# ADVENTURES IN APPLYING ITERATION LEMMAS

**Markus Johannes Pfeiffer**

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

**2013**

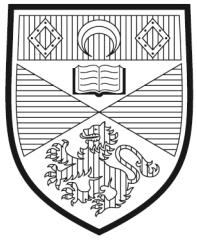
# Adventures in Applying Iteration Lemmas

Markus Johannes Pfeiffer

Thesis submitted for the Degree of PhD in Mathematics

University of St Andrews

15 April 2013



University of
St Andrews

600
YEARS

# *Declarations*

## *Candidate's Declarations*

I, Markus Pfeiffer, hereby certify that this thesis, which is approximately 35,000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

I was admitted as a research student and as a candidate for the degree of Doctor of Philosophy in September 2008; the higher study for which this is a record was carried out in the University of St Andrews between 2008 and 2012.

I received assistance in the writing of this thesis in respect of language and syntax, which was provided by Tara Brough.

Date: Signature of candidate:

## *Supervisors' Declarations*

I, Nik Ruškuc, hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy 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:

I, Max Neunhöffer, hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy 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:

## *Permission for Electronic 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 candidate and supervisor regarding the electronic publication of this thesis:

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

Date: Signature of supervisor:

Date: Signature of supervisor:

Date: Signature of candidate:

# *Abstract*

The word problem of a finitely generated group is commonly defined to be a formal language over a finite generating set.

The class of finite groups has been characterised as the class of finitely generated groups that have word problem decidable by a finite state automaton.

We give a natural generalisation of the notion of word problem from finitely generated groups to finitely generated semigroups by considering relations of strings. We characterise the class of finite semigroups by the class of finitely generated semigroups whose word problem is decidable by finite state automata.

We then examine the class of semigroups with word problem decidable by asynchronous two tape finite state automata. Algebraic properties of semigroups in this class are considered, towards an algebraic characterisation.

We take the next natural step to further extend the classes of semigroups under consideration to semigroups that have word problem decidable by a finite collection of asynchronous automata working independently.

A central tool used in the derivation of structural results are so-Called iteration lemmas.

We define a hierarchy of the considered classes of semigroups and connect our original results with previous research.

# *Contents*

# *List of Figures*

# *Prologue*

*"Bouncy trouncy flouncy pouncy, fun fun fun fun fun.*
*The most wonderful thing about tiggers is I'm the only one!"*
*—Tigger*
*(unique up to isomorphism)*

## *Overview*

At its core, this thesis is concerned with two disciplines within mathematics, the theory of *semigroups* and the theory of *formal languages and computation*. Only briefly we touch the topic of formal logic. Both disciplines are comparatively young, with both semigroups and computation attracting attention only in the early 20th century. They are also both naturally intertwined on many levels.

The main topic of this thesis are finitely generated semigroups that admit a low complexity algorithm to solve the word problem. Low complexity in our case means that there exists a finite state computation that determines equality of elements represented by potentially different strings.

At face value we take a very theoretical point of view with no obvious direct applications. It should be noted that, quite to the contrary, almost all concepts are at least implementable as computer algorithms and therefore available for applications in computational algebra.

For every lemma or theorem we give a proof if this is doable within the bounds of this document, even if the result is well-known. Some proofs had to be omitted since they would have taken up too much space or would have required to divert too far to provide a full proof. Wherever proofs have been omitted, a reference is given. Giving a proof is not equivalent to claiming originality of the result, even if we give a proof and no reference, and most well-known results should be considered folklore then.

As it is common for a document concerned with mathematics, we give the very foundational definitions and conventions in Chapter 1. We will be concerned with classical mathematics and only assume familiarity with the notions of *set* and *map*. We note that it is maybe of interest to find equivalent constructions in intuitionistic and constructive mathematics, and will further hint at such possibilities in Chapter 11. One notion worth mentioning here is the notion of specification which will be briefly touched in Section 1.8. The means of specification is usually not consciously noticed in mathematics, but it has particular importance in computation: How is the input for an algorithm specified, how is the output specified?

In the same way Chapter 2 goes on to define semigroups, monoids and groups and gives a few theorems that are either referenced in later chapters or give important insights into semigroup theory. Most of this sections contents are standard in semigroup theory, and more detailed treatise of the material can for example be found in [How95].

The following Chapter 3 is solely concerned with subsets of semigroups and introduces the notions of recognisable, rational, polyrational and extended rational subsets and lays down the groundwork for everything in Chapters 7 to 10. The notions of recognisable, rational, polyrational and extended rational subset all share that they are strong finiteness conditions. On one hand this leads to very restricted classes of sets, but on the other hand it leads to strong results and in particular decidability results. Extensive treatment of

recognisable and rational subsets of semigroups, monoids and groups can be found in [Ber79] and [Eil76a]. The latter offers some generalisations of the notion of rational subsets of a given semigroup and the author hints at the possibility of treating what we call extended rational and polyrational subsets in the preface of [Eil76a]. One of the most important tools in the context of examining these finiteness conditions are iteration lemmas, which are employed to show that a subset cannot fall into one of the mentioned classes.

Unfortunately Eilenberg has never finished Volume C of his book and to our knowledge there has not been a thorough treatment of these notions. We therefore define extended rational and polyrational subsets and claim originality of the surrounding results. Since the notion of extended rational subsets of a semigroup are not central to our work, there is possibility for research branching from here. The sections on rational, extended rational and polyrational relations touch on methods of formal logic with definitions of syntax and semantics by induction.

In Chapter 4 we define what we formally mean by the notion of *computation*. A computation is always carried out with *finite state* but there might be an infinite set of *configurations* caused by the availability of memory or storage. We will mainly be concerned with computation that can be carried out nondeterministically by devices that only have a finite amount of memory. This chapter is inspired and influenced by [Eil76a]. We give the known result that the notions of rational subset and finite state computability are equivalent for certain semigroups and monoids. We introduce our notion of a parallel finite automaton and show that the notions of polyrational subsets and parallel finite computability are equivalent for certain semigroups and monoids. We also take the time to introduce Eilenberg's notion of a machine, mainly with view on extensions of the presented material.

Chapter 5 gives specifications of semigroups that serve as examples throughout the remainder of this work. We also prove some properties of the given

semigroups.

Chapter 6 gets us to the main topic of this thesis: we give the motivation for our work with roots in the work of Max Dehn in group theory in the early 20th century. We define what Max Dehn's definition of the word problem of a group is and give a natural generalisation of the word problem to semigroups and relations on a semigroup. We also define the notion of coword problem.

In Chapter 7 we present an equivalent of Anisimov's theorem for semigroups. Anisimov's theorem first appeared in [Ani71] and connects group theory and formal language theory. Slightly more formally it states that the word problem of a group is finite state computable if and only if the group is finite. Anisimov's theorem is widely considered to be the first of its kind. We prove that the class of semigroups with finite state computable word problem of a certain class is exactly the class of finite semigroups, therefore establishing a generalisation of Anisimov's theorem for the definition of word problem we gave in 6. Although the proof of this theorem almost completely relies on a result by Mezei, it is nonetheless a new result.

Chapter 8 is arguably the centre of this thesis and consists almost exclusively of original research. We introduce a class of semigroups with finite state computable word problem which we call semigroups with rational word problem. The class of semigroups with rational word problem contains all finite semigroups, and also some infinite semigroups. We find as many properties as possible for these semigroups, towards a characterisation. Since this could not be achieved yet, we try bounding the class of semigroups with rational word problem using properties of elements, subsets and Green's relations. As mentioned earlier, we make heavy use of iteration lemmas.

More specifically, we prove the following main results. Firstly, having rational word problem does not depend on the choice of a finite generating set. An infinite semigroup with rational word problem has an element of infinite order, and elements of finite order have to have bounded period. We

conjecture that the index of such elements is bounded as well. We show that Kleene's theorem holds in semigroups of this class, and that as a consequence all semigroups in the class are residually finite. We also give a proof that any finitely generated semigroup in which all elements have regular sets of representatives are residually finite. We show how having rational word problem passes through to subsemigroups and oversemigroups of finite Rees and Green index. A section on product constructions show that the class of semigroups with rational word problem is not closed under taking direct products, the proof of which employs an iteration lemma, but it is closed under semigroup free products and zero unions. We also show that Green's relations on semigroups with rational word problem are polyrational and for semigroups that are cancellative and have rational word problem we show that the Green's relations $\mathcal{R}$ and $\mathcal{L}$ are rational. The $\mathcal{H}$-classes of a semigroup with rational word problem have to be all finite. This is proven by employing an important result discovered by Schützenberger, and again an iteration lemma. We also hint at the appeal of semigroups with rational word problem with respect to decidability of certain properties. Among these properties there is the word problem, all Green's relations word problems, triviality and finiteness. It is also decidable whether a semigroup with rational word problem is a group. Some results in this chapter can also be found in the paper [NPR11] which has been submitted for peer review and, at the time of this writing, is awaiting referee's feedback.

Since in particular the results about direct products in Chapter 8 are not quite satisfactory we realise a slightly larger class of semigroups in Chapter 9, the class of semigroups with polyrational word problem. This class is shown to share many of the important properties of the class of semigroups with rational word problem with the additional property that it is closed under taking finite direct products. We show that there is an infinite hierarchy of semigroups with ever increasing complexities of the word problem, very

probably much like Eilenberg envisioned in [Eil76a]. To establish this infinite hierarchy we again use an iteration lemma type argument. The results from this chapter will appear in publication in the near future in cooperation with Tara Brough and Nik Ruškuc.

In Chapter 10 we establish how our research and the classes of semigroups found in the previous chapters fit into the known landscape of word problem complexities. We refer to many surrounding results, proposing to establish a fine-grained hierarchy of word problem complexities and filling white spots.

The closing chapter will then hint at the open questions asked throughout this thesis and possible directions for future research.

## *Acknowledgements*

I would like to thank the following people and institutions for their support in undertaking this project. Without them I would not have been able to complete it.

I thank my parents, Ortrud and Wilhelm Pfeiffer who have always encouraged me to pursue my aims and without whom I would not be the person that I am today. Also I thank my brother Martin Pfeiffer and my sister Anne Mühlenberg who supported me during the hard time that was the beginning of my time in Saint Andrews.

Also I thank my partner, office mate and fellow mathematician, Jennifer Awang for being who she is and introducing me to Doctor Who and the work of Alan Alexander Milne.

I am very grateful to Nik Ruškuc, who helped me with my application for funding, my admission to Saint Andrews and accommodation for the first months of my studies. He also was one of my supervisors and suggested the topic for the presented research project. His contributions not only to this thesis but also to my development as a mathematician and a person are

much more substantial: He taught me how to ask interesting questions, a valuable skill for a mathematician to have, and how to phrase theorems. He also made me think about how important it is to be careful with arguments, in particular in semigroup theory, to which I was introduced by him. His cheerful personality also added to the fact that the School of Mathematics and Statistics in Saint Andrews is such a wonderful place. I hope his influence will stay with me and I will be able to pass the knowledge on to students of my own one day.

No less important was my second supervisor, Max Neunhöffer, whom I had already met in Aachen and who was virtually always available for discussion of my ideas. He made me explain my mathematics in detail and therefore made me recognise important details. Discussions with him showed me how essential precise communication and changes of one's point of view are. Also, he read parts of the manuscript very carefully, suggested improvements and found mistakes.

In the final few months of my research work Tara Brough has been a great help in many productive discussions about the topic. She also read the manuscript and suggested a number of improvements. She particularly helped with extending what is now Theorem 8.7.7 and with Theorem 8.7.11.

I thank Gerhard Hiss for encouraging me to apply to Saint Andrews, and I thank Erich Grädel for providing a reference.

I would like to thank my former office mates Andreas Distler and Victor Maltcev and my fellow student Simon Craik for their ideas and willingness to listen to my sometimes vague ones. The treatment of Green index and Green's relations in Chapter 8 owes a lot to the discussions with Simon Craik in particular.

I also thank John Howie, Samuel Eilenberg and Marcel Schützenberger for providing such excellent monographs on the topics relevant to my research. I took great inspiration from many aspects of their writing from notation over

techniques to presentation.

Also, I thank my fellow students Claire Pollard, Samuel Baynes, Anna Schroeder, Nina Menezes, James Hyde and Arthur Geddes who have provided me with fun chat and cake. In addition, I would also like to thank all the people at the Mathematical Institute who have provided me with such a stimulating environment. This especially includes all the supporting staff such as secretaries, computing officers and estates staff.

A very special thank you goes to Jon Cohen and Megan Stahl who have made the year 2011 one of the most memorable ones of my life.

I would like to thank the University of Saint Andrews and the town of Saint Andrews for providing such a pleasant and quiet, yet stimulating research environment.

The research for this thesis was carried out over the course of the years 2008 to 2012 at the University of Saint Andrews, with financial support provided by the EPSRC doctoral training grant and the School of Mathematics and Statistics, without which I would not have been able to work as productively and independently.

In closing, it is of great personal importance to me to thank the European Union for making it possible for me and all Europeans to live, travel and work in freedom. I would like to encourage the people of Europe to further pursue the idea of a united Europe, even in the face of the current problems. I also would like to encourage every European citizen to actively work towards the goal of a united and free Europe.

# 1

○ ○ ⊙

# *Concepts*

In this chapter we fix notation and conventions for the basic mathematical notions that are used. The most important being *sets*, with the *natural numbers* being explicitly defined, *maps* and *relations*.

## *1.1 Sets*

We base our work on the system ZF, the Zermelo-Fränkel system of axioms for set theory. In places we might need the axiom of choice or equally powerful axioms, but these should be sparse and arguments should in general be constructive.

Defining sets is the central topic of ZF and we refer the reader to a book on the topic for further reference. One of the axioms of ZF ensures the existence of the *powerset*, the set of all subsets, of any given set X. We denote the powerset of a set X by $\hat{X}$.

## 1.2 Natural Numbers

The natural numbers capture the abstract concepts of quantity and of discrete linear orders.

There is always discord about whether zero is a natural number or not. We will make the following choices. We inductively define the set $\mathbb{N}$ of natural numbers as follows

- $\{\} \in \mathbb{N}$, and
- For $n \in \mathbb{N}$, the set $n \cup \{n\} \in \mathbb{N}$.

We can give a decimal representation of every natural number by defining the decimal representation of $\{\}$ to be $0$ and the decimal representation of $n \cup \{n\}$ to be $n + 1$. Therefore the natural numbers contain $0$. Since we regularly refer to $\mathbb{N} \setminus \{0\}$, we denote this subset of $\mathbb{N}$ by $\mathbb{N}_{>0}$.

## 1.3 Maps

A *map* from a set $X$ to a set $Y$ assigns to every element of $X$ precisely one element of $Y$. We use the following conventions.

Let $X$ and $Y$ be two sets. We denote a map $f$ from $X$ to $Y$ by

$$X \xrightarrow{f} Y.$$

We denote the element of $Y$ which is assigned to $x \in X$ by the map $f$ by $xf$, and we say that $f$ is *applied* to the *argument* $x$.

