with both of these words on the sequence x gives $x^{n+1} = x^{k+1}$ which is a contradiction as x has infinite order. Hence $\overline{x}$ has infinite order. □

We turn now to look at the specific cases of monoids. For a monoid M denote the group of units of M (that is, all elements $x \in M$ such that there exists $y \in M$ and $xy = yx = 1$) by $U(M)$. If $U(M)$ is non-trivial then by Theorem 7.8 and Proposition 3.22 $\Sigma(\mathcal{C}(M))$ contains a free subsemigroup of rank equal to the cardinality of $U(M)$.

An infinite monoid M either contains a copy of the Bicyclic Monoid B or $M \backslash U(M)$ is an ideal (see [23, Theorem 6.6.7, Corollary 6.6.5] and [9, Lemma 1.31]). We will consider this latter case first before returning to the Bicyclic Monoid.

Lemma 7.19. *Let M be an infinite monoid and $X \subseteq M$. If $\Sigma(\mathcal{C}(M))$ is generated by $\{\overline{x} : x \in X\}$ then M is generated by X. In particular, if $\Sigma(\mathcal{C}(M))$ is finitely generated then so is M.*

Proof. Suppose that $\Sigma(\mathcal{C}(M)) = \langle \overline{x} : x \in X \rangle$ and let $y \in M$ be arbitrary. Then we may write $\overline{y} = \overline{x_{i_1}} \cdot \overline{x_{i_2}} \cdot \ldots \cdot \overline{x_{i_k}}$ where $x_{i_j} \in X$. By acting on the sequence 1 with both words we obtain $y = x_{i_1}x_{i_2}\dots x_{i_k}$ and hence M is generated by X. $\square$

Notice also that the finite generation case is a consequence of Lemma 7.14 since the congruence $\sim$ defined above is trivial on monoids.

The converse to Lemma 7.19 is false. Consider the free monoid of rank one $\mathbb{N}\cup\{0\}$. This is cancellative and so by Theorem 7.6, $\Sigma(\mathcal{C}(\mathbb{N}\cup\{0\}))$ is free of countable rank.

Lemma 7.20. *Let M be an infinite monoid and $U(M)$ its non-trivial group of units. Suppose that $M\setminus U(M)$ is an ideal. Then for $x_i \in U(M)$, the word $\overline{x_1}\cdot\overline{x_2}\cdot\ldots\cdot\overline{x_n}$ is uniquely represented in $\Sigma(\mathcal{C}(M))$.*

Proof. Since $U(M)$ is a subgroup of M we have $F_{|U(M)|} \leq \Sigma(\mathcal{C}(M))$ (where $F_{|U(M)|}$ denotes the free semigroup of rank equal to the cardinality of $U(M)$). Elements of $F_{|U(M)|}$ have unique representatives as products of elements of $\{\overline{u} : u \in U(M)\}$ so assume that

$$\overline{x_1}\cdot\overline{x_2}\cdot\ldots\cdot\overline{x_n} = \overline{m_1}\cdot\overline{m_2}\cdot\ldots\cdot\overline{m_k}$$

where $x_i \in U(M)$ and $m_j \in M$ with at least one $m_j \in M\setminus U(M)$.

Since $M\setminus U(M)$ is an ideal of M, act on the sequence $\alpha = 1$ of length one with both words to obtain

$$U(M) \ni x_1x_2\ldots x_n = m_1m_2\ldots m_k \in M\setminus U(M)$$

which is a contradiction. Hence $\overline{x_1} \cdot \overline{x_2} \cdot \ldots \cdot \overline{x_n}$ is uniquely represented in $\Sigma(\mathcal{C}(M))$. $\square$

Corollary 7.21. *Let M be an infinite monoid and $U(M)$ its group of units where $M \setminus U(M)$ is an ideal. Suppose that $U(M)$ is infinite. Then $\Sigma(\mathcal{C}(M))$ is not finitely generated.*

Proof. By Lemma 7.20 all words $\overline{x}$ of length 1 where $x \in U(M)$ are indecomposable in $\Sigma(\mathcal{C}(M))$. Since there are infinitely many indecomposable elements, these must be present in any generating set for $\Sigma(\mathcal{C}(M))$. $\square$

Lemma 7.22. *Let M be a monoid containing some non-idempotent element. Then $\overline{1}$ is not the identity in $\Sigma(\mathcal{C}(M))$.*

Proof. Let $a \in M$ be such that $a^2 \neq a$. Acting with $\overline{a}$ on the sequence $(1)(1)$ gives $\overline{a} \cdot (1)(1) = (a)(a)$ whilst acting with $\overline{1} \cdot \overline{a}$ gives $\overline{1} \cdot \overline{a} \cdot (1)(1) = (a)(a^2)$. Hence $\overline{1}$ is not a left-identity so is consequently not an identity. $\square$

Lemma 7.23. *Let $\Sigma(\mathcal{C}(M))$ contain an element that can not be written as words of two different lengths. Then $\Sigma(\mathcal{C}(M))$ is not a monoid.*

Proof. Let $\overline{x_1} \cdot \ldots \cdot \overline{x_n}$ be a word in $\Sigma(\mathcal{C}(M))$ that is not equal to a word of any other length. Assume that $\overline{y_1} \cdot \ldots \cdot \overline{y_k}$ is the identity in $\Sigma(\mathcal{C}(M))$. Then we have $\overline{x_1} \cdot \ldots \cdot \overline{x_n} \cdot \overline{y_1} \cdot \ldots \cdot \overline{y_k} = \overline{x_1} \cdot \ldots \cdot \overline{x_n}$ which is a contradiction. Hence there is no identity. $\square$

Notice that the the proofs of Lemmas 7.23 and 7.22 did not use the fact that

M was infinite. Hence these results also apply to finite monoids. In fact, Lemma 7.22 also applies to finite semigroups that are not monoids.