If $Y \xrightarrow{g} Z$ is another map then the *composition* of $f$ and $g$ is denoted by $fg$ or

$$X \xrightarrow{f} Y \xrightarrow{g} Z.$$

For any given set $X$ the *identity map* $X \xrightarrow{\iota_X} X$ is defined by

$$\iota_X : X \longrightarrow X,\ x \mapsto x,$$

and the *full transformation monoid* $\mathcal{T}_X$ is the set of all maps $X \xrightarrow{f} X$.

A map $X \xrightarrow{f} Y$ is *injective* if for all maps $Z \xrightarrow{g_1} X$ and $Z \xrightarrow{g_2} X$ the equality $g_1 f = g_2 f$ implies $g_1 = g_2$, it is *surjective* if for all maps $Y \xrightarrow{g_1} Z$ and $Y \xrightarrow{g_2} Z$ the equality $f g_1 = f g_2$ implies $g_1 = g_2$ and it is *bijective* if there is a map $Y \xrightarrow{f'} X$ such that $ff' = \iota_X$ and $f'f = \iota_Y$.

## 1.4 Relations

We adopt the definition of relations as used by Eilenberg in [Eil76a]. Relations are a generalisation of a maps, since a relation between a set X and a set Y relates any element of x with a subset of Y.

**Definition 1.4.1**

*Let* X *and* Y *be sets. A* relation ρ from X to Y, *denoted* $X \xrightarrow{\rho} Y$ *is a map* $\hat{X} \xrightarrow{\hat{\rho}} \hat{Y}$ *such that for any family* $(X_i)_{i\in I}$ *of subsets of* X

$$\Big(\bigcup_{i\in I} X_i\Big)\,\hat{\rho} = \bigcup_{i\in I} (X_i\hat{\rho})\,.$$

It follows that a relation $X \xrightarrow{\rho} Y$ is defined by the images of $\hat{\rho}$ on singleton subsets of X. We will identify elements $x \in X$ with the singleton subset $\{x\} \subset X$, and therefore can also view a relation $X \xrightarrow{\rho} Y$ as a map $X \xrightarrow{\rho} \hat{Y}$. Note also that for any map $X \xrightarrow{f} Y$ we can define a relation $X \xrightarrow{f} Y$ by

$$\hat{f} : \hat{X} \longrightarrow \hat{Y},\ \{x\} \mapsto \{xf\},$$

which justifies using the same notation for maps and relations and interpreting maps as relations without explicitly stating this. For relations $X \xrightarrow{\rho} Y$ and $X \xrightarrow{\sigma} Y$ we write $\sigma \subset \rho$ if for $x \in X$ the image $x\sigma$ is a subset of $x\rho$.

For two relations $X \xrightarrow{\rho} Y$ and $Y \xrightarrow{\sigma} Z$ their *composition* $X \xrightarrow{\rho\sigma} Z$ can be straightforwardly defined by composition of the underlying maps: $\widehat{\rho\sigma} = \hat{\rho}\hat{\sigma}$.

We will also need the following characterisation.

**Lemma 1.4.2**

*Let* $X \xrightarrow{\rho} Y$ *and* $Y \xrightarrow{\sigma} Z$ *be two relations. Then* $z \in x\rho\sigma$ *if and only if there exists* $y \in x\rho$ *such that* $z \in y\sigma$.

For a given relation $X \xrightarrow{\rho} Y$ the *domain* $\operatorname{dom}\ \rho$ of $\rho$ is the set

$$\operatorname{dom}\ \rho = \{x \in X \mid x\rho \neq \emptyset\},$$

the *image* $\operatorname{im}\ \rho$ of $\rho$ is the set

$$\operatorname{im}\ \rho = \{y \in Y \mid \exists x \in X \text{ with } y \in x\rho\}.$$

The *reverse* $\rho^r$ of $\rho$ is defined by

$$y\rho^r = \{x \in X \mid y \in x\rho\},$$

and is itself a relation. The *graph* $\mathcal{G}_\rho$ of $\rho$ is the set of pairs

$$\mathcal{G}_\rho = \{(x, y) \in X \times Y \mid x \in X, y \in x\rho\}.$$

It is more common to define relations by their graphs.

For any set $X$ we denote by $\mathcal{R}_X$ the set of all relations $X \xrightarrow{\rho} X$ and call it the *full relation monoid* on $X$.

Let $X$ be a set and fix a subset $A \subset X$. Define the *diagonal relation* $\cap A$ by

$$\hat{\cap A} : \hat{X} \longrightarrow \hat{X},\ Y \mapsto Y \cap A.$$

Note that the graph of $\cap A$ is exactly the diagonal set $\{(a, a) \mid a \in A\}$.

The *universal relation* $X \xrightarrow{\mu_X} X$ is defined by

$$\hat{\mu}_X : \hat{X} \longrightarrow \hat{X},\ Y \mapsto X.$$

We prove this small lemma needed in a later proof, it is taken from [Eil76a].

**Lemma 1.4.3**

*Let $X$,$Y_1$,$Y_2$ be sets and $X \xrightarrow{\rho} Y_1 \times Y_2$ and $X \xrightarrow{\rho_i} Y_i$ for $i \in \{1,2\}$ be relations such that*

$$x\rho = (x\rho_1) \times (x\rho_2)$$

*for $x \in X$. Let $Z \subset X$ and let $Y_1 \xrightarrow{\sigma} Y_2$ be defined by the composition*

$$Y_1 \xrightarrow{\rho_1^r} X \xrightarrow{\cap Z} X \xrightarrow{\rho_2} Y_2.$$

*Then $\mathcal{G}_\sigma = Z\rho$.*

*Proof.* Let $Y = Y_1 \times Y_2$ and $Y \xrightarrow{\pi_i} Y_i$ for $i \in \{1,2\}$ be projections onto the factors. Now $\rho_i = \rho\pi_i$ and we can write $\sigma$ as

$$Y_1 \xrightarrow{\pi_1^r} Y \xrightarrow{\rho^r} X \xrightarrow{\cap Z} X \xrightarrow{\rho} Y \xrightarrow{\pi_2} Y_2$$

which is equal to

$$Y_1 \xrightarrow{\pi_1^r} Y \xrightarrow{\cap B} Y \xrightarrow{\pi_2} Y_2.$$

where $B = Z\rho$ and the graph of the above composition is $B$. □

We also define the *intersection* of a finite family of relations as we will need this notion later. We note that the intersection of relations is in fact a relation.

**Definition 1.4.4**

*Let $X$ and $Y$ be sets, $k \in \mathbb{N}$ and let $X \xrightarrow{\rho_i} Y$ for $i \in \underline{k}$ be relations. We define the* intersection $\bigcap_{1 \le i \le k} \rho_i$ *as*

$$\bigcap_{1 \le i \le k} \rho_i : X \longrightarrow Y,\ x \mapsto \bigcap_{1 \le i \le k} x\rho_i.$$

## 1.5 Equivalence Relations

Equivalence relations are an abstraction of equality. A relation $X \xrightarrow{\rho} X$ is an *equivalence relation*, or *equivalence* for short, if

$$\iota_X \subset \rho, \qquad \rho^r \subset \rho, \text{ and} \qquad \rho\rho \subset \rho. \tag{1.1}$$

Writing $x \sim_\rho y$ instead of $x \in y\rho$ we get the familiar axioms for an equivalence relation. For any $x \in X$ the *equivalence class* of $x$ with respect to the equivalence relation $\rho$ is now the image of $\{x\}$ under the map $\rho$. The equivalence classes partition the set X.

A *cross section of* $\rho$ is a subset D of X such that $|D \cap x\rho| = 1$ for all $x \in X$, in other words D contains exactly one representative for each equivalence class.

We write $X/_\rho$ to denote the set of all equivalence classes of $\rho$. Note that associated with every equivalence relation on a set X there is a natural map

$$\pi_\rho : X \longrightarrow X/_\rho,\ x \mapsto x\rho.$$

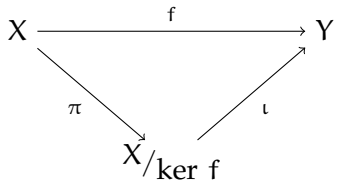
Conversely we note that any map $X \xrightarrow{f} Y$ defines the equivalence relation $\ker f$ on X as $x \sim_{\ker f} y$ if and only if $xf = yf$. Furthermore f uniquely factorises into

$$X \xrightarrow{\pi_{\ker f}} X/_{\ker f} \xrightarrow{\iota} Y,$$

where $\iota$ is injective. This fact is the base of all isomorphism theorems in algebra, and we will state it as a theorem explicitly as follows.

**Theorem 1.5.1**

*Let* $X \xrightarrow{f} Y$ *be a map. Then there is a surjective map* $X \xrightarrow{\pi} X/_{\ker f}$ *and an injective map* $X/_{\ker f} \xrightarrow{\iota} Y$ *such that* $f = \pi\iota$*, or equivalently, the following diagram commutes.*




## 1.6 Linear Orders

A *total linear order* on a set X is a relation $X \xrightarrow{\lambda} X$ such that for all $x, y, z \in X$

- either $y \in x\lambda$ or $x \in y\lambda$

- $y \in x\lambda$ and $x \in y\lambda$ implies $x = y$
- $y \in x\lambda$ and $z \in y\lambda$ implies $z \in x\lambda$.

We write $x \leq y$ for $y \in x\lambda$ for clarity.

We refer to the finite total linear order of size $n$ by $\underline{n}$. One convenient model of $\underline{n}$ is $(\{1, \ldots, n\}, \leq)$ where $\leq$ is the restriction of the order $\leq$ on the natural numbers, which in terms of the definition given in Section 1.2 is the subset relation.

## 1.7 Strings

We take the opportunity here to introduce the notion of *strings* over an alphabet. We will use this notion in Chapter 2 as well as Chapter 4. Strings are a central tool in the theory of computation, one of their main uses being encoding objects. Strings will also be used to demonstrate that computation is a natural domain of the theory of semigroups. On one hand Turing machines, one of the most general models of computation, use strings to encode input, output and intermediate state, on the other hand the set of all strings forms a very natural semigroup. To form strings we first need the basic building blocks, which we call symbols. We choose a collection of symbols and call it an *alphabet*. We allow for infinite alphabets for generality, but most commonly alphabets will be finite.

**Definition 1.7.1**
*Let* $A$ *be an alphabet. A* string *of length* $m$ *over* $A$ *is a map* $\underline{m} \xrightarrow{s} A$.

A convenient and consistent notation for all strings of length $m$ over an alphabet $A$ is now $A^{\underline{m}}$. We denote the set of all strings of any length over $A$ by $A^*$, which includes $\underline{0} \xrightarrow{\varepsilon_A} A$, the empty string.

Given any string $s \in A^*$, we denote by $|s|$ the $n \in \mathbb{N}$ such that $s \in A^{\underline{n}}$ and given $a \in A$ and $s \in A^*$ we denote by $|s|_a$ the cardinality of the set $as^{-1}$, or in other words the number of occurrences of the letter $a$ in the string $s$.

Given two strings $\underline{m} \xrightarrow{s} A$ and $\underline{n} \xrightarrow{t} A$ we define the *concatenation* $st$ *of* $s$ *and* $t$ by the juxtaposition of $s$ and $t$. More formally let $\underline{m} \xrightarrow{i} \underline{m+n}$ and $\underline{n} \xrightarrow{j} \underline{m+n}$ be the embeddings of $\underline{m}$ and $\underline{n}$ into $\underline{m+n}$ such that $ki < lj$ holds for all $k \in \underline{m}$ and $l \in \underline{n}$.

The concatenation of $s$ and $t$ is now the map

$$st : \underline{m+n} \longrightarrow A,\ k \mapsto \begin{cases} ki^{-1}s & k \in \underline{m}i \\ kj^{-1}t & k \in \underline{n}j \end{cases}.$$

If we want to give a string explicitly we use the model $(\{1, \ldots, n\}, \leq)$ of $\underline{n}$ and the notation $s = [\mathbf{a_1} \ldots \mathbf{a_n}]$ for a string $s$ with $is = a_i$ for $i \in \{1, \ldots, n\}$.

Let $s \in A^*$ be a string. We say that $v \in A^*$ is a *prefix of* $s$ if there is a string $x \in A^*$ such that $s = vx$, we say that $v$ is a *suffix of* $s$ if there is $x \in A^*$ such that $s = xv$. We say $v$ is an *infix of* $s$ if there are strings $x \in A^*$ and $z \in A^*$ such that $s = xvz$.

A *substring* $v$ of $s$ is the restriction of $s$ to an arbitrary suborder of $\underline{n}$. For any subword of $s$ we denote by $\mathrm{supp}_s\, v$ the subset of $\underline{n}$ that we restrict to.

## *1.8 Specification*

For every mathematical object there are natural ways of *specifying*, or describing, the object in a formal way. There are a number of ways to specify semigroups, the central object of this work. We choose to use the term *specification* to avoid confusion, since terms like definition, presentation and representation are already widely used for related concepts that do not quite capture the concept of specification.

There are many *types* of specifications for semigroups, for example presentations or transformation representations. We call a type $\mathcal{T}$ of specification *universal* if for any semigroup $S$ there exists a specification of type $\mathcal{T}$.

We will introduce *presentations* in Section 2.7 and *transformation representations* in Section 2.8 of Chapter 2. Most importantly we will show how semigroups can be specified by computational devices, in particular finite state automata in Chapter 8. While the first two types are universal, the latter is not. There are many more types of specification for semigroups, for example matrices over Sumerian's, rings or fields or rewriting systems.

Different types of specification have different strengths and weaknesses. While transformation representations are very suitable for specifying finite semigroups and efficiently doing computations on a computer, presentations are more suited to specify infinite semigroups and make some computations tractable. A particularly important property for computational algebra is that a finite amount of information is needed to specify an infinite object.

# 2

○ ○ ●

# *Semigroups*

We introduce the notions of semigroup theory needed in later chapters. We start with the definitions of semigroups, monoids and groups and the corresponding morphisms in Section 2.1.

Sections 2.2 and 2.4 give further basic definitions connected with semigroups. We will expand on subsets of semigroups in Chapter 3.

In Section 2.5 we define cancellativity, local finiteness and residual finiteness.

The following Section 2.9 treats Green's relations which is ubiquitous in the theory of semigroups and Section 2.6 gives the basic notions of congruences and quotient structures of semigroups. Congruences describe the kernels of semigroup morphisms and the possible quotients of a given semigroup.

Free semigroups and presentations are the topic of Section 2.7, and provide a universal type of specification for semigroups: we encode elements of semigroups as strings over a generating set. Multiplication in the semigroup is then done by concatenating representing strings. A very important task

will be determining equality of elements represented by strings over a generating set. Encoding elements of semigroups as strings over an alphabet will also be a key tool for computatioval considerations.

## 2.1 Semigroups, Monoids and Groups

We define the notions of semigroup and semigroup morphism and extend to monoids and groups.

**Definition 2.1.1**

*A* semigroup *is an algebraic structure* $\langle S, \cdot \rangle$ *where* $S$ *is a set and* $S \times S \xrightarrow{\cdot} S$ *is a binary function such that*

$$(\forall a, b, c \in S)\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

*holds.*

The property that the operation of a semigroup has is called *associativity*, which is one of the properties of the composition of maps. For simplicity we usually denote a semigroup $\langle S, \cdot \rangle$ by $S$, and omit the explicit notation for the binary function, unless we want to emphasise its importance.

The binary function $\cdot$ is often called multiplication or concatenation. We choose infix notation for $\cdot$ because it allows for clean notation. In some cases where multiplication is understood we even leave $\cdot$ out completely and use juxtaposition of elements.

Two special families of semigroups are the family of monoids and the family of groups. Monoids possess a special element, the *identity element*.

**Definition 2.1.2**

*A* monoid $\mathrm{mon}\langle M, \cdot \rangle$ *is a semigroup such that*

$$(\exists e \in M)\,(\forall m \in M)\ (e \cdot m = m) \wedge (m \cdot e = m)$$

*holds.*

Groups are a family of monoids. They have the global property that every element has a uniquely defined inverse element.

**Definition 2.1.3**

*A* group $\langle G, \cdot \rangle$ *is a monoid such that*

$$(\forall m \in M)\,(\exists m' \in M)\ \big(m \cdot m' = e\big) \wedge \big(m' \cdot m = e\big)$$

*holds.*

Let X be a set. The set $\mathcal{T}_X$ of all maps $X \xrightarrow{f} X$ forms a monoid with multiplication being composition of maps, called the *full transformation monoid*. The identity element is the identity map on X.

The set $\mathcal{R}_X$ of all relations $X \xrightarrow{\rho} X$ forms a monoid with multiplication being composition of relations, called the *full relation monoid*. The identity element is the identity relation on X.

The subset of bijective maps in $\mathcal{R}_X$ is the *symmetric group* on X.

With every algebraic structure comes the notion of morphisms as the algebraic tool to compare structures. Semigroup morphisms are defined as follows.

**Definition 2.1.4**

*Let* $\langle S, \circ \rangle$ *and* $\langle T, * \rangle$ *be semigroups. A map* $S \xrightarrow{\varphi} T$ *is a* semigroup morphism *if*

$$\big(\forall s, s' \in S\big)\ (s \circ s')\varphi = (s\varphi) * (s'\varphi).$$

A semigroup morphism $S \xrightarrow{\varphi} T$ is a *monomorphism*, if $f\varphi = g\varphi$ implies $f = g$ for all semigroup morphisms $U \xrightarrow{f} S$ and $U \xrightarrow{g} S$. A semigroup morphism $S \xrightarrow{\varphi} T$ is an *epimorphism* if $\varphi f = \varphi g$ implies $f = g$ for all semigroup morphisms $T \xrightarrow{f} U$ and $T \xrightarrow{g} U$. A semigroup morphism $S \xrightarrow{\varphi} T$ is an *isomorphism* if there exists a semigroup morphism $T \xrightarrow{\varphi^{-1}} S$ such that $\varphi\varphi^{-1} = \iota_S$ and $\varphi^{-1}\varphi = \iota_T$.

If M and N are monoids, a semigroup morphism $M \xrightarrow{\varphi} N$ is a monoid morphism if

$$\mathbf{e}_M\, \varphi = \mathbf{e}_N,$$

where $\mathbf{e}_M$ is the identity element of M and $\mathbf{e}_N$ is the identity element of N. If M and N are groups then $\varphi$ is also a group morphism.

## 2.2 *Elements*

In this section we introduce properties semigroup elements. Let in the following $\langle S, \cdot \rangle$ be a semigroup.

An element $z \in S$ is a *left zero* if

$$(\forall s \in S)\ (zs = z)\,,$$

and $z$ is a *right zero* if

$$(\forall s \in S)\ (sz = z)\,.$$

An element $z \in S$ is a *zero* if $z$ is a left and a right zero. We denote a zero element by $\mathbf{z}$ and note that if a semigroup S contains a zero element then it is unique.

An element $e \in S$ is a *left identity* if

$$(\forall s \in S)\ (es = s)\,,$$

and $e$ is a *right identity* if

$$(\forall s \in S)\ (se = s)\,.$$

An element $e \in S$ is an *identity* if $e$ is a left and a right identity. We note that if S contains an identity it is uniquely defined and we sometimes denote the identity by $\mathbf{e}$.

Although a semigroup S need not contain a zero or an identity, we can simply add elements to S and extend the operation accordingly. Note that we can add a new zero or an identity to a semigroup that already contains a zero or an identity respectively.

We denote by $S^{\mathbf{z}}$ the semigroup $\langle S \cup \{\mathbf{z}\}, \cdot^{\mathbf{z}} \rangle$ where $\mathbf{z} \cdot^{\mathbf{z}} s = s \cdot^{\mathbf{z}} \mathbf{z} = \mathbf{z}$ for all $s \in S^{\mathbf{z}}$ and $s \cdot^{\mathbf{z}} t = s \cdot t$ for all $s$ and $t$ in S.

We denote by $S^{\mathbf{e}}$ the semigroup $\langle S \cup \{\mathbf{e}\}, \cdot^{\mathbf{e}} \rangle$ where $\mathbf{e} \cdot^{\mathbf{e}} s = s \cdot^{\mathbf{e}} \mathbf{e} = s$ for all $s \in S^{\mathbf{e}}$ and $s \cdot^{\mathbf{e}} t = s \cdot t$ for all $s$ and $t$ in $S$.

An element $f$ of $S$ is called *idempotent* if $ff = f$. Certainly identities and zeros are idempotent. If $s$ is an element of a semigroup $S$ then either the subset $\{s^i \mid i \in \mathbb{N}_{>0}\}$ is infinite or there exist minimal $i \in \mathbb{N}_{>0}$ and $k \in \mathbb{N}_{>0}$ such that $s^{i+k} = s^i$. In the first case we say that $s$ has *infinite order* in the second case we say that $s$ has *index* $i$ and *period* $k$.

If for any two elements $x$ and $y$ of $S$ the equation $xy = yx$ holds we say that $x$ and $y$ *commute*.

## 2.3 Subsets

Let $X$ and $Y$ be subsets of a semigroup $S$. We define the *product* $XY$ of $X$ and $Y$ as

$$XY = \{xy \mid x \in X, y \in Y\} \subset S,$$

which is a subset of $S$ again. It follows that for any semigroup $S$ the power set $\hat{S}$ is a semigroup with respect to the operation defined above. This semigroup is called the *power semigroup of* $S$.

In accordance with our convention, in the case of $X$ or $Y$ being singletons we also write $xY$ or $Xy$ instead of $\{x\}Y$ or $X\{y\}$.

For a fixed element $x$ from $S$ we define the map $S \xrightarrow{\rho_x} S$ by

$$\rho_x : S \longrightarrow S,\ s \mapsto sx$$

and the map $S \xrightarrow{\lambda_x} S$ by

$$\lambda_x : S \longrightarrow S,\ s \mapsto xs.$$

By extending $\rho_x$ and $\lambda_x$ to subsets $X \subset S$ we get relations $S \xrightarrow{\rho_X} SX$ and $S \xrightarrow{\lambda_X} S$. The relations $\rho_X^r$ and $\lambda_X^r$ assign to any element $s \in S$ the set $Y \subset S$ of elements $y \in S$ such that there is an $x \in X$ with $s = yx$ or $s = xy$. We can think of this as a generalisation of quotients.

For a monoid $M$ and a subset $X \subset M$ we inductively define for all $n \in \mathbb{N}$ the subsets

- $X^0 = \{\mathbf{e}\}$
- $X^{n+1} = XX^n$

of $M$, and denote the union of the previously defined subsets of $M$ as

$$X^* = \bigcup_{n \in \mathbb{N}} X^n.$$

The set $X^*$ is sometimes called the *Kleene star of* $X$.

If $S$ is a semigroup without an identity element, we can apply the above definition to subsets of $S^{\mathbf{e}}$ and the set

$$X^+ = \bigcup_{n \in \mathbb{N}_{>0}} X^n,$$

is then a subset of $S$.

## 2.4 Subsemigroups

For a given semigroup $S$, any subset $T$ of $S$ which is itself a semigroup is called a *subsemigroup*.

**Definition 2.4.1**

*Let $S$ be a semigroup. A non-empty subset $T \subset S$ is a* subsemigroup of $S$, *denoted $T \leq S$ if $TT \subset T$.*

In group theory the notion of *index* is used to measure the relative size of a subgroup inside a group. The index of a subgroup $H$ of a group $G$ is the number of *cosets* of $H$, the size of the set $\{gH \mid g \in G\}$. In particular if $H = \{\mathbf{e}\}$ then the index of $H$ in $G$ is the size of $G$.

In semigroup theory the definition of index as a measure of relative size of a subsemigroup inside a semigroup is not as clear cut: While cosets partition a group, the set $\{sT \mid s \in S\}$ can be a singleton, for example if $T = \mathbf{z}$. As

a consequence there have been multiple attempts at defining an index of a subsemigroup inside a semigroup. The most straightforward notion of index is the *Rees index*. For a semigroup $S$ and a subsemigroup $T$ the Rees index of $T$ in $S$ is defined to be $|S\backslash T|$.

Given a semigroup property $\mathcal{P}$, a semigroup $S$ and a subsemigroup $T$ of finite index, there are two natural questions to ask.

- If $T$ has the property $\mathcal{P}$, does $S$ have the property $\mathcal{P}$?
- if $S$ has the property $\mathcal{P}$, does $T$ have the property $\mathcal{P}$?

As an example, the following theorem from [Cam+95] shows that both questions can be answered in the positive for finite generation.

**Theorem 2.4.2**

*Let $S$ be a semigroup and let $T \leq S$ be a subsemigroup of $S$ of finite Rees index. Then $S$ is finitely generated if and only if $T$ is finitely generated.*

*Proof.* If $S$ is generated by some finite set $A$ and $T$ is a finite Rees index subsemigroup then the set

$$C = \{xaz \mid x, z \in S^e\backslash T,\ a \in A,\ xa, xaz \in T\}$$

is finite and generates $T$.

If $T$ is generated by some finite set $B$ then certainly $B \cup (S\backslash T)$ is finite and generates $S$. □

We will define a further notion of index in a later section, the notion of *Green index*, which has the property that it generalises the group index.

Some of the concepts of semigroup theory originate in ring theory. This is because the reduct of a ring to multiplication forms a semigroup. One such concept is that of an *ideal*. Unlike ideals in rings, ideals in semigroups do not play the role of kernels of morphisms: With any ideal $I$ of $S$ we can associate a semigroup morphism and therefore a congruence on $S$, but not every semigroup morphism gives rise to an ideal.

**Definition 2.4.3**

*Let* $S$ *be a semigroup. A non-empty subset* $I \subset S$ *of* $S$ *is a* left ideal *if* $SI \subset I$*, it is a* right ideal *if* $IS \subset S$*. The subset* $I$ *is an* ideal *if it is both a left and a right ideal.*

If a semigroup $S$ does not have any ideal $I \subset S$ with $I \neq S$, then $S$ is *simple*. If the only two ideals of $S$ are $\{\mathbf{z}\}$ and $S$ itself, then $S$ is called $0$-*simple*.

If $S$ is a monoid, then there is a special subsemigroup, the group of units, denoted $\mathcal{U}(S)$. It is the largest subsemigroup of $S$ that contains the identity element of $S$ and is a group.

## 2.5 *Properties*

In this section we define properties of semigroups that are more global in nature, namely *cancellativity* and *residual finiteness*.

If a semigroup is cancellative, we can cancel common factors in a product. This is made precise in the following definition.

**Definition 2.5.1**

*A semigroup* $S$ *is* right-cancellative *if*

$$(\forall x, y, a \in S)\ xa = ya \Rightarrow x = y,$$

*it is* left-cancellative *if*

$$(\forall x, y, a \in S)\ ax = ay \Rightarrow x = y,$$

*and it is* cancellative *if it is right- and left-cancellative*

One can also define cancellativity in terms of $\rho_x$ and $\lambda_x$; a semigroup is right-cancellative if and only if $\rho_x$ is injective for all $x$ and it is left-cancellative if and only if $\lambda_x$ is injective for all $x$. All groups are cancellative, and all finite cancellative semigroups are groups. There are also infinite cancellative semigroups that are not groups, for example the free semigroup on a non-empty

set. It is well-known that in a cancellative monoid the complement of the group of units is an ideal.

**Lemma 2.5.2**

*Let* $M$ *be a cancellative monoid and let* $\mathcal{U}(M)$ *be its unit group. Then* $M \setminus \mathcal{U}(M)$ *is an ideal of* $M$.

*Proof.* Let $x \in M \setminus \mathcal{U}(M)$ and $m \in M$. For a contradiction assume that $xm \in \mathcal{U}(M)$. This means that there is $u \in \mathcal{U}(M)$ such that $(xm)u = \mathbf{e}$, which implies $x(mu) = \mathbf{e}$. Now $(mu)x(mu) = (mu)\,\mathbf{e}$, which implies $(mu)x(mu) = \mathbf{e}(mu)$ and since $M$ is assumed to be cancellative, $(mu)x = \mathbf{e}$. Therefore $mu$ is a multiplicative inverse for $x$ in contradiction to the assumption that $x \in M \setminus \mathcal{U}(M)$. □

Residual finiteness reflects in how far a semigroup can be locally approximated by a finite semigroup. All finite semigroups are residually finite, but there are also many infinite semigroups that are residually finite.

**Definition 2.5.3**

*A semigroup* $S$ *is* residually finite *if for any two elements* $a, b$ *in* $S$ *with* $a \neq b$ *there is a finite semigroup* $T$ *and a semigroup morphism* $\varphi : S \to T$ *such that* $a\varphi \neq b\varphi$.

## 2.6 Congruences and Quotients

Congruences on a semigroup $S$ are precisely the equivalence relations on $S$ such that the set of equivalence classes forms a semigroup. In other words congruences on $S$ are in one to one correspondence with quotients of $S$.

**Definition 2.6.1**

*Let* $S$ *be a semigroup. An equivalence relation* $S \xrightarrow{\rho} S$ *is a* left congruence *on* $S$ *if*

$$(\forall s, c \in S)\, c\,(s\rho) \subset (cs)\,\rho,$$

*a* right congruence *on* $S$*, if*

$$(\forall s, c \in S)\,(s\rho)\,c \subset (sc)\,\rho,$$

*and a* congruence *on* $S$ *if it is a left and a right congruence.*

Two natural examples of congruences are the identity relation $S \xrightarrow{\iota_S} S$ and the universal congruence $S \xrightarrow{\mu} S$ where $s\mu = S$ for all $s \in S$.

A semigroup is *congruence-free* if there is no congruence on $S$ other than $\iota_S$ and $\mu$. In group theory groups that are congruence-free are commonly called *simple groups*, and we note that this notion is fundamentally different from the notion of simplicity in semigroup theory. A semigroup can be simple without being congruence-free: every group is simple as a semigroup, but not every group is a simple group. Simple groups are congruence-free as semigroups.

We show that the equivalence classes of a congruence $\rho$ on a semigroup $S$ form a semigroup the *quotient of* $S$ *by* $\rho$ denoted $S/\rho$.