7.3 Bicyclic Monoid

We now consider the Cayley automaton semigroup arising from the bicyclic monoid. This is the next natural example of an infinite semigroup to consider, having already determined the Cayley automaton semigroups arising from infinite groups and cancellative semigroups in Theorems 7.6 and 7.8.

Definition 7.24. The *bicyclic monoid* is the monoid with presentation

$$B = \langle b, c | bc = 1 \rangle.$$

Elements in B have a unique normal form of $c^i b^j$ for some $i, j \geq 0$. Alternatively, we can think of B as $(\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$ with the operation

$$(a, b)(c, d) = (a - b + \max(b, c), d - c + \max(b, c))$$

with generators $(1, 0)$ and $(0, 1)$ and identity $(0, 0)$. The two descriptions of B are related by $c^i b^j \leftrightarrow (i, j)$.

First notice that by Theorem 3.6 we have $\overline{x} \neq \overline{y} \in \Sigma(\mathcal{C}(B))$ for all $x \neq y \in B$.

Lemma 7.25. $\Sigma(\mathcal{C}(B))$ *is not finitely generated.*

Proof. Suppose for a contradiction that $\Sigma(\mathcal{C}(B))$ is finitely generated. Then since $\Sigma(\mathcal{C}(B))$ is generated by $\{\overline{b} : b \in B\}$ there must exist some $\overline{y}$ (where $y \in B$) that is non-trivially decomposable. Suppose that $\overline{y} = \overline{x_1} \cdot \overline{x_2} \ldots \overline{x_k}$ where $x_i \in B$ and $k \geq 2$. Let $\alpha_1, \alpha_2 \in B$. By acting on the sequence $\alpha_1\alpha_2$ we obtain

$$\begin{aligned}
(y\alpha_1)(y\alpha_1\alpha_2) &= \overline{y} \cdot \alpha_1\alpha_2 \\
&= \overline{x_1} \cdot \overline{x_2} \cdot \ldots \cdot \overline{x_k} \cdot \alpha_1\alpha_2 \\
&= (x_1x_2 \ldots x_k\alpha_1)((x_1x_2 \ldots x_k)\alpha_1(x_2 \ldots x_k)\alpha_1 \ldots (x_k)\alpha_1\alpha_2)
\end{aligned}$$

By equating the first outputs and choosing $\alpha_1 = 1$ we see $y = x_1x_2 \ldots x_k$.

Now consider the second outputs. Write $y\alpha_1 = (i, j)$,
$(x_1x_2 \ldots x_k)\alpha_1(x_2 \ldots x_k)\alpha_1 \ldots (x_k)\alpha_1 = (m, n)$ and $\alpha_2 = (p, q)$
where $i, j, m, n, p, q \geq 0$. Equality of the second outputs forces

$$\begin{aligned}
(i, j)(p, q) =& (i - j + \max(j, p), q - p + \max(j, p)) \\
=& (i - j - n + m + \max((n - m + \max(j, m)), p), \\
& \quad q - p + \max((n - m + \max(j, m), p))) \\
=& (i, j)(m, n)(p, q).
\end{aligned}$$

Equating the first components gives

$$\max(j,p) = m - n + \max((n - m + \max(j,m)), p).$$

We now show that we can choose α_1 such that $m - n \neq 0$.

Consider $(x_1x_2\ldots x_k)\alpha_1(x_2\ldots x_k)\alpha_1\ldots(x_{k-1}x_k)\alpha_1(x_k)\alpha_1$. Let $x_dx_{d+1}\ldots x_k = (m_d,n_d)$. Let $\alpha_1 = (r,0)$ where $r > \max(n_1,n_2,\ldots,n_k)$. Then

$$(m_d,n_d)(r,0) = (m_d - n_d + r, 0)$$

and

$$(m_d - n_d + r, 0)(m_{d+1} - n_{d+1} + r, 0) = ([m_d - n_d] + [m_{d+1} - n_{d+1}] + 2r, 0).$$

Hence

$$\begin{aligned}(m,n) &= (m_1,n_1)(r,0)(m_2,n_2)(r,0)\ldots(m_k,n_k)(r,0)\\ &= ([m_1 - n_1] + [m_2 - n_2] + \ldots + [m_k - n_k] + kr, 0).\end{aligned}$$

Notice that

$$\begin{aligned}&[m_1 - n_1] + [m_2 - n_2] + \ldots + [m_k - n_k] + kr\\ &\qquad = [m_1 - n_1 + r] + [m_2 - n_2 + r] + \ldots + [m_k - n_k + r] > 0\end{aligned}$$

as $r-n_i > 0$ for all i as r was chosen to be such that $r > \max(n_1, n_2, \ldots, n_k)$. Hence $m - n \neq 0$.