**Lemma 2.6.2**

*Let* $S$ *be a semigroup and let* $S \xrightarrow{\rho} S$ *be a congruence on* $S$*. Then* $S/\rho$ *is a semigroup with multiplication* $(s\rho)\,(t\rho) = (st)\rho$*.*

*Proof.* Let $s\rho$ and $t\rho$ be elements of $S/\rho$ and define $(s\rho)\,(t\rho) = (st)\rho$. We have to show that this operation is well-defined: Let $s$, $s'$, $t$ and $t'$ elements of $S$ with $s' \in s\rho$ and $t \in t\rho$. By the definition of the product of subsets of $S$ and because $S \xrightarrow{\rho} S$ is a right congruence it holds that

$$(s\rho)\,(t\rho) = \bigcup_{x \in t\rho} (s\rho)\,x \supset \left(st'\right)\rho, \tag{2.1}$$

and because $S \xrightarrow{\rho} S$ is a left congruence it holds that

$$(s\rho)\left(t'\rho\right) = \bigcup_{y \in s\rho} y\left(t'\rho\right) \supset \left(s't'\right)\rho. \tag{2.2}$$

Therefore

$$(st)\rho \overset{\text{def}}{=} (s\rho)\,(t\rho) \overset{2.1}{\supset} \left(st'\right)\rho = (s\rho)\left(t'\rho\right) \overset{2.2}{\supset} \left(s't'\right)\rho,$$

and in conclusion $(st)\rho = (s't')\rho$. □

For any semigroup morphism $S \xrightarrow{\varphi} T$ define the following congruence S, the *kernel of* $\varphi$.

**Definition 2.6.3**

*Let* S *and* T *be semigroups and let* $S \xrightarrow{\varphi} T$ *be a semigroup morphism. The* kernel $\ker\,\varphi$ of $\varphi$ *is defined as*

$$\ker\,\varphi : S \longrightarrow S,\ s \mapsto s\varphi\varphi^{-1}.$$

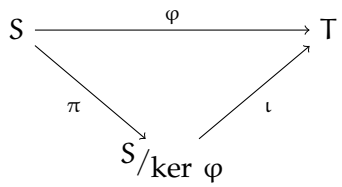
In group theory one usually defines the kernel of a group morphism to be just $\mathbf{e}\,\varphi^{-1}$. This is consistent with our definition since $x \in y\varphi\varphi^{-1}$ if and only if $x\varphi = y\varphi$ which is the case if and only if $(x\varphi)^{-1}(y\varphi) = \mathbf{e}$ and therefore $x^{-1}y$ is in $\mathbf{e}\,\varphi^{-1}$. Given a congruence $\rho$ on a semigroup S the canonical map

$$\pi : S \longrightarrow S/\rho,\ s \mapsto s\rho$$

is a semigroup morphism. The preceding paragraph described what can be summarised as the well-known *first isomorphism theorem for semigroups*.

**Theorem 2.6.4**

*Let* S *and* T *be semigroups and let* $S \xrightarrow{\varphi} T$ *be a semigroup morphism. There exists a surjective morphism* $S \xrightarrow{\pi} S/\ker\,\varphi$ *and an injective morphism* $S/\ker\,\varphi \xrightarrow{\iota} T$ *such that* $\varphi = \pi\iota$*, or equivalently the following diagram commutes.*




*Proof.* We let

$$\pi : S \longrightarrow S/\ker\,\varphi,\ s \mapsto s\rho,$$

so $\pi$ is a surjective semigroup morphism. We further define

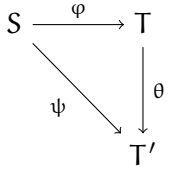
$$\iota : S/\ker\,\varphi \longrightarrow T,\ s\rho \mapsto s\varphi.$$

We have to show that $\iota$ is well-defined and injective. For $s, s' \in S$ it holds that $s' \in s\,(\ker\,\varphi)$ if and only if $s\varphi = s'\varphi$ so $\iota$ is well-defined and injective. To show that the diagram commutes let $s \in S$, then $s\pi\iota = (s\rho)\,\iota = s\varphi$. □

The isomorphism theorem for semigroups is a tool to characterise quotients of a semigroup by surjective morphisms. The *second isomorphism theorem for semigroups* helps comparing quotients of a given semigroup.

**Theorem 2.6.5**

*Let* $S \xrightarrow{\varphi} T$ *be a surjective semigroup morphism and* $S \xrightarrow{\psi} T'$ *be a semigroup morphism. If* $\ker\,\varphi \subset \ker\,\psi$ *then there exists a uniquely defined morphism* $T \xrightarrow{\theta} T'$ *such that* $\psi = \varphi\theta$*, or equivalently the following diagram commutes.*




*Proof.* If we define $T \xrightarrow{\theta} T'$ by $(t\varphi)\theta = t\psi$ then $\theta$ is well-defined and $\psi = \varphi\theta$. □

We briefly touch on the notion of congruence generation, the definition of which is straightforward and standard throughout mathematics.

**Definition 2.6.6**

*Let* $S$ *be a semigroup. Given a set* $R \subset S \times S$ *of pairs the* congruence $\rho(R)$ on $S$ generated by $R$ *is the smallest congruence on* $S$ *that contains* $R$*, or more formally*

$$\rho(R) = \bigcap_{\substack{\sigma \in \mathcal{C}(R) \\ R \subset \sigma}} \sigma,$$

*where* $\mathcal{C}(R)$ *is the family of all congruences on* $S$*.*

We call a congruence $\rho$ *finitely generated* if there is a finite set $R$ with $\rho = \rho(R)$.

## 2.7 Free Semigroups and Presentations

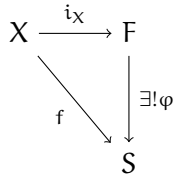
In this section we introduce the notions of a *free semigroup on a set* and a *semigroup presentation*. Free semigroups are in a sense the semigroups with the least structure one can construct from any given set. Semigroup presentations are, next to transformation representations as shown in Theorem 2.8.1, a universal type of specification for semigroups.

While the transformation representations semigroup puts an emphasis on transformations of a set and therefore completely describing the behaviour of an element, semigroup presentations put the emphasis on generators and relations between elements.

We define the notion of a *free semigroup on a set* using the following universal property.

**Definition 2.7.1**

*Let $X$ be a set. A semigroup $F$ is* free on $X$ *if there is a map $X \xrightarrow{i_X} F$ such that for any map $X \xrightarrow{f} S$ there exists a unique semigroup morphism $F \xrightarrow{\varphi} S$ with $i_X\varphi = f$, or equivalently the following diagram commutes.*




We make sure that for any given set $X$ there exists at least one semigroup $F_X$ which is free on $X$. This semigroup has already been introduced in Section 1.7; it is the set of all strings over the set $X$ together with the concatenation operation.

**Lemma 2.7.2**

*Let $X$ be a set. The set $X^+$ of all nonempty strings over $X$ together with concatenation is a free semigroup on $X$.*

*Proof.* It is clear that concatenation of strings is associative, therefore the set $X^+$ together with concatenation is a semigroup. Take $X \xrightarrow{i_X} X^+$ to be the map that takes any element $x \in X$ to the string $[\mathbf{x}]$ of length one. For any $X \xrightarrow{f} S$ define $X^+ \xrightarrow{\varphi} S$ by

$$[\mathbf{x_1} \dots \mathbf{x_n}]\,\varphi = (x_1 f)(x_2 f) \cdots (x_n f).$$

It follows that $i_X \varphi = f$ for all $x \in X$, and for any other morphism $F \xrightarrow{\psi} S$ with this property the equation $\varphi = \psi$ holds. □

Applying the universal property used in Definition 2.7.1, we show that for any cardinal there is only one free semigroup on sets of that cardinality.

**Theorem 2.7.3**

*Let $X$ and $Y$ be sets and let $F_X$ and $F_Y$ be free semigroups on $X$ and $Y$ respectively. Then $F_X \cong F_Y$ if, and only if, there is a bijective map $X \xrightarrow{h} Y$.*

*Proof.* If $F_X \xrightarrow{\varphi} F_Y$ is an isomorphism then $X \xrightarrow{\varphi|_X} Y$ is a bijection.

Conversely, let $X \xrightarrow{h} Y$ be bijective. Then by Definition 2.7.1 there are maps $X \xrightarrow{i_X} F_X$ and $Y \xrightarrow{i_Y} F_Y$ such that for $X \xrightarrow{h i_Y} F_Y$ there is a unique semigroup morphism $F_X \xrightarrow{\varphi} F_Y$ with $i_X \varphi = h i_Y$ and such that for $Y \xrightarrow{h^{-1} i_X} F_X$ there is a unique semigroup morphism $F_Y \xrightarrow{\psi} F_X$ with $i_Y \psi = h^{-1} i_X$.

Since $h$ is bijective $i_X \varphi = h i_Y \Leftrightarrow h^{-1} i_X \varphi = i_Y$, therefore $h^{-1} i_X \varphi \psi = h^{-1} i_X$ and thus $i_X \varphi \psi = i_X$, thus $F_X \xrightarrow{\varphi\psi} F_X$ is a morphism with the property that $i_X \varphi \psi = i_X$. Since $i_X \iota_{F_X} = i_X$ and by uniqueness from Definition 2.7.1, the equality $\varphi\psi = \iota_{F_X}$ holds. Similar reasoning gives $\psi\varphi = \iota_{F_Y}$. We conclude that $\varphi$ and $\psi$ are mutually inverse semigroup morphisms. □

We denote *the* free semigroup on a set $X$ by $X^+$.

A *generating set* for a semigroup $S$ is usually defined to be a *subset* $X$ of $S$ such that all elements of $S$ can be written as a product of elements in $X$. We choose a slightly different definition.

**Definition 2.7.4**

*A semigroup S is generated by a set X if there is a map* $X \xrightarrow{p} S$ *such that* $X^+ \xrightarrow{\pi_X} S$ *is surjective.*

Note that generating sets are separate from the semigroup S, in particular *not* a subset of S. This is important when we encode elements of semigroups by strings over a set and we have to make a clear distinction between strings over a generating set and elements of the semigroup.

Given a semigroup S, a generating set X and $X \xrightarrow{p} S$ we encode elements of S as strings over X, and any string $v \in X^+$ encodes an element of S. Applying $\pi_X$ to any string $v$ in $X^+$ gives us the element of S encoded by $v$. Sometimes we denote the element of S encoded by a string $v \in X^+$ by $\overline{v}$ if the set X and the map p is understood. If there is more than one generating set considered we make this explicit if necessary by writing $v\pi_X$.

We call cross-sections of $\ker \pi$ sets of *normal forms* or sets of *unique representatives*. Given a semigroup S and a generating set X, elements of S can have infinitely many representatives. In general there does not exist an algorithmic method to tell whether two elements of $X^+$ represent the same element of S. In the theory of computation we say that this problem is *undecidable*.

For any semigroup S, the set S itself is a generating set, but generally a much smaller generating set is sufficient. If there is a finite set of generators for a semigroup S, we call S *finitely generated*. If there is a generating set for S that only contains one element we call S *monogenic*.

We now have the necessary tools to define *semigroup presentations*.

**Definition 2.7.5**

*Let X be a set and let* $R \subset X^+ \times X^+$ *be a set of pairs of strings over* X. *The* semigroup generated by X with relations R *is the semigroup* $X^+/\rho(R)$ *denoted by* $\mathrm{sg}\langle X \mid R\rangle$.

Here $\rho(R)$ is the congruence on $X^+$ generated by the images of the elements of R under the morphism $\pi_X$ extended to pairs, that is the smallest congruence

$\rho$ on $X^+$ such that for $(v, w) \in R$ it holds that $v\pi_X \in w\pi_X\rho$. We usually use $v = w$ to denote pairs $(v, w) \in R$

Semigroup presentations allow us to specify a semigroup by choosing a generating set and relations between elements of the semigroup. Conversely, any given semigroup S has a presentation consisting of the set S as generating set and the multiplication table of S as set of relations. In other words, specification by presentations is universal.

Presentations make it algorithmically trivial to multiply two elements: Given two strings $v$ and $w$ over a generating set X for S, a representative for $(v\pi_X w\pi_X)$ is $vw$. It was already mentioned earlier that presentations make it algorithmically very hard in general to tell whether two strings $v$ and $w$ over X represent the same element of S.

We say that S is *finitely presented* if there *exists* a presentation $\langle X, R\rangle$ with X and R finite such that $S \cong \langle X, R\rangle$.

We will give examples of finitely generated and finitely presented semigroups in Chapter 5.

Analogously to the above we can define *monoid presentations*.

**Definition 2.7.6**

*Let* X *be a set and let* $R \subset X^* \times X^*$ *be a set of pairs of strings over* X. *The* monoid generated by X with relations R *is the monoid* $X^*/_{\rho(R)}$ *denoted by* $\mathrm{mon}\langle X \mid R\rangle$.

Here $\rho(R)$ is the congruence on $X^*$ generated by the images of the elements of R under the morphism $\pi_X$ extended to pairs, that is the smallest congruence $\rho$ on $X^*$ such that for $(v, w) \in R$ it holds that $v\pi_X \in w\pi_X\rho$.

Every monoid now has a semigroup presentation and a semigroup presentation. Monoid presentations make the identity element implicit by asserting that the empty string is the canonical representative for the identity.

Given a monoid presentation $\mathrm{mon}\langle X \mid R\rangle$ for a monoid M, we can give a semigroup presentation for M by adding a generator $e$ for the identity to X and relations $([\mathbf{ee}], [\mathbf{e}])$ and $([\mathbf{ex}], [\mathbf{x}])$ and $([\mathbf{xe}], [\mathbf{x}])$ for every $x \in X$. Given a

semigroup presentation $\mathrm{sg}\langle X \mid R\rangle$ for a monoid $M$ we find a representative $v \in X^+$ for the identity element of $M$ and add the relation $(v, \varepsilon)$ to $R$ and this yields a monoid presentation. Note however that it might not be constructive finding a representative for the identity element of $M$.

## 2.8 Transformation Representations

With transformation representations we introduce a second universal means of specifying semigroups. Cayley's theorem from group theory demonstrates how every group can be represented as a group of permutations of a set, and hence is isomorphic to a subgroup of a symmetric group. There is an equivalent theorem to Cayley's theorem in semigroup theory.

**Theorem 2.8.1**

*Let $S$ be a semigroup. Then $S$ is isomorphic to a subsemigroup of $\mathcal{T}_{S^e}$.*

*Proof.* The map

$$\rho_x : S^e \longrightarrow S^e,\ s \mapsto sx$$

is an element of $\mathcal{T}_{S^e}$ for all $x \in S$ and the map

$$\varphi : S \longrightarrow \mathcal{T}_{S^e},\ x \mapsto \rho_x$$

is a semigroup morphism. It is injective, since

$$x\varphi = y\varphi \Rightarrow \rho_x = \rho_y \Rightarrow s\rho_x = s\rho_y \text{ for all } s \in S^e \tag{2.3}$$

$$\Rightarrow \mathbf{e}x = \mathbf{e}y \Rightarrow x = y \tag{2.4}$$

Note that it is essential in the above proof to use $\mathcal{T}_{S^e}$ and not $\mathcal{T}_S$ to ensure injectivity of $\varphi$ if $S$ is not a monoid. Subsemigroups of $\mathcal{T}_X$ are called *transformation semigroups* and for a given semigroup $S$ a morphism $S \xrightarrow{\varphi} \mathcal{T}_X$ for some set $X$ is called a *transformation representation of* $S$. A transformation representation is called *faithful* if it is injective. Specifying semigroups as transformation semigroups is often useful in computer algebra.

Any given semigroup $S$ can have many different transformation representations. As a means of comparing transformation semigroups we introduce equivalence of transformation semigroups.

**Definition 2.8.2**

*Let $X$ and $Y$ be sets, and let $S \leq \mathcal{T}_X$ and $T \leq \mathcal{T}_Y$ be two transformation semigroups. Then $S$ and $T$ are called* equivalent *if there is an isomorphism $S \xrightarrow{\varphi} T$ and a bijection $X \xrightarrow{f} Y$ such that*

$$(\forall s \in S)\, \forall x \in X \;\; (xf)\,(s\varphi) = (xs)\,f$$

## 2.9 *Green's Relations*

*Green's relations* are a very pervasive notion in the theory of semigroups and were introduced by Green in [Gre51]. Green's relations relate elements of semigroups by comparing the principal ideals they generate. Since we also want to define the Green index, which was introduced by Gray and Ruskuc in [GR08], we start with a slightly more general definition, *Green's relations relative to a subsemigroup*. The notion of relative Green's relations was introduced by A.D. Wallace in [Wal63]. In later sections we will almost exclusively be considering the classical Green's relations.

**Definition 2.9.1**

*Let $S$ be a semigroup and let $T$ be a subsemigroup of $S$.* Green's relations relative to $T$ *on $S$ are equivalence relations on $S$ defined as follows*

- $\mathcal{R}^T : S \longrightarrow S,\ a \mapsto aT^e$
- $\mathcal{L}^T : S \longrightarrow S,\ a \mapsto T^e a$
- $\mathcal{J}^T : S \longrightarrow S,\ a \mapsto T^e a T^e$
- $\mathcal{H}^T : S \longrightarrow S,\ a \mapsto a\mathcal{R}^T \cap a\mathcal{L}^T$
- $\mathcal{D}^T : S \longrightarrow S,\ a \mapsto a\mathcal{R}^T\mathcal{L}^T$

For $S = T$ these are known as *Green's relations*. If we are talking about Green's relations we will leave out the superscript.

The *Green index* of a subsemigroup $T$ in $S$ was introduced by Gray and Ruskuc in [GR08]. It is defined as the number of $\mathcal{H}^T$-classes in $S\backslash T$, or

$$[S : T]_G = \left| {}^{(S\backslash T)}/_{\mathcal{H}^T} \right| + 1.$$

If a subsemigroup $T$ of a semigroup $S$ has finite Rees index, then $T$ also has finite Green index. The converse is not true: If $T$ has finite Green index it need not have finite Rees index in general, as the example in 5.7 shows. If $T$ has finite Green index in $S$ and all $\mathcal{H}^T$-classes in $S\backslash T$ are finite, then $T$ also has finite Rees index.

We will need the following properties of the $\mathcal{H}$ relation: If an $\mathcal{H}-$class $H$ of a semigroup $S$ contains an idempotent, then $H$ is a subgroup of $S$. Even if an $\mathcal{H}$-class $H$ is not a group, there exists a permutation group that acts on the set $H$ in a very natural way. This was discovered by Schützenberger. We give the necessary definitions and a theorem first discovered by Schützenberger and published in [Sch57].

We first introduce a notion which is familiar from group theory.

**Definition 2.9.2**

*Let $S$ be a semigroup and let $X$ be a subset of $S$. The* right stabiliser $\mathrm{RStab}_{S^e}(X)$ *of $X$ is defined to be the submonoid*

$$\mathrm{RStab}_{S^e}(X) = \{s \in S^e \mid Xs \subset X\}$$

*of $S^e$.*

For a semigroup $S$ and a $\mathcal{H}$-class $H$ consider the right stabiliser $\mathrm{RStab}_S(H)$. We define a congruence on $\mathrm{RStab}_S(H)$ by

$$x \sim y \text{ if and only if } hx = hy \text{ for some } h \in H,$$

and call the quotient ${}^{\mathrm{RStab}_S(H)}/_{\sim}$ the *transition monoid* or *Schützenberger monoid* of $\mathrm{RStab}_S(H)$, denoted by $\mathcal{T}_S(H)$.

The following theorems summarise the properties of the Schützenberger monoid of an $\mathcal{H}-$class $H$ that we are interested in. Relevant proofs can be found in [Sch57] and [Lal79, Ch. 3].

**Theorem 2.9.3**

*Let $S$ be a semigroup and let $H$ be a $\mathcal{H}-$class. Then the following statements hold.*

- *The transition monoid $\mathcal{T}_S(H)$ of the right stabiliser $\mathrm{RStab}_S(H)$ is a group of permutations of $H$ and for $h \in H$ the stabiliser $\mathrm{RStab}_{\mathcal{T}_S(H)}(h)$ is trivial.*
- *If $H$ and $H'$ are two $\mathcal{H}$-classes contained in the same $\mathcal{D}$-class, then $\mathcal{T}_S(H)$ and $\mathcal{T}_S(H')$ are equivalent permutation groups.*
- *If $H$ is a maximal subgroup of $S$, then $H$ and $\mathcal{T}_S(H)$ are isomorphic.*

A corollary of the above theorem is that for any $\mathcal{H}$-class $H$ it holds that $|\mathcal{T}_S(H)| = |H|$.

A finiteness condition for semigroups is if $\mathcal{J} = \mathcal{D}$, that is the relations $\mathcal{J}$ and $\mathcal{D}$ coincide.

Stability was introduced and studied by Koch and Wallace in [KW57] for topological semigroups, and in the same paper Koch and Wallace also show that in stable semigroups $\mathcal{J} = \mathcal{D}$. See also [CP67, §6.6] for a further reference on stability.

**Definition 2.9.4**

*Let $S$ be a semigroup. Then $S$ is called* left stable *if for $a$ and $b$ in $S$ the inclusion $Sa \subset Sab$ implies $Sa = Sab$. The semigroup $S$ is called* right stable *if for all $a$ and $b$ in $S$ the inclusion $aS \subset baS$ implies $aS = baS$. The semigroup $S$ is called* stable *if $S$ is right stable and left stable. $S$ is called* weakly stable *if $S^e$ is stable.*

We note that if $S$ is stable, then so is $S^e$, and therefore every stable semigroup is also weakly stable. The converse does not hold in general and a few counterexamples can be found in [OCa69].

Koch and Wallace also show in [KW57] that in a weakly stable semigroup it holds that $\mathcal{J} = \mathcal{D}$. We first start by proving a technical lemma.

**Lemma 2.9.5**

*Let $S$ be a weakly stable semigroup. For all $a$ and $b$ from $S$ with $a\mathcal{J} = b\mathcal{J}$ it holds that $S^e a \subset S^e b$ implies $S^e a = S^e b$, and $aS^e \subset bS^e$ implies $aS^e = bS^e$.*

*Proof.* Let $S$ be a weakly stable semigroup and let $a$ and $b$ be elements of $S$ with $a\mathcal{J} = b\mathcal{J}$. There exist $x$ and $z$ in $S^e$ with $b = xaz$. If additionally $S^e a \subset S^e b$, then

$$S^e a \subset S^e b = S^e xaz \subset S^e az.$$

It follows by left stability of $S$ that $S^e a = S^e az$, and therefore $S^e a = S^e b$. An analogous proof holds for $aS^e \subset bS^e$. □

Using the above lemma we can prove the desired theorem.

**Theorem 2.9.6**

*Let $S$ be a weakly stable semigroup. It holds that $\mathcal{J} = \mathcal{D}$.*

*Proof.* We note that in any semigroup $\mathcal{D} \subset \mathcal{J}$ holds. Let $S$ be a weakly stable semigroup and let $a$ and $b$ be in $S$ with $a\mathcal{J} = b\mathcal{J}$. The goal is to show that $a\mathcal{D} = b\mathcal{D}$, which by definition of $\mathcal{D}$ is to prove the existence of an element $c$ in $S^e$ such that $a\mathcal{R} = c\mathcal{R}$ and $c\mathcal{L} = b\mathcal{L}$.

Since $a\mathcal{J} = b\mathcal{J}$, there are elements $x$ and $z$ in $S^e$ such that $a = xbz$. We note that $xb\mathcal{J} = b\mathcal{J}$. It holds that $S^e xb \subset S^e b$ and therefore $S^e xb = S^e b$, hence $xb\mathcal{L} = b\mathcal{L}$. It also holds that

$$aS^e = xbzS^e \subset xbS^e$$

and therefore $aS^e = xbS^e$, by application of Lemma 2.9.5. Hence $a\mathcal{R} = xb\mathcal{R}$. □

## 2.10 Product Constructions

We define the notions of direct product, free product, and zero union of semigroups. For the direct product and the free product we use the universal

properties from category theory. We skip proofs of existence and uniqueness as they can be found in standard literature about semigroups.

**Definition 2.10.1**

*Let $S_1$ and $S_2$ be semigroups. A semigroup $S$ is a* direct product *of $S_1$ and $S_2$, usually denoted by $S_1 \times S_2$, if there are morphisms $S \xrightarrow{\pi_i} S_i$ for $i \in \{1,2\}$ such that for any pair $T \xrightarrow{\varphi_i} S_i$ of morphisms there exists a unique morphism $T \xrightarrow{\varphi} S$ with $\varphi\pi_i = \varphi_i$.*

The following theorem will help us classify semigroups with polyrational word problem in Chapter 9. This is known in the more general context of algebraic structures. We state it for semigroups.

**Theorem 2.10.2**

*Let $S$ be a semigroup and let $S \xrightarrow{\rho_1} S$ and $S \xrightarrow{\rho_2} S$ be congruences on $S$ such that $\rho_1 \cap \rho_2 = \iota_S$ and such that the smallest congruence that contains $\rho_1$ and $\rho_2$ is the universal congruence $S \xrightarrow{\mu_S} S$. Then*

$$S \cong \left(S/\rho_1\right) \times \left(S/\rho_2\right).$$

*Proof.* We use Definition 2.10.1. We note that $S \cong S/(\rho_1 \cap \rho_2)$ by the assumption that $\rho_1 \cap \rho_2 = \iota_S$. Since $\rho_1 \subset (\rho_1 \cap \rho_2)$ and $\rho_2 \subset (\rho_1 \cap \rho_2)$ the second isomorphism theorem ensures the existence of unique surjective morphisms $S \xrightarrow{\pi_1} S/\rho_1$ and $S \xrightarrow{\pi_2} S/\rho_2$.

Let $T \xrightarrow{\varphi_1} S/\rho_1$ and $T \xrightarrow{\varphi_2} S/\rho_2$ be morphisms. We define the morphism $T \xrightarrow{\varphi} S$ by $t\varphi = s$ such that $s\pi_1 = t\varphi_1$ and $s\pi_2 = t\varphi_2$.

We first show that $\varphi$ is a uniquely defined morphism of semigroups. From the definition of $\varphi$ it follows that $s \in t\varphi_1\pi_1^{-1}$ and that $s \in t\varphi_2\pi_2^{-1}$. This means that $s\rho_1 = s\rho_2$. By the assumption that $\rho_1 \cap \rho_2 = \iota_S$, it follows that if $\varphi$ is defined, then it is uniquely defined. By the assumption that the smallest congruence that contains $\rho_1$ and $\rho_2$ is the universal congruence, it follows that

there is at least one $s$ in the intersection of congruence classes of $\rho_1$ and $\rho_2$. It follows that $\varphi$ is a uniquely defined morphism, since $\pi_1$ and $\pi_2$ are uniquely defined morphisms. To conclude the proof, by the definition of $\varphi$ it holds that $\varphi\pi_1 = \varphi_1$ and $\varphi\pi_2 = \varphi_2$. By the definition of direct products it follows that $S$ is isomorphic to the direct product of $S/\rho_1$ and $S/\rho_2$. □

The above theorem can be generalised in the following way, which will be useful in the context of polyrational word problems in Chapter 9. The proof follows by applying the isomorphism theorems.

**Theorem 2.10.3**

*Let $S$ be a semigroup and let $\rho_1$ and $\rho_2$ be congruences such that the smallest congruence on $S/(\rho_1 \cap \rho_2)$ that contains the congruences $\rho_1$ and $\rho_2$ is the universal congruence. Then*

$$S/(\rho_1 \cap \rho_2) \cong S/\rho_1 \times S/\rho_2$$

The free product in the category of semigroups is defined as follows. Again, it exists and it is unique. We can in the same way define the free product in the category of monoids, and note that the free product of two monoids in the category of semigroups is *not* isomorphic to the free product of two monoids in the category of monoids.

**Definition 2.10.4**

*Let $S_1$ and $S_2$ be semigroups. A semigroup $S$ is the* semigroup free product *of $S_1$ and $S_2$ if there are morphisms $S_i \xrightarrow{\iota_i} S$ for $i \in \{1,2\}$ such that for any pair $S_i \xrightarrow{\varphi_i} T$ there exists a uniquely defined morphism $S \xrightarrow{\varphi} T$ such that $\iota_i\varphi = \varphi_i$ for $i \in \{1,2\}$.*

The last product construction we introduce is a bit more semigroup specific, it is the *zero union*.

**Definition 2.10.5**

*Let* $U$ *be a semigroup with zero. If there exist subsemigroups* $S$ *and* $T$ *such that* $S \cap T = \emptyset$ *and* $st = z = ts$ *for all* $s \in S$ *and for all* $t \in T$ *then* $U$ *is a* zero union *of* $S$ *and* $T$*, denoted by* $S \cup_z T$.

# 3

○ ⊙ ●

# *Subsets of Semigroups*

For any semigroup S we introduce the families of recognisable, rational and extended rational subsets of S and establish a hierarchy for finitely generated semigroups.

The family of *recognisable subsets* of a semigroup S is introduced in Section 3.2 and are specified by finite quotients of S. The families of *rational subsets* and *extended rational subsets* are introduced in Section 3.3 and Section 3.5 respectively and rely on a specification by formulas. All the named families are of interest in the theory of computation. It is *Kleene's Theorem* which identifies the families of recognisable, rational and extended rational subsets of free semigroups.

We then define relations on semigroups that are *recognisable*, *rational* or *polyrational*, these will become the point of focus in Chapter 8 and 9

## 3.1 The Syntactic Congruence

We associate with every subset $X$ of a semigroup $S$ a congruence, the *syntactic congruence* of $X$ in $S$. This congruence is particularly important for recognisable subsets introduced in Section 3.2.