Now choose $p > \max(j, \max(n-m+\max(j,m)))$. This gives $p = m - n + p$ which is a contradiction as $m - n \neq 0$. Hence all words of length one in $\Sigma(\mathcal{C}(B))$ are indecomposable and so must be present in any generating set. Thus $\Sigma(\mathcal{C}(B))$ is not finitely generated. $\square$

We go on now to show that there are no relations between words of different lengths in $\Sigma(\mathcal{C}(B))$.

Lemma 7.26. *Let $x_i, y_j, a, b \geq 0$ and $n \geq 1$. Then*

$$\overline{(x_n, y_n)} \cdot \ldots \cdot \overline{(x_1, y_1)} \cdot (a, b) = (x_n - y_n + \max(A_{n,1}, A_{n,2}), b - a + [y_1 - x_1] + \\ \ldots + [y_{n-1} + x_{n-1}] + \max(A_{n,1}, A_{n,2}))$$

where $A_{1,n}, A_{2,n}$ are terms involving $x_1, \ldots, x_n, y_1, \ldots, y_n, a, b$.

Proof. We prove this by induction. By direct calculations, we obtain

$$\overline{(x_1, y_1)} \cdot (a, b) = (x_1 - y_1 + \max(A_{1,1}, A_{1,2}), b - a + \max(A_{1,1}, A_{1,2}))$$

and

$$\overline{(x_2, y_2)} \cdot \overline{(x_1, y_1)} \cdot (a, b) \\ = (x_2 - y_2 + \max(A_{2,1}, A_{2,2}), b - a + [y_1 - x_1] + \max(A_{2,1}, A_{2,2}))$$

and so the claim holds for $n = 1$ and 2.

Now assume that the claim is true for an arbitrary k. That is,

$$\overline{(x_k, y_k)} \cdot \ldots \cdot \overline{(x_1, y_1)} \cdot (a, b) = (x_k - y_k + \max(A_{k,1}, A_{k,2}), b - a + [y_1 - x_1] + \\ \ldots + [y_{k-1} + x_{k-1}] + \max(A_{k,1}, A_{k,2})).$$

Now consider $\overline{(x_{k+1}, y_{k+1})} \cdot \overline{(x_k, y_k)} \cdot \ldots \cdot \overline{(x_1, y_1)} \cdot (a, b)$. By the inductive hypothesis, we obtain

$$\begin{aligned}
&(x_{k+1}, y_{k+1})(x_k - y_k + \max(A_{k,1}, A_{k,2}), b - a + [y_1 - x_1] + \\
&\qquad\qquad \ldots + [y_{k-1} + x_{k-1}] + \max(A_{k,1}, A_{k,2})) \\
&= (x_{k+1} - y_{k+1} + \max(A_{k+1,1}, A_{k+1,2}), \\
&\quad b - a + [y_1 - x_1] + \ldots + [y_{k-1} - x_{k-1}] + \max(A_{k,1}, A_{k,2}) - (x_k - y_k) \\
&\qquad\qquad - \max(A_{k,1}, A_{k,2}) + \max(A_{k+1,1}, A_{k+1,2})) \\
&= (x_{k+1} - y_{k+1} + \max(A_{k+1,1}, A_{k+1,2}), b - a + [y_1 - x_1] + \\
&\qquad\qquad \ldots + [y_k - x_k] + \max(A_{k+1,1}, A_{k+1,2}))
\end{aligned}$$

and hence the claim is true for all n. □

We will now act on the sequence $(a, b)(c, d)$ and consider the form of the second letter in the output. The form of the first letter is known by Lemma 7.26.

Lemma 7.27. *Let $x_i, y_j, a, b, c, d \geq 0$ and $n \geq 1$. Then the second letter in* *the output of*

$$\overline{(x_n, y_n)} \cdot \ldots \cdot \overline{(x_1, y_1)} \cdot (a, b)(c, d)$$

has the form

$$\begin{aligned}([x_n - y_n] + \ldots + [x_1 - y_1] + a - b + \max(B_{n,1}, B_{n,2}),\\ d - c + (n-1)[y_1 - x_1] + (n-2)[y_2 - x_2] + \ldots + 2[y_{n-2} - x_{n-2}] +\\ [y_{n-1} - x_{n-1}] + (n-1)(b - a) + \max(B_{n,1}, B_{n,2}))\end{aligned}$$

where $B_{1,n}, B_{2,n}$ *are terms involving* $x_1, \ldots, x_n, y_1, \ldots, y_n, a, b, c, d$.