**Definition 3.1.1**

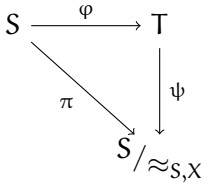
*Let $S$ be a semigroup and let $X \subset S$ be a subset of $S$. Then the* syntactic congruence of $X$ on $S$ *is defined by*

$$s \approx_{S,X} t \text{ if and only if } \forall x, z \in S^1 \; xsz \in X \Leftrightarrow xtz \in X.$$

The syntactic congruence is the largest congruence on $S$ such that the quotient semigroup can still separate $X$ from its complement.

**Theorem 3.1.2**

*Let $S$ be a semigroup and let $X$ be a subset of $S$. If $S \xrightarrow{\varphi} T$ is a surjective semigroup morphism with $X = F\varphi^{-1}$ for some $F \subset T$ then there exists a morphism $T \xrightarrow{\psi} S/_{\approx_{S,X}}$ with $\varphi\psi = \pi_{\approx_{S,X}}$, or equivalently the following diagram commutes.*




*Proof.* To show the existence of $\psi$ and that the diagram commutes, we have to check the hypothesis of Theorem 2.6.5, that is we show that $\ker\varphi \subset \ker\pi$.

$$\begin{aligned} t \in s \ker\varphi &\Rightarrow s\varphi = t\varphi && (3.1)\\ &\Rightarrow \forall x, z \in S^1 xsz\varphi \in F \Leftrightarrow xtz\varphi \in F && (3.2)\\ &\Rightarrow \forall x, z \in S^1 xsz \in X \Leftrightarrow xtz \in X && (3.3)\\ &\Rightarrow t \in s \ker\pi && (3.4) \end{aligned}$$

## 3.2 *Recognisable Subsets*

The notion of recognisable subset can be seen as a generalisation of residual finiteness to subsets, and therefore recognisability is a finiteness condition for subsets of a semigroup.

In Section 3.4 we will show that the recognisable subsets of a free semigroup are exactly the regular languages. These are precisely the sets of strings that are the behaviour of a finite A-automaton. Therefore one can think of recognisability as an algebraic characterisation of regular languages.

We define the family $\mathrm{Rec}\, S$ of *recognisable subsets* of a semigroup $S$ by the following definition of a recognisable subset of $S$.

**Definition 3.2.1**

*Let $S$ be a semigroup. A subset $X \subseteq S$ is* recognisable *if there is a semigroup morphism $S \xrightarrow{\varphi} T$ where $T$ is a finite semigroup and such that $X = F\varphi^{-1}$ for some subset $F \subset T$.*

Note that without loss of generality we can assume $\varphi$ in the above definition to be surjective. It also follows directly from the above definition that the empty subset $\emptyset$ and the subset $S$ of $S$ are recognisable.

We will discuss a few important properties of recognisable subsets of a given semigroup $S$, first of all their behaviour under morphisms. Recognisability is preserved under preimages of morphisms, but not necessarily preserved under morphisms.

**Lemma 3.2.2**

*Let $S \xrightarrow{\varphi} S'$ be a semigroup morphism. If $Y$ is a recognisable subset of $S'$ then $Y\varphi^{-1}$ is a recognisable subset of $S$.*

*Proof.* Let $S \xrightarrow{\varphi} S'$ be a semigroup morphism and let $Y$ be in $\mathrm{Rec}\, S'$. Then there is a semigroup morphism $S' \xrightarrow{\psi} T$, where $T$ is finite, such that $Y = F\psi^{-1}$. It follows that $Y\varphi^{-1} = F\psi^{-1}\varphi^{-1}$ so $\varphi\psi$ recognises $Y\varphi^{-1}$. □

We show that the family of recognisable subsets of a semigroup forms a Boolean algebra.

**Lemma 3.2.3**

*Let $S$ be a semigroup.*

- *If* $X \in \operatorname{Rec} S$ *then* $S\backslash X \in \operatorname{Rec} S$.
- *If* $X_1, X_2 \in \operatorname{Rec} S$ *then* $X_1 \cup X_2 \in \operatorname{Rec} S$.
- *If* $X_1, X_2 \in \operatorname{Rec} S$ *then* $X_1 \cap X_2 \in \operatorname{Rec} S$.

*It follows that* $\operatorname{Rec} S$ *is a Boolean algebra.*

*Proof.* Let $X \in \operatorname{Rec} S$, which by definition means that there is a surjective semigroup morphism $S \xrightarrow{\varphi} T$ with $T$ finite and $F \subset T$ such that $X = F\varphi^{-1}$. Then $(T\backslash F)\,\varphi^{-1} = S\backslash X$ and therefore $S\backslash X \in \operatorname{Rec} S$.

Let $X_1, X_2 \in \operatorname{Rec} S$. There are surjective morphisms $S \xrightarrow{\varphi_1} T_1$ and $S \xrightarrow{\varphi_2} T_2$ with $T_1$ and $T_2$ finite and sets $F_1 \subset T_1$ and $F_2 \subset T_2$ such that $X_1 = F_1\varphi_1^{-1}$ and $X_2 = F_2\varphi_2^{-1}$. Define

$$\varphi : S \longrightarrow T_1 \times T_2,\ s \mapsto (s\varphi_1, s\varphi_2),$$

and

$$F = \{(t_1, t_2) \in T_1 \times T_2 \mid t_1 \in F_1 \text{ or } t_2 \in F_2\}.$$

Consequently $s \in F\varphi^{-1}$ if and only if $s \in F_1\varphi^{-1}$ or $s \in F_2\varphi^{-1}$ so $\varphi$ recognises $X_1 \cup X_2$.

The fact that $X_1 \cap X_2 \in \operatorname{Rec} S$ follows by applying DeMorgan's laws. □

The following lemma is known as Ogden's iteration lemma. It was first proven by William Ogden in [Ogd68] for context-free languages. The following theorem is an adaption of Ogden's ideas to regular languages, with additional help from the version and proof given in [Ber79]. This lemma is a strengthening of the well-known pumping lemma, or iteration lemma, in

automata theory. We prove it in the context of recognisable subsets of the free semigroup on a finite set. Ogden's iteration lemma is one of the most important tools in our work in later chapters.

**Theorem 3.2.4**

*Let $A$ be a finite alphabet and let $X$ be a recognisable subset of $A^+$. Then there exists a natural number $n_0$ such that for any element $s \in A^+$ and any choice $M \subset \underline{|s|}$ of marked positions with $|M| \geq n_0$ the element $s$ admits a factorisation $s = xuy$ with $x$, $u$ and $y \in A^*$ such that the following holds.*

- *There is at least one and at most $n_0$ marked positions in $u$.*
- $xu^iy \in X$ *for all* $i \in \mathbb{N}$ *if and only if* $xuy \in X$.

*Proof.* Let $X$ be a recognisable subset of $A^+$. This means that there is a morphism $A^+ \xrightarrow{\varphi} T$ with $T$ finite, and $F \subset T$ such that $X = F\varphi^{-1}$. Let $n_0 = |T|$ and

$$w = a_1 a_2 \dots a_k$$

be an element of $A^+$ and let $M = \{i_1, i_2, \dots, i_n\} \subset \underline{k}$ be a set of at least $n_0$ marked positions. Define a factorisation

$$w = w_0 w_1 \dots w_{n_0+1}$$

of $w$ by

$$\begin{aligned} w_0 &= a_1 \dots a_{i_1-1} \\ w_1 &= a_{i_1} \\ w_j &= a_{i_{j-1}+1} \dots a_{i_j} \text{for } 2 \leq j \leq n_0 \\ w_{n_0+1} &= a_{i_{n_0}+1} \dots a_n \end{aligned}$$

and elements $s_j \in T$ by $s_0 = w_0\varphi$ and $s_{j+1} = s_j\,(w_{j+1})\,\varphi$ for $1 \leq j \leq n_0$. Since $|T| = n_0$ there exist two indices $j_1$ and $j_2$ such that $s_{j_1} = s_{j_2}$, and therefore for

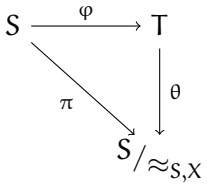
$$x = w_0 w_1 \dots w_{j_1},\ u = w_{j_1+1} \dots w_{j_2},\ \text{ and } \ y = w_{j_2+1} \dots w_{n_0+1} \tag{3.5}$$

it holds that $(xy)\,\varphi = \left(xu^i y\right)\varphi$ for all $i \in \mathbb{N}_{>0}$ and therefore $xy \in X$ if and only if $xu^i y \in X$. □

For any $X \in \operatorname{Rec} S$ the canonical morphism $S \xrightarrow{\pi} S/_{\approx_{S,X}}$ recognises $X$ and $S/_{\approx_{S,X}}$ is minimal in the sense that it is a quotient of any $T$ where $S \xrightarrow{\varphi} T$ recognises $X$. This also shows that a subset of $S$ is recognisable if and only if its syntactic quotient is finite.

**Theorem 3.2.5**

*Let $S$ be a semigroup and let $X \in \operatorname{Rec} S$. Then $S \xrightarrow{\pi} S/_{\approx_{S,X}}$ recognises $X$ and for any morphism $S \xrightarrow{\varphi} T$ that recognises $X$ there exists a morphism $T \xrightarrow{\theta} S/_{\approx_{S,X}}$ such that $\pi = \varphi\psi$, or equivalently the following diagram commutes.*




*Proof.* We first show that $S \xrightarrow{\pi} S/_{\approx_{S,X}}$ recognises $X$. For this let $F$ be the image of $X$ under the relation $\approx_{S,X}$. We show that $X = F\pi^{-1}$. If $x \in X$ then $x\pi \in F$ and therefore $x \in F\pi^{-1}$. Conversely, let $s \in F$ then there is $t \in s$ with $t \in X$, and by the definition of $\approx_{S,X}$ this implies that $s\pi^{-1} \subset X$.

The rest of the proof follows from Theorem 3.1.2. □

## 3.3 Rational Subsets

Rationality also is a finiteness condition on subsets of a semigroup in the sense that there is an inductive specification for each set of this class. Inductive definitions are used in formal logic and recursion theory. More specifically, we will define by induction the *syntax* and the *semantics* of expressions. The syntax is the definition of *rational expressions* and *extended rational expressions*, and the semantics assign to every rational expression a subset of a semigroup. We call the family of subsets thus defined the family of *rational subsets of* $S$.

In the previous section, we stated that that recognisability is an algebraic way to specify regular languages. Rational expressions are the formal logic approach to specify regular languages.

**Definition 3.3.1**

*Let* $X$ *be a set. The set* $\mathrm{RatExp}\, X$ *of* rational expressions over $X$ *is inductively defined as follows.*

- *The expression* $\lambda$ *is an element of* $\mathrm{RatExp}\, X$,
- *any element* $x \in X$ *is an element of* $\mathrm{RatExp}\, X$,
- *if* $\alpha$ *is in* $\mathrm{RatExp}\, X$, *then the expression* $\alpha^+$ *is in* $\mathrm{RatExp}\, X$,
- *if* $\alpha$ *and* $\beta$ *are elements of* $\mathrm{RatExp}\, X$, *then the expression* $(\alpha\beta)$ *is an element of* $\mathrm{RatExp}\, X$,
- *if* $\alpha$ *and* $\beta$ *are elements of* $\mathrm{RatExp}\, X$, *then the expression* $(\alpha \cup \beta)$ *is an element of* $\mathrm{RatExp}\, X$.

Given a semigroup $S$ and a map $X \xrightarrow{f} S$, we assign to each rational expression a subset of $S$ by inductively defining the map $[\![]\!]_f$. Usually we will choose $X = S$ and $f$ to be the identity map $\iota S$. If $S$ is finitely generated, we can do with $X$ being a generating set for $S$.

**Definition 3.3.2**

*Let* $X$ *be a set,* $S$ *be a semigroup and* $X \xrightarrow{f} S$ *be a map. The map* $[\![]\!]_f$ *is inductively defined as follows.*

- $[\![\lambda]\!]_f = \emptyset$,
- $[\![x]\!]_f = \{xf\}$,
- $[\![\alpha^+]\!]_f = [\![\alpha]\!]_f^+$,
- $[\![\alpha \cup \beta]\!]_f = [\![\alpha]\!]_f \cup [\![\beta]\!]_f$,
- $[\![\alpha\beta]\!]_f = [\![\alpha]\!]_f\, [\![\beta]\!]_f$.

We denote the family of all rational subsets of $S$ with respect to $X$ and $f$ by $\operatorname{Rat} S_f$. Note that $f$ implicitly defines the set $X$. If $S$ is generated by $X \xrightarrow{f} S$ and $Y \xrightarrow{g} S$ is another generating set for $S$, then $\operatorname{Rat} S_f = \operatorname{Rat} S_g$. This can easily be seen in Definition 3.3.2.

Rational subsets behave dually to recognisable subsets under morphisms: they are preserved under morphism, but not under taking preimages.

**Lemma 3.3.3**
*Let $S \xrightarrow{\varphi} S'$ be a semigroup morphism. If $X$ is a rational subset of $S$ then $X\varphi$ is a rational subset of $T$.*

*Proof.* This follows by induction over the definition of rational expressions, the map $[\![]\!]$ and from the fact that $\varphi$ is a map and a morphism. □

Given a surjective semigroup morphism $S \xrightarrow{\varphi} T$ and a rational subset $Y$ of $T$ we can prove the existence of a rational subset of $X$ of $S$ such that $Y = X\varphi$.

**Lemma 3.3.4**
*Let $S \xrightarrow{\varphi} T$ be a surjective semigroup morphism. If $Y \in \operatorname{Rat} T$ then there exists $X \in \operatorname{Rat} S$ with $Y = X\varphi$.*

*Proof.* Consider the family $R \subset \hat{T}$ with $Y \in R$ if and only if there is $X \in \operatorname{Rat} S$ with $Y = X\varphi$. We show by induction that $R \supset \operatorname{Rat} T$.

- $\emptyset \in R$, because $\emptyset\varphi = \emptyset$.
- Since $\varphi$ is surjective, for all $t \in T$ there is $s \in S$ with $t = s\varphi$, therefore $\{t\} \in R$.
- If $Y$ is an element of $R$, then there is $X \in \operatorname{Rat} S$ with $Y = X\varphi$, and therefore $Y^+ = X^+\varphi$ is an element of $R$.
- If $Y$ and $Y'$ are elements of $R$, then there are $X$ and $X'$ in $\operatorname{Rat} S$ with $Y = X\varphi$ and $Y' = X'\varphi$, therefore $Y \cup Y' = (X \cup X')\,\varphi$ is an element of $R$.

- If $Y$ and $Y'$ are elements of $R$, then there are $X$ and $X'$ in $\operatorname{Rat} S$ with $Y = X\varphi$ and $Y' = X'\varphi$, therefore $YY' = (XX')\,\varphi$ is an element of $R$. □

We also note that there is a natural definition of rational expressions for monoids $M$ that include a rational expression $\epsilon$ with $[\![\epsilon]\!]_f = \varepsilon$ and a rational expression $\alpha^*$ with $[\![\alpha^*]\!]_f = [\![\alpha]\!]_f^*$.

## 3.4 Kleene's Theorem

*Kleene's Theorem*, named after its discoverer Stephen Kleene [Kle56], identifies rational and recognisable subsets of free semigroups. The technique used to prove that $\operatorname{Rec} A^+ \subset \operatorname{Rat} A^+$ has been applied in more general settings and is known today as the Kleene-Floyd-Warshall method.