Proof. By direct calculations in the cases $n = 1$ and 2 we see

$$\begin{aligned}&\overline{(x_1, y_1)} \cdot (a, b)(c, d) =\\ &\quad (x_1 - y_1 + \max(A_{1,1}, A_{1,2}), b - a + \max(A_{1,1}, A_{1,2}))\\ &\quad ([x_1 - y_1] + a - b + \max(B_{1,1}, B_{1,2}), d - c + \max(B_{1,1}, B_{1,2}))\end{aligned}$$

and

$$\begin{aligned}&\overline{(x_2, y_2)} \cdot \overline{(x_1, y_1)} \cdot (a, b)(c, d) =\\ &\quad (x_2 - y_2 + \max(A_{2,1}, A_{2,2}), b - a + y_1 - x_1 + \max(A_{2,1}, A_{2,2}))\\ &\quad (([x_2 - y_2] + [x_1 - y_1] + (a - b) + \max(B_{2,1}, B_{2,2}),\\ &\quad d - c + [y_1 - x_1] + (b - a) + \max(B_{2,1}, B_{2,2}))\end{aligned}$$

and so the claim holds in these cases.

Now assume that the claim is true for an arbitrary k. That is, the second letter in the output of $\overline{(x_k, y_k)} \cdot \ldots \cdot \overline{(x_1, y_1)} \cdot (a, b)(c, d)$ is

$$\begin{aligned}&([x_k - y_k] + \ldots + [x_1 - y_1] + a - b + \max(B_{k,1}, B_{k,2}),\\ &\quad d - c + (k-1)[y_1 - x_1] + (k-2)[y_2 - x_2] + \ldots + 2[y_{k-2} - x_{k-2}] +\\ &\qquad\qquad [y_{k-1} - x_{k-1}] + (k-1)(b-a) + \max(B_{k,1}, B_{k,2})).\end{aligned}$$

By the inductive hypothesis and Lemma 7.26 we obtain as the second letter in the output of $\overline{(x_{k+1}, y_{k+1})} \cdot \ldots \cdot \overline{(x_1, y_1)} \cdot (a, b)(c, d)$

$$\begin{aligned}&(x_{k+1} - y_{k+1} + \max(A_{k+1,1}, A_{k+1,2}),\\ &b - a + [y_1 - x_1] + \ldots + [y_k - x_k] + \max(A_{k+1,1}, A_{k+1,2}))\\ &([x_k - y_k] + \ldots + [x_1 - y_1] + a - b + \max(B_{k,1}, B_{k,2}),\\ &d - c + (k-1)[y_1 - x_1] + (k-2)[y_2 - x_2] +\\ &\ldots + 2[y_{k-2} - x_{k-2}] + [y_{k-1} - x_{k-1}] + (k-1)(b-a) + \max(B_{k,1}, B_{k,2}))\\ &= ([x_{k+1} - y_{k+1}] + \ldots + [x_1 - y_1] + a - b + \max(B_{k+1,1}, B_{k+1,2}),\\ &d - c + k[y_1 - x_1] + (k-1)[y_2 - x_2] + \ldots + 2[y_{k-1} - x_{k-1}] + [y_k - x_k] +\\ &k(b-a) + \max(B_{k+1,1}, B_{k+1,2}))\end{aligned}$$

and so the claim is true for all n. □

Lemma 7.28. *Let* $x_i, y_i, p_i, q_i \geq 0$. *If* $n \neq k$ *then* $\overline{(x_n, y_n)} \cdot \ldots \cdot \overline{(x_1, y_1)} \neq \overline{(p_k, q_k)} \cdot \ldots \cdot \overline{(p_1, q_1)}$.

Proof. Suppose that $\overline{(x_n, y_n)} \cdot \ldots \cdot \overline{(x_1, y_1)} = \overline{(p_k, q_k)} \cdot \ldots \cdot \overline{(p_1, q_1)}$ where $n \neq k$.

Act on a sequence $(a, b)(c, d)$ with both words and equate the second letters of outputs. By Lemma 7.27 we obtain

$$[x_n - y_n] + \ldots + [x_1 - y_1] + a - b + \max(B_{n,1}, B_{n,2}) =$$
$$[p_k - q_k] + \ldots + [p_1 - q_1] + a - b + \max(C_{n,1}, C_{n,2})$$

where $C_{n,1}, C_{n,2}$ are terms involving $p_1, \ldots, p_k, q_1, \ldots, q_k, a, b, c, d$, and

$$d - c + (n-1)[y_1 - x_1] + \ldots + 2[y_{n-2} - x_{n-2}] + [y_{n-1} - x_{n-1}] +$$
$$(n-1)(b-a) + \max(B_{n,1}, B_{n,2})$$
$$= d - c + (k-1)(q_1 - p_1) + \ldots + 2[q_{k-2} - p_{k-2}] + [q_{k-1} - p_{k-1}] +$$
$$(k-1)(b-a) + \max(C_{n,1}, C_{n,2}).$$

Solving these equations simultaneously gives

$$[x_n - y_n] + 2[x_{n-1} - y_{n-1}] + \ldots + n[x_1 - y_1] =$$
$$[p_k - q_k] + 2[p_{k-1} - q_{k-1}] + \ldots + k[p_1 - q_1] + (n-k)(b-a).$$

All values of x_i, y_i, p_i and q_i are fixed and we have a free choice for a and b. Since $n - k \neq 0$ we can obtain a contradiction in the above equality by an appropriate choice of a and b.

Hence $\overline{(x_n, y_n)} \cdot \ldots \cdot \overline{(x_1, y_1)} \neq \overline{(p_k, q_k)} \cdot \ldots \cdot \overline{(p_1, q_1)}$ and we conclude that there are no relations between pairs of words of different lengths. $\square$

We now turn to look at relations between pairs of words of the same length in $\Sigma(\mathcal{C}(B))$.

There are infinitely many relations of the form $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(c,d)} \cdot \overline{(x,y)}$ as a consequence of $(a,b)(x,y) = (c,d)(x,y) \in B$. We now try to find a "canonical" (c,d) so that we may rewrite products $\overline{(a,b)} \cdot \overline{(x,y)}$ in a normal form with a view to obtaining a presentation for $\Sigma(\mathcal{C}(B))$.

For the relation $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(c,d)} \cdot \overline{(x,y)}$ to hold, we must have $(a,b)(x,y) = (c,d)(x,y)$ which holds if and only if $a-b=c-d$ and $\max(b,x) = \max(d,x)$.

Given that the values of a,b,x,y are fixed, $\max(b,x)$ is also fixed and this will determine a range of possible values for d and hence c. Observe first that we must have $d \leq \max(b,x)$. We now consider two cases:

Case 1: $\max(b,x) = b > x$. Then $b=d$ which forces $a=c$. In this case we will say that the word is already in normal form.

Case 2: $\max(b,x) = x \geq b$. Then $0 \leq d \leq x$ and $c = a-b+d$. If $a \geq b$ then set $d=0$ and we obtain $\overline{(a-b,0)} \cdot \overline{(x,y)}$ as the normal form. Otherwise set $c=0$ to obtain as the normal form $\overline{(0,b-a)} \cdot \overline{(x,y)}$.

We summarise this as follows:

Lemma 7.29. *Every product $\overline{(a,b)} \cdot \overline{(x,y)} \in \Sigma(\mathcal{C}(B))$ is equal to precisely one of the following:*

1. $\overline{(a,b)} \cdot \overline{(x,y)}$ *where* $b > x$,

2. $\overline{(a-b,0)} \cdot \overline{(x,y)}$ *where* $b \leq x$ *and* $b \leq a$,

3. $\overline{(0,b-a)} \cdot \overline{(x,y)}$ *where* $b \leq x$ *and* $b > a$.

Lemma 7.30. *The normal forms constructed above are unique.*

Proof. Consider $\overline{(a,b)} \cdot \overline{(x,y)}$. If $b > x$ then $b \geq 1$ as $x \geq 0$ and hence this relation cannot be of type 2 above. We saw earlier that if $\overline{(a,b)} \cdot \overline{(x,y)} = \overline{(c,d)} \cdot \overline{(x,y)}$ (for $c, d \geq 0$) and $b > x$ then we have $\overline{(a,b)} = \overline{(c,d)}$.

Suppose that $\overline{(p,0)} \cdot \overline{(x,y)} = \overline{(q,0)} \cdot \overline{(x,y)}$. Then, by acting on the sequence $\alpha = (0,0)$ and equating the outputs we obtain $(p+x,y) = (q+x,y)$ and hence $p = q$.

If $\overline{(p,0)} \cdot \overline{(x,y)} = \overline{(0,q)} \cdot \overline{(x,y)}$ then again by acting on the sequence $\alpha = (0,0)$ we obtain $(p+x,y) = (-q+\max(q,x), y-x+\max(q,x))$ which gives $x = \max(q,x)$ and hence $p = -q$. By the non-negativity requirement we have $p = q = 0$.

If $\overline{(0,p)} \cdot \overline{(x,y)} = \overline{(0,q)} \cdot \overline{(x,y)}$ then again by acting on the sequence $\alpha = (0,0)$ we obtain $(-p+\max(p,x), y-x+\max(p,x)) = (-q+\max(q,x), y-x+\max(q,x))$ which forces $\max(p,x) = \max(q,x)$ and hence $p = q$. $\square$

Applying Lemma 7.30 from right to left to words of length at least two will give us a normal form for words in $\Sigma(\mathcal{C}(B))$ which leads us to conjecture the following:

Conjecture 7.31. *An infinite presentation for* $\Sigma(\mathcal{C}(B))$ *is*

$$\Sigma(\mathcal{C}(B)) = \langle \overline{(i,j)}(i,j \geq 0) | \overline{(a,b)} \cdot \overline{(x,y)} = \overline{(a-b,0)} \cdot \overline{(x,y)}(a,x \geq b), \\ \overline{(a,b)} \cdot \overline{(x,y)} = \overline{(0,b-a)} \cdot \overline{(x,y)}(x \geq b > a) \rangle.$$

7.4 Examples

We conclude this chapter by examining some more examples of Cayley automaton semigroups arising from infinite semigroups.

Example 7.32. Let R be the infinite right-zero semigroup and let $x, y \in R$. Then $xa = ya$ for all $a \in R$ and so the congruence $\sim$ defined in Section 7.2 has only one congruence class. By Lemma 7.10 $\Sigma(\mathcal{C}(R))$ is generated by one element. By Proposition 3.10 this element is a right-zero. Hence $\Sigma(\mathcal{C}(R))$ is trivial.