**Theorem 3.4.1**
*Let $A$ be a finite alphabet. Then* $\operatorname{Rec} A^+ = \operatorname{Rat} A^+$.

A semigroup in which Kleene's theorem holds is called a Kleene semigroup. A natural task is now to characterise the class of all Kleene semigroups, which is an open research problem.

Applying Kleene's theorem and properties of rational and recognisable subsets we can prove the following theorem for finitely generated semigroups, which was proven by McKnight [McK64].

**Theorem 3.4.2**
*Let $S$ be a finitely generated semigroup. Then* $\operatorname{Rec} S \subset \operatorname{Rat} S$.

*Proof.* Let $A$ be a finite generating set for $S$. Then $A^+ \xrightarrow{\pi} S$ is surjective and for any recognisable subset $X$ of $S$ the preimage $X\pi^{-1}$ is a recognisable subset of $A^+$. By Kleene's theorem 3.4.1 the set $X\pi^{-1}$ is also a rational subset of $A^+$ and therefore $X = X\pi^{-1}\pi$ is a rational subset of $S$. □

For semigroups that are not finitely generated, Theorem 3.4.2 does not hold. Furthermore, the inclusion $\operatorname{Rec} S \supset \operatorname{Rat} S$ does not hold in general for finitely generated semigroups. For example in $CS(2)$, which is defined in Section 5.2, the set $\{ab\}^+$ is rational but not recognisable which can be shown by applying an iteration lemma. The following result is known for finitely generated semigroups.

**Theorem 3.4.3**

*Let $S$ be a semigroup and let $X$ be in* $\operatorname{Rat} S$. *Then there exists a finitely generated subsemigroup $T$ of $S$ such that $X \subset T$.*

*Proof.* Let $R$ be the class of all subsets of $S$ that are contained in a finitely generated subsemigroup of $S$. We show by induction that $\operatorname{Rat} S \subset R$.

- The empty set $\emptyset$ is in $R$.
- For all $s \in S$, the singleton set $\{s\}$ is in $R$.
- If $X \in R$ and $T \subset S$ a finite subset of $S$ such that $X \subset T^+$, then $X^+ \subset T^+$.
- If $X \in R$ and $Y \in R$ and $T \subset S$ and $U \subset S$ are finite subsets of $S$ with $X \subset T^+$ and $Y \subset U^+$ respectively, then $X \cup Y \subset (T \cup U)^+$
- If $X \in R$ and $Y \in R$ and $T \subset S$ and $U \subset S$ are finite subsets of $S$ with $X \subset T^+$ and $Y \subset U^+$ respectively, then $XY \subset (T \cup U)^+$. □

Another consequence of Theorem 3.4.1 is that in a free semigroup the family of rational subsets forms a Boolean algebra. This is not true for general semigroups, for consider the monoid $M = \{a\}^* \times \{b, c\}^*$ and the rational subsets $X$ and $Y$ defined as follows.

$$X = [\![(a, b)^+(\varepsilon, c)^+]\!] = \left\{(a^n, b^n c^k) \in M \mid n, k > 0\right\}$$
$$Y = [\![(\varepsilon, b)^+(a, c)^+]\!] = \left\{(a^n, b^k c^n) \in M \mid n, k > 0\right\}$$

Now

$$X \cap Y = \{(a^n, b^n c^n) \in M \mid n > 0\}.$$

Let $M \xrightarrow{\pi} \{b, c\}$ be the projection onto the second factor of the direct product. If $X \cap Y$ were rational, then $(X \cap Y)\pi = \{b^n c^n \in \{b, c\}^* \mid n \in \mathbb{N}\}$ would be rational, which it is not. This can be shown by applying Theorem 3.2.4.

If we restrict one set to be recognisable, then we can prove a lemma about intersections.

**Lemma 3.4.4**

*Let $S$ be a semigroup. If $X \in \operatorname{Rec} S$ and $Y \in \operatorname{Rat} S$ then $X \cap Y \in \operatorname{Rat} S$.*

*Proof.* Since $Y \in \operatorname{Rat} S$ by Theorem 3.4.3 there exists a finitely generated subsemigroup $S'$ of $S$ such that $Y \in \operatorname{Rat} S'$. This implies that there is a finite generating set $A$ for $S'$, that is a surjective morphism $A^+ \xrightarrow{\pi} S'$, and by Lemma 3.3.4 a rational subset $Y'$ of $A^+$ such that $Y'\pi = Y$. Applying Theorem 3.4.1 yields that $Y'$ is recognisable. Since by assumption $X \in \operatorname{Rec} S$, the preimage $X' = X\pi^{-1}$ is a recognisable subset of $A^+$. The intersection $X' \cap Y'$ is a recognisable subset of $A^+$, and again by Theorem 3.4.1 rational and therefore $(X' \cap Y')\,\pi$ is a rational subset of $S$. Now

$$(X' \cap Y')\,\pi = \left(X' \cap Y\pi^{-1}\right)\pi = X'\pi \cap Y = X \cap Y,$$

and therefore $X \cap Y \in \operatorname{Rat} S$. □

## 3.5 *Extended Rational Subsets*

We take the above results as a motivation to define the family of *extended rational subsets* of a semigroup $S$. Extended rational subsets are not well-studied in the literature yet. Nothing prevents us from adding intersection and complement operations to the basic operations allowed in Definition 3.3.1 and Definition 3.3.2. By De Morgan's laws it would technically suffice to add the

complement operation to define the family of extended rational subsets of a given semigroup. We opt to add intersections because we will be interested in intersections in Chapter 9.

**Definition 3.5.1**

*Let* $X$ *be a set. The family* $\mathrm{ERatExp}\, X$ *of* extended rational expressions *over* $X$ *is inductively defined as follows.*

- *For* $\alpha \in \mathrm{RatExp}\, X$ *the expression* $\alpha \in \mathrm{ERatExp}\, X$,
- *for* $\alpha \in \mathrm{ERatExp}\, X$ *the expression* $\overline{\alpha} \in \mathrm{ERatExp}\, X$,
- *for* $\alpha, \beta \in \mathrm{ERatExp}\, X$ *the expression* $(\alpha \cap \beta) \in \mathrm{ERatExp}\, X$.

The definition of the map $[\![]\!]_f$ for extended rational expressions is also straightforward.

**Definition 3.5.2**

*Let* $X$ *be a set,* $S$ *be a semigroup and* $X \xrightarrow{f} S$ *be a map. We define the map* $[\![]\!]_f$ *for every* $\alpha \in \mathrm{ERatExp}\, X$ *inductively as follows.*

- $[\![\alpha]\!]_f$ *for* $\alpha \in \mathrm{RatExp}\, X$ *is the same as in Definition 3.3.2*
- $[\![\overline{\alpha}]\!]_f = S \setminus [\![\alpha]\!]_f$
- $[\![\alpha \cap \beta]\!]_f = [\![\alpha]\!]_f \cap [\![\beta]\!]_f$

We call the family of subsets of $S$ defined by extended rational expressions *extended rational subsets of* $S$ and denote this family by $\mathrm{ERat}\, S$.

For extended rational expressions $\alpha$ we inductively define some measures of complexity, the *depth* $d(\alpha)$,

- $d(\alpha) = 0$ if $\alpha \in \mathrm{RatExp}\, X$
- $d(\overline{\alpha}) = d(\alpha) + 1$
- $d(\alpha \cap \beta) = \max\{d(\alpha), d(\beta)\} + 1$,

the *complement complexity* $\mathrm{cc}(\alpha)$

- $\mathrm{cc}(\alpha) = 0$ if $\alpha \in \mathrm{RatExp}\, X$
- $\mathrm{cc}(\overline{\alpha}) = \mathrm{cc}(\alpha) + 1$
- $\mathrm{cc}(\alpha \cap \beta) = \mathrm{cc}(\alpha) + \mathrm{cc}(\beta)$,

and the *intersection complexity* $\mathrm{ic}(\alpha)$ by

- $\mathrm{ic}(\alpha) = 1$ if $\alpha \in \mathrm{RatExp}\, X$
- $\mathrm{ic}(\overline{\alpha}) = \mathrm{ic}(\alpha)$
- $\mathrm{ic}(\alpha \cap \beta) = \mathrm{ic}(\alpha) + \mathrm{ic}(\beta)$.

For a set $X \in \mathrm{ERat}\, S$, to get well-defined notions of depth, complement complexity and intersection complexity we define the depth $\mathrm{d}(X)$, $\mathrm{cc}(X)$ and $\mathrm{ic}(X)$ of $X$ to be the minimal $\mathrm{d}(\alpha)$, $\mathrm{cc}(\alpha)$ and $\mathrm{ic}(\alpha)$ among all extended rational expressions $\alpha$ with $[\![\alpha]\!] = X$.

We define a subfamily of extended rational subsets of $S$, the *polyrational subsets of* $S$, which are intersections of rational subsets.

Given $k \in \mathbb{N}_{>0}$, we call a subset $X$ of $S$ a *strictly* $k$*-rational subset* of $S$ for some $k \in \mathbb{N}_{>0}$ if there exists an extended rational expression $\alpha$ with $[\![\alpha]\!] = X$ and $\mathrm{cc}(X) = 0$ and $\mathrm{ic}(X) = k$, in other words it is possible to write $X$ as an intersection of exactly $k$ rational subsets of $S$ and no less. We make it a convention that a 1-rational subsets of $S$ are just the rational subsets.

We denote the family of all subsets of $S$ that are *at most* $k$-rational by $k\text{-Rat}\, S$ and call the elements of $k\text{-Rat}\, S$ the $k$-rational subsets of $S$. With this we have $k\text{-Rat}\, S \subset (k+1)\text{-Rat}\, S$.

A subset $X$ of $S$ is *polyrational* if and only if $X \in k\text{-Rat}\, S$ for some $k \in \mathbb{N}_{>0}$. We denote the family of polyrational subsets by $\mathrm{PRat}\, S$.

We get

$$\mathrm{Rec}\, S \subset \mathrm{Rat}\, S = 1\text{-Rat}\, S \subset 2\text{-Rat}\, S \subset \ldots \subset \mathrm{PRat}\, S \subset \mathrm{ERat}\, S.$$

We note that it would also have been possible to define polyrational expressions by just admitting the intersection operation for expressions and defining the semantics accordingly.

In light of Kleene's theorem we have the following.

**Theorem 3.5.3**
*Let $A$ be a finite set. Then* $\operatorname{Rec} A^+ = \operatorname{Rat} A^+ = \operatorname{PRat} A^+ = \operatorname{ERat} A^+$.

*Proof.* It suffices to show that $\operatorname{Rec} A^+ = \operatorname{ERat} A^+$. Let $X \in \operatorname{ERat} A^+$. If $X \in \operatorname{Rat} A^+$ then $X \in \operatorname{Rec} A^+$. If $X = \overline{Y}$ or $X = Y \cap Z$ then by induction $Y$ and $Z$ are in $\operatorname{Rec} A^+$ and therefore $\overline{Y}$ and $Y \cap Z$ are recognisable and again by Kleene's theorem rational. □

We will show in Chapter 9 that

$$k\text{-Rat}\left(A^+ \times A^+\right) \subset (k+1)\text{-Rat}\left(A^+ \times A^+\right)$$

holds for all $k \in \mathbb{N}_{>0}$.

As stated above, the theory of extended rational subsets of semigroups and extended rational relations is, to the knowledge of the author, not well-understood. In particular it should be examined which levels of complexity can be achieved.

Extended rational relations are accepted by finite trees of finite state automata. We will not go further into this matter and leave this as a potentially interesting area of research, in particular finding out which complexity levels are realisable as word problems.

## 3.6 Recognisable Relations

This section serves the purpose of characterising relations that are recognisable. This result was first proven by Mezei in [EM65]. We first define what we mean by a recognisable relation.

**Definition 3.6.1**

*Let* $S$ *and* $T$ *be semigroups. A relation* $S \xrightarrow{\rho} T$ *is* recognisable *if* $\mathcal{G}_\rho$ *is a recognisable subset of* $S \times T$.

The following theorem is due to Mezei and characterises recognisable relations between monoids. Note that we can turn any semigroup into a monoid by adding an identity element.

**Theorem 3.6.2**

*Let* $S_1$ *and* $S_2$ *be monoids and let* $S = S_1 \times S_2$. *Then* $U \in \operatorname{Rec} S$ *if and only if*

$$U = \bigcup_{i \in I} X_i \times Y_i,$$

*where* $X_i \in \operatorname{Rec} S_1$ *and* $Y_i \in \operatorname{Rec} S_2$ *and* $I$ *is a finite index set.*

*Proof.* Let $S_1$ and $S_2$ be monoids and let $S = S_1 \times S_2$.

Let $S \xrightarrow{\pi_i} S_i$ be the projections on $S_i$ for $i \in \{1, 2\}$. If $X \in \operatorname{Rec} S_1$ and $Y \in \operatorname{Rec} S_2$ then

$$X \times Y = (X \times S_2) \cap (S_1 \times Y) = X\pi_1^{-1} \cap Y\pi_2^{-1}.$$

Hence, since $\operatorname{Rec} S$ is closed under finite union $U \in \operatorname{Rec} S$.

Conversely let $U \in \operatorname{Rec} S$, which by definition implies that there is a morphism $S \xrightarrow{\varphi} T$, with $T$ finite, such that $U = F\varphi^{-1}$ for some $F \subset T$. Define two morphisms $S_i \xrightarrow{\psi_i} T$ for $i \in \{1, 2\}$ by

$$s_1\psi_1 = (s_1, \mathbf{e})\varphi \qquad\qquad s_2\psi_2 = (\mathbf{e}, s_2)\varphi, \tag{3.6}$$

and define $S \xrightarrow{\theta} T \times T$ by

$$(s_1, s_2)\theta = (s_1\psi_1, s_2\psi_2)\,. \tag{3.7}$$

Now $U$ is the preimage of the subset

$$F' = \{(t_1, t_2) \in T \times T \mid t_1 t_2 \in F\}$$

of $T \times T$ under $\theta$ and therefore

$$U = \bigcup_{(t_1, t_2) \in F'} \left(t_1\psi_1^{-1}\right) \times \left(t_2\psi_2^{-1}\right).$$

## 3.7 *Rational Relations*

We define the class of rational relations between semigroups. There are rational relations between free semigroups that are not recognisable. We know from Theorem 3.4.2 that for finitely generated $S \times T$ all recognisable relations are also rational. This is in contrast with recognisable and rational subsets of free semigroups, where these two classes of subsets are the same.

**Definition 3.7.1**

*Let $S$ and $T$ be semigroups. A relation $S \xrightarrow{\rho} T$ is* rational *if $\mathcal{G}_\rho$ is a rational subset of $S \times T$.*

We call rational relations $S \xrightarrow{\rho} S$ which are equivalence relations or congruence relations *rational equivalences* and *rational congruences* respectively. We note that the kernel of a semigroup morphism is a congruence and therefore we can also speak of a rational morphism $S \xrightarrow{\varphi} T$ if the kernel of $\varphi$ is a rational congruence.