Example 7.33. Let L be the infinite left-zero semigroup. Then for each $x \in L$ we have that $[x] = \{x\}$ and so $\Sigma(\mathcal{C}(L))$ is generated by infinitely many elements which are all left-zeros by Proposition 3.9. Hence $\Sigma(\mathcal{C}(L)) \cong L$.

Example 7.34. Let Z be the infinite null semigroup and let $x, y \in Z$. Then $xa = ya = 0$ for all $a \in Z$ and so the congruence $\sim$ defined in Section 7.2 has only one congruence class. By Lemma 7.10 $\Sigma(\mathcal{C}(Z))$ is generated by one element. By Corollary 3.11 this element is a zero. Hence $\Sigma(\mathcal{C}(Z))$ is trivial.

Example 7.35. Let $S = \{x_1, x_2 \ldots, y_1, y_2 \ldots\}$ be defined by the relations $x_i a = x_1$ and $y_i a = y_1$ for all $a \in S$ and $i \geq 1$. Then the congruence $\sim$ has two classes, namely $[x_1]$ and $[y_1]$. Thus we may take $\overline{x_1}$ and $\overline{y_1}$ as generators for $\Sigma(\mathcal{C}(S))$. Note also that $\overline{x} \cdot \alpha = (x_1)^\omega$ and $\overline{y_1} \cdot \alpha = (y_1)^\omega$ for all sequence $\alpha \in S^*$. Hence $\Sigma(\mathcal{C}(S)) \cong L_2$.

Note also that this example is easily extended and we may obtain L_n for any $n \geq 1$.

Example 7.36. Let S be an infinite rectangular band (i.e. a direct product of a left- and a right-zero semigroup, at least one of which is infinite). Then $\sim$ has classes $[(l_1, r_1)], [(l_2, r_1)], [(l_3, r_1)] \ldots$. If the left-zero semigroup is finite then there are only finitely many classes and by Lemma 7.10 $\Sigma(\mathcal{C}(S))$ is finitely generated; otherwise $\Sigma(\mathcal{C}(S))$ is generated by the elements $\{\overline{(l_i, r_1)}\}$ where $i \in \mathbb{N}$. In either case, as per Example 3.15, $\Sigma(\mathcal{C}(S))$ is isomorphic to a left-zero semigroup.

Chapter 8

Further Questions

In this final chapter we present some questions which have not been fully answered in this thesis which may lead to further work in the area of Cayley automaton semigroups.

In Chapter 5 we considered self-automaton semigroups, defined to be those semigroups satisfying $S \cong \Sigma(\mathcal{C}(S))$ under the map $s \mapsto \overline{s}$. We commented in Section 5.1 that this definition is not a direct analogue of the original definition given by Cain in [7], where a semigroup S was said to be self-automaton if $S \cong \Sigma(\mathcal{C}(S))$ for any isomorphism. A lack of examples of semigroups satisfying $S \cong \Sigma(\mathcal{C}(S))$ but not via the map $s \mapsto \overline{s}$ led to the use of the more restricted Definition 5.3. However, the question of what is the "correct"definition of a self-automaton semigroup remains open, and is recorded below:

Question 8.1. *Do there exist semigroups S satisfying $S \cong \Sigma(\mathcal{C}(S))$ but not under the mapping $s \mapsto \overline{s}$?*

It was noted in Section 5.1 that if such an example exists then it does not have a faithful left-regular representation. When considering the map $s \mapsto \overline{s}$ in Chapter 5 we were able to determine precisely when it is injective in Lemma 5.6. In the case of bands, we showed in Lemma 5.9 that the map is always a homomorphism, and in Lemma 5.14 we generalised this to semigroups where S^2 is a band. However, in Example 5.16 we were not able to make use of these lemmas to show that $s \mapsto \overline{s}$ was a homomorphism and had to show this explicitly. This raises the following question:

Question 8.2. *For which semigroups is the map $s \mapsto \overline{s}$ a homomorphism?*

If an answer to Question 8.2 is obtainable then this, together with Lemma 5.6 would enable us to classify all self-automaton semigroups when we take the map $s \mapsto \overline{s}$ being an isomorphism as the definition of being self-automaton.

Regardless of what the correct definition of self-automaton is, the natural question to consider is that of classifying all self-automaton semigroups. Cain posed this question originally in [7] in the setting of right-actions, but his suggested answer of bands with square $\mathcal{D}$-classes and every maximal $\mathcal{D}$-class being a singleton was shown to be false in Example 5.27. In attempting to classify self-automaton semigroups (using Definition 5.3) we were able to obtain results for the classes of finite bands, monoids and regular semigroups. All self-automaton semigroups in these classes were shown to be bands with faithful left-regular representations, but examples not fitting this classification were constructed in Sections 5.3 and 5.4. A complete classification remains an open problem, which is stated below:

Question 8.3. *Is it possible to completely classify the finite self-automaton semigroups?*

The focus of Chapter 5 was on finite self-automaton semigroups. Infinite semigroups were considered in Chapter 7 and so we may ask at this point if we can say anything about infinite self-automaton semigroups. Notice that the proofs of Lemmas 5.6 and 5.9 and Theorems 5.10 and 5.11 did not actually depend on the semigroup being finite. Thus the results there immediately translate to infinite semigroups and we see that the infinite self-automaton bands, monoids, regular semigroups and semigroups with relative left and right identities are precisely the bands with faithful left-regular representations. It remains to be seen if other infinite semigroups are self-automaton:

Question 8.4. *Is it possible to completely classify the infinite self-automaton semigroups?*

Following on from self-automaton semigroups, Chapter 6 considered Cayley chains of finite aperiodic semigroups; that is, the sequence of semigroups obtained by iterating the Cayley automaton semigroup construction. Recall that for a semigroup S, $S_0 = S$ and $S_i = \Sigma(\mathcal{C}(S_{i-1}))$ for $i \geq 1$. We showed that there exist semigroups where the length of the chain is infinite, and that there exist semigroups with $S_{n-1} = S_n$ for every $n \geq 1$ (see Proposition 6.3

and Example 6.5). Currently, there are no examples of Cayley chains with a non-trivial loop and so we pose the following:

Question 8.5. *Does there exist a finite aperiodic semigroup S with $S_k = S_{k+r}$ where $k \geq 0$ and $r \geq 2$?*

If such an example exists then the semigroup $U = S_k \cup_0 S_{k+1} \cup_0 \ldots \cup_0 S_{k+r-1}$ would satisfy $U \cong \Sigma(\mathcal{C}(U))$ and would be a positive answer to Question 8.1. Note that such an example cannot satisfy $U \cong \Sigma(\mathcal{C}(U))$ under the mapping $u \mapsto \overline{u}$ as this would force S_k to be self-automaton as per Definition 5.3 and hence we would have $S_k = S_{k+1}$ (this follows from Proposition 3.8 which states that $\Sigma(\mathcal{C}(V \cup_0 W)) \cong \Sigma(\mathcal{C}(V)) \cup_0 \Sigma(\mathcal{C}(W))$ for semigroups V and W).

We know that there exist examples of finite aperiodic semigroups with Cayley chains of any arbitrary finite length and examples where the Cayley chain is infinite. We have not seen any way of determining if the Cayley chain is finite or infinite without explicitly constructing it and so we pose the following question:

Question 8.6. *For a given finite aperiodic semigroup S, is it decideable whether or not $\Delta(S) < \infty$?*

In Theorem 6.13 we considered a semigroup T satisfying $\Delta(T) = n$ and T_n is self-automaton (in the sense of Definition 5.3). We showed that for a subsemigroup $S \leq T$ there exists k such that $S_k = S_{k+1}$. We see from this that a negative answer to Question 8.1 would give a negative answer to Question 8.5.

Proposition 6.7 showed how the lengths $\Delta(S)$ and $\Delta(T)$ of two semigroups S and T were related to the length of the zero-union of S and T and Proposition 6.15 considered how the length of the chain behaves after a zero element has been adjoined to the semigroup. Other semigroup constructions (such as direct product, semidirect products, wreath products, normal ideal extensions and so on) could be considered and so we ask the following:

Question 8.7. *Let S, T be semigroups satisfying $\Delta(S), \Delta(T) < \infty$ and let $\circledcirc$ denote a semigroup construction. Is it possible to express $\Delta(S \circledcirc T)$ in terms of $\Delta(S)$ and $\Delta(T)$?*

Before attempting to classify self-automaton semigroups in Chapter 5, we were able to classify the Cayley automaton semigroups arising from finite monogenic semigroups in Chapter 4 . One may ask if it is possible to obtain a similar result for other "nice"classes of semigroup, such as Rees-Matrix semigroups, regular semigroups, inverse semigroups and so on. We ask the following question:

Question 8.8. *For which classes of semigroup is it possible to completely classify all such $\Sigma(\mathcal{C}(S))$ where S is a member of the given class?*

Finally, in Chapter 7, we considered Cayley automaton semigroups of infinite semigroups. Examples 7.32, 7.33, 7.35 and 7.36 showed that the resulting Cayley automaton semigroup can be either finite or infinite. Lemma 7.10 gave a sufficient condition for $\Sigma(\mathcal{C}(S))$ to be finitely generated (but not necessarily finite). This leads to the following questions:

Question 8.9. *For an infinite semigroup S, under which conditions is $\Sigma(\mathcal{C}(S))$ finitely generated?*

Question 8.10. *For an infinite semigroup S, under which conditions is $\Sigma(\mathcal{C}(S))$ finite?*

In Section 7.3 we constructed the Cayley automaton semigroup of the bicyclic monoid. A natural question to ask following on from this is:

Question 8.11. *Let*

$$P_n = \langle b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_n | b_i c_i = 1, b_i c_j = 0 (i \neq j) \rangle$$

be the polycyclic monoid of rank n where $n \geq 2$. What is $\Sigma(\mathcal{C}(P_n))$?

Bibliography

[1] A. Akhavi, I. Klimann, S. Lombardy, and J. Mairesse. On the finiteness problem for automaton (semi)groups. *International Journal of Algebra and Computation*, 22(4), 2011.

[2] S.V. Aleshin. Finite automata and Burnside's problem for periodic groups. *Mathematical Notes of the Academy of Sciences of the USSR*, 11:199–203, 1972.

[3] M. Arbib, K. Krohn, and J. Rhodes. *Algebraic Theory of Machines, Languages and Semigroups.* Academic Press, 1968.

[4] L. Bartholdi, R.I. Grigorchuk, and Z. Šunić. Branch groups. In *Handbook of Algebra*, volume 3. North Holland, Amsterdam, 2003.

[5] L. Bartholdi, R.I. Grigorchuk, and Z. Šunić. From fractal groups to fractal sets. In *Fractals in Graz 2001*, Trends in Mathematics, pages 25–118. Birkhauser, Basel, 2003.

[6] L. Bartholdi and V. Nekrashevych. Thurston equivalence of topological polynomials. *Acta Mathematica*, 197:1–51, 2006.

[7] A.J. Cain. Automaton semigroups. *Theoretical Computer Science*, 410:5022–5038, 2009.

[8] C.M. Campbell, E.F. Robertson, N. Ruškuc, and R.M. Thomas. Reidemeister–schreier type rewriting for semigroups. *Semigroup Forum*, 51:47–62, 1995.

[9] A.H. Clifford and G.B. Preston. *The Algebraic Theory of Semigroups*, volume 1. American Mathematical Society, 1961.

[10] A.H. Clifford and G.B. Preston. *The Algebraic Theory of Semigroups*, volume 2. American Mathematical Society, 1967.

[11] E. Deza and M. Deza. *Figurate Numbers*. World Scientific, 2012.

[12] L.E. Dickson. *History of the Theory of Numbers*, volume 2. Carnegie Institute of Washington, 1920.

[13] S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, New York, 1974.

[14] N.J. Fine. Binomial coefficients modulo a prime. *The American Mathematical Monthly*, 54(10):589–592, 1947.

[15] P. Gallagher. *On the Finite Generation and Presentability of Diagonal Acts, Finitary Power Semigroups and Schützenberger Products*. PhD thesis, University of St Andrews, 2005.

[16] R.I. Grigorchuk. On Burnside's problem on periodic groups. *Functional Analysis and its Applications*, 14(1):53–54, 1980.

[17] R.I. Grigorchuk, V. Nekrashevich, and V.I. Sushchanskii. Automata, dynamical systems and groups. *Proceedings of the Steklov Institute of Mathematics*, 231:128–203, 2000.

[18] R.I. Grigorchuk and Z. Šunić. Self-similarity and branching in group theory. In *Groups St Andrews 2005*, volume 1 of *London Mathematical Society Lecture Note Series*, page 339. Cambridge University Press, 2007.

[19] N. Gupta and S. Sidki. On the Burnside problem for periodic groups. *Mathematische Zeitschrift*, 182(3):385–388, 1983.

[20] M. Hoffmann, R.M. Thomas, and N. Ruškuc. Automatic semigroups with subsemigroups of finite Rees index. *International Journal of Algebra and Computation*, 12(3):463–476, 2002.

[21] J.M. Howie. *Fundamentals of Semigroup Theory.* London Mathematical Society Monographs New Series. Clarendon Press, 1995.

[22] K. Krohn and J. Rhodes. Algebraic theory of machines 1: Prime decomposition theorem for finite semigroups and machines. *Transactions of the American Mathematical Society*, 116:450–464, 1965.

[23] E.S. Ljapin. *Semigroups*, volume 3 of *Translations of Mathematical Monographs.* American Mathematical Society, 1963.

[24] C.T. Long. Pascal's triangle modulo p. *Fibonacci Quarterly*, 19(3):458–463, 1981.

[25] V. Maltcev. Cayley automaton semigroups. *International Journal of Algebra and Computation*, 19(1):79–95, 2009.

[26] D. McCune. *Groups and Semigroups Generated by Automata*. PhD thesis, University of Nebraska, Lincoln, 2011.

[27] A. McLeman. Self-automaton semigroups. *Semigroup Forum*, 2014. DOI 10.1007/s00233-014-9610-3.

[28] A. Mintz. On the Cayley semigroup of a finite aperiodic semigroup. *International Journal of Algebra and Computation*, 19(6):723–746, 2009.

[29] V. Nekrashevych. Self-similar groups. In *Mathematical Surveys and Monographs*, volume 117. American Mathematical Society, 2005.

[30] B.H. Neumann. Embedding theorems for semigroups. *Journal of the London Mathematical Society*, 35:184–192, 1960.

[31] N. Ruškuc. On large subsemigroups and finiteness conditions of semigroups. *Proceedings of the London Mathematical Society*, 76(3):383–405, 1998.

[32] P.V. Silva and B. Steinberg. On a class of automata groups generalizing lamplighter groups. *International Journal of Algebra and Computation*, 15(5 and 6):1213–1234, 2005.

[33] B. Steinberg. Contribution to “Existence of a possible counterexample in automaton semigroups”. `mathoverflow.net/questions/134694`, 2013.