We prove a characterisation of rational relations due to Nivat [Niv68]. It relates rational relations to recognisable subsets of a free semigroup, and as a consequence we can prove an iteration lemma for rational relations. We again take the route that Eilenberg chose in his book "Automata, Languages, Machines" [Eil76a]. Eilenberg himself attributes most of these results to Elgot, Mezei and Nivat.

The following theorem is the *first factorisation theorem* in Eilenberg's book. It is Theorem 2.2 in Chapter IX of [Eil76a].

**Theorem 3.7.2**

*Let $S$ and $T$ be finitely generated semigroups. A relation $S \xrightarrow{\rho} T$ is rational if and only if it admits a factorisation*

$$S \xrightarrow{\alpha^r} C^* \xrightarrow{\cap K} C^* \xrightarrow{\omega} T, \tag{3.8}$$

*where $C^* \xrightarrow{\alpha} S$ and $C^* \xrightarrow{\omega} T$ are morphisms and $K$ is a rational subset of $C^*$.*

*Proof.* Assume that $\rho$ is as in (3.8), then by Lemma 1.4.3 it follows that $\mathcal{G}_\rho = K\gamma$ where $C^* \xrightarrow{\gamma} S \times T$ and $s\gamma = (s\alpha, s\beta)$. Now since $K$ is a rational subset of $C^*$ so is $K\gamma$.

Conversely, let $S \xrightarrow{\rho} T$ be a rational relation. Let $X$ and $Y$ be finite generating sets for $S^1$ and $T^1$ respectively. Then $Z = X \times Y$ is a generating set for $S^1 \times T^1$. There exists a finite alphabet $C$ and a morphism $C^* \xrightarrow{\gamma} S^1 \times T^1$ and rational $K \subset C^*$ such that $C\gamma \subset Z$ and $K\gamma = \mathcal{G}_\rho$. Define $C^* \xrightarrow{\alpha} S$ and $C^* \xrightarrow{\beta} T$ such that $s\gamma = (s\alpha, s\beta)$. Then $C\alpha \subset \mathbf{e}_S \cup X$ and $C\beta \subset \mathbf{e}_T \cup Y$, and by Lemma 1.4.3 the relation $\rho$ is equal to the composition (3.8). □

One application of the factorisation theorem is to show that a rational relation preserves rational subsets. This is Eilenberg's *evaluation theorem*, Theorem 3.1 in Chapter IX of [Eil76a].

**Theorem 3.7.3**

*Let* $A^+ \xrightarrow{\rho} S$ *be a rational relation between the semigroups* $A^+$ *and* $S$. *If* $X \in \operatorname{Rat} A^+$ *then* $X\rho \in \operatorname{Rat} S$.

*Proof.* Applying Theorem 3.7.2 to $A^+ \xrightarrow{\rho} S$ yields the factorisation

$$A^+ \xrightarrow{\alpha^r} C^* \xrightarrow{\cap K} C^* \xrightarrow{\omega} S,$$

where $C^* \xrightarrow{\alpha} A^+$ and $C^* \xrightarrow{\omega} S$ are morphisms and $K$ is a rational subset of $C^*$.

Now $X\alpha^{-1}$ is a rational subset of $C^*$ by Lemma 3.3.4 and Theorem 3.4.1. Therefore $K \cap \left(X\alpha^{-1}\right)$ is a rational subset of $C^*$ and therefore

$$\left(K \cap \left(X\alpha^{-1}\right)\right)\omega$$

is a rational subset of $S$. □

Our second application of the first factorisation theorem is this composition theorem which establishes when the composition of two rational relations is rational. A proof of this theorem can be found in [Eil76a, Chapter IX] or in [Ber79, Chapter 33].

**Theorem 3.7.4**

*Let $S$ and $T$ be semigroups and let $A^+$ be a free semigroup on the finite set $A$. Let furthermore $S \xrightarrow{\rho} A^+$ and $A^+ \xrightarrow{\sigma} T$ be rational relations. Then the composition*

$$S \xrightarrow{\rho} A^+ \xrightarrow{\sigma} T$$

*is a rational relation.*

The hypothesis of the middle semigroup being free is necessary.

The following theorem is Eilenberg's *second factorisation theorem*, Theorem 5.1 in Chapter IX of [Eil76a].

**Theorem 3.7.5**

*Let $A$ and $B$ be alphabets. A relation $A^* \xrightarrow{\rho} B^*$ with $\varepsilon\rho \neq \emptyset$ is rational if and only if it admits a factorisation*

$$A^* \xrightarrow{\alpha} C^* \xrightarrow{\cap K} C^* \xrightarrow{\omega^r} B^*,$$

*where $A^* \xrightarrow{\alpha} C^*$ is a morphism with $A\alpha \subset C$ and $B^* \xrightarrow{\omega} C^*$ is a rational substitution and $K$ is a rational subset of $C^*$.*

And finally we get an iteration lemma, for rational relations. A proof can be found again in [Eil76a], Proposition 9.1 of Chapter IX.

**Proposition 3.7.6**

*Let $A^+ \xrightarrow{\rho} B^+$ be a rational relation. Then there exists $n_0 \in \mathbb{N}$ such that $v \in A^+$, and $w \in v\rho$ with $|v| + |w| \geq n_0$ admits factorisations $v = x_1u_1z_1$ and $w = x_2u_2z_2$ with*

- $0 < |u_1| + |u_2| \leq n_0$
- $x_2u_2^iz_2 \in x_1u_1^iz_1r$ *for all* $i \in \mathbb{N}$.

The following theorem was found by Johnson while doing research for his PhD thesis [Joh83; Joh85]. One of Johnson's goals was to show that rational equivalence relations have recognisable cross section. He did not succeed and

to this day it is an open question whether rational equivalence relations have recognisable cross sections. The following proposition is proved in Johnson's PhD thesis.

**Proposition 3.7.7**

*Let* $A^* \xrightarrow{\rho} A^*$ *be a rational equivalence relation. There exists a recognisable subset* $D \subseteq A^*$ *such that*

- *the composition*

$$D \xrightarrow{\iota_D} A^* \xrightarrow{\rho} A^* \xrightarrow{\iota_D^r} D$$

  *is an equivalence relation on* $D$,

- *for every* $v \in A^*$ *there exists a* $w \in D$ *such that* $w \in v\rho$, *and*

- $|v\rho \cap D|$ *is finite.*

We explicitly ask the following two open questions.

**Open Question 3.7.1**

*Given a rational equivalence relation* $A^* \xrightarrow{\rho} A^*$, *does there exist a recognisable set* $D \subset A^*$ *such that* $|v\rho \cap D| = 1$ *for all* $v \in A^*$.

Obviously a positive answer to the above would imply a positive answer to the following question, but not the converse, but failing to show the above result it might be possible to show the following using the special properties of a congruence.

**Open Question 3.7.2**

*Given a rational congruence relation* $A^* \xrightarrow{\rho} A^*$, *does there exist a recognisable set* $D \subset A^*$ *such that* $|v\rho \cap D| = 1$ *for all* $v \in A^*$.

## 3.8 Polyrational Relations

This section is devoted to showing that the composition of a polyrational relation with a rational relation is a polyrational relation. We focus our attention

on polyrational relations since these are needed in Chapter 9. The notion of extended rational relations is not well understood and a possible area for future research.

We define the notion of a polyrational relation.

**Definition 3.8.1**

*Let* $S$ *and* $T$ *be semigroups. A relation* $S \xrightarrow{\rho} T$ *is* polyrational *if* $\mathcal{G}_\rho$ *is a polyrational subset of* $S \times T$.

We show that composition of a rational relation and a polyrational relation is a polyrational relation.

**Theorem 3.8.2**

*Let* $A$ *and* $B$ *be alphabets, let* $A^+ \xrightarrow{\rho} A^+$ *be a polyrational relation and let* $B^+ \xrightarrow{\tau} A^+$ *be a rational relation. Then the relation* $B^+ \xrightarrow{\tau\rho} A^+$ *is polyrational.*

*Proof.* By Definition 3.8.1 it holds that

$$\rho = \bigcap_{i \in \underline{k}} \rho_i$$

for some $k \in \mathbb{N}_{>0}$ and rational relations $A^+ \xrightarrow{\rho_i} A^+$. Therefore by Lemma 3.7.4 the relations $\tau\rho_i$ are rational and it follows from the proof of Lemma 3.7.4 that the set

$$R_i = \{(v, u, w) \mid u \in w\tau \text{ and } w \in u\rho_i\},$$

is a rational subset of $B^+ \times A^+ \times A^+$.

Define the morphism $\pi$ as

$$\pi : B^+ \times A^+ \times A^+ \longrightarrow B^+ \times A^+,\ (v, u, w) \mapsto (v, w).$$

Since $\pi$ is a morphism and $R_i$ is a rational subset for $i \in \underline{k}$, the image $R_i\pi$ of $R_i$ under $\pi$ is a rational subset of $B^+ \times A^+$.

We show that

$$(\bigcap_{i \in \underline{k}} R_i)\,\pi = \bigcap_{i \in \underline{k}} (R_i\pi),$$

and hence that $\mathcal{G}_{\tau\rho}$ is a polyrational subset of $B^+ \times A^+$ and therefore the relation $B^+ \xrightarrow{\tau\rho} A^+$ is a polyrational relation.

For the remainder of this proof let all intersections range over $i \in \underline{k}$.

If $(v, w) \in (\bigcap R_i)\,\pi$ then there is $u \in A^+$ such that for all $i \in \underline{k}$ it holds that $(v, u, w) \in R_i$. This means that for all $i \in \underline{k}$ the pair $(v, w) \in R_i\pi$ and therefore $(v, w) \in \bigcap (R_i\pi)$.

Conversely, if $(v, w) \notin (\bigcap R_i)\,\pi$, then for all $u \in A^+$ there exists an $i \in \underline{k}$ such that $(v, u, w) \notin R_i$ and therefore $(v, w) \notin R_i\pi$, which implies that $(v, w) \notin \bigcap (R_i\pi)$.

This concludes the proof of the claim that the composition of $\tau$ and $\rho$ is a polyrational relation. □

The proof of the following theorem is just as above and we state the theorem for completeness.

**Theorem 3.8.3**

*Let* $A$ *and* $B$ *be alphabets, let* $A^+ \xrightarrow{\rho} A^+$ *be a polyrational relation and let* $A^+ \xrightarrow{\sigma} B^+$ *be a rational relation. Then the relation* $A^+ \xrightarrow{\rho\sigma} B^+$ *is polyrational.*

# 4

○ ⊙ ○

# *Computation*

We introduce the necessary notions and theorems from the theory of automata and computation. A lot of the material in this chapter is inspired by Chapter X of Eilenberg's book Automata, Languages and Machines [Eil76a]. We start by defining finite state automata and show how finite state automata relate to recognisable and rational subsets of semigroups and relations between semigroups. We then introduce the notion of a machine as defined by Eilenberg, in terms of which we can define one-counter and pushdown automata as well as Turing machines. We also give a short overview of the notion of complexity.

## *4.1 Automata*

The most important ingredient for a theory of computation are, of course, models of computation. Our model of computation is the *automaton*. An automaton consists of *states* and possible *transitions*. At any point in time an

automaton is in exactly one state, and reading an input changes the state. Sequences of inputs form a free semigroup acting on the states. This already hints at the close relationship between semigroups and computation.

**Definition 4.1.1**

*Let $A$ be an alphabet. An* $A$-automaton $\mathcal{A}$ *is a tuple*

$$\mathcal{A} = \left\langle Q, q_0, F, (\xrightarrow{a})_{a \in A} \right\rangle,$$

*where* $Q$ *is a finite set of* states, $q_0 \in Q$ *is the* initial state, $F \subset Q$ *is the set of* final states *and* $(\xrightarrow{a})_{a \in A}$ *is a family of relations on* $Q$ *labelled by* $A$.

Note that we do not require the alphabet in Definition 4.1.1 to be finite. We will say that an $A$-automaton is finite if $A$ is finite.

We denote transitions of $\mathcal{A}$ by $q \xrightarrow{a} q'$ and call $a$ the *label of* $q \xrightarrow{a} q'$. Two transitions $q \xrightarrow{a} q'$ and $q' \xrightarrow{a'} q''$ can be composed to form a *partial computation*

$$q \xrightarrow{a} q' \xrightarrow{a'} q'',$$

and therefore we can compose transitions $q_i \xrightarrow{a_i} q_{i+i}$ for $1 \leq i \leq n$ into *partial computations* of $\mathcal{A}$, which we denote by

$$\gamma : q_1 \xrightarrow{s} q_{n+1}$$

where $s = [\mathbf{a_1} \dots \mathbf{a_n}]$. We call $q_1$ the start state and $q_{n+1}$ the end state of $\gamma$. The string $s$ is the *label of* $\gamma$ denoted $|\gamma|$.

Given two partial computations $\gamma : q_1 \xrightarrow{s} q_2$ and $\gamma' : q_2 \xrightarrow{t} q_3$ the *composite computation* $\gamma \cdot \gamma'$ is a computation from $q_1$ to $q_3$ labelled by $s \cdot t$.

As a convention we can also always include the identity computation $q \xrightarrow{\varepsilon} q$.

If defined, the concatenation of computations is associative, so the set $\Gamma(\mathcal{A})$ of all computations of an automaton is a semigroupoid. The labels of defined computations of an automaton form a subset of the free monoid $A^*$.

Computations that start in the state $q_0$ are treated specially. A state $q \in Q$ is *accessible* if there is a computation $\gamma : q_0 \xrightarrow{s} q$, it is *coaccessible* if there is a computation $\gamma : q \xrightarrow{s} q'$ with $q'$ in $F$. An $A$-automaton $\mathcal{A}$ is *deterministic*, if for all $s \in A^*$ there is at most one computation $\gamma : q_0 \xrightarrow{s} q$. A computation $\gamma : q_0 \xrightarrow{s} q$ is *accepting* or *successful* if $q \in F$.

We define the *behaviour* $|\mathcal{A}|$ *of* $\mathcal{A}$ by

$$|\mathcal{A}| = \{|\gamma| \mid \gamma \text{ successful}\},$$

and we say that the automaton $\mathcal{A}$ *decides the set* $|\mathcal{A}|$.

We show that the behaviour of a finite automaton $\mathcal{A}$ is a recognisable subset of $A^*$, and that any recognisable subset of $A^*$ is the behaviour of a finite automaton.

**Theorem 4.1.2**

*Let $A$ be a finite alphabet. Then $X \in \operatorname{Rec} A^*$ if and only if there exists a finite $A$-automaton with $|\mathcal{A}| = X$.*

*Proof.* If $X$ is an element of $\operatorname{Rec} A^*$, then by definition there exists a monoid morphism $A^* \xrightarrow{\varphi} T$, where $T$ is finite, and some $F \subset T$ such that $X = F\varphi^{-1}$. Define the automaton

$$\mathcal{A} = \left\langle T, \mathbf{e}, F, (\xrightarrow{a})_{a \in A} \right\rangle,$$

with transitions

$$t \xrightarrow{a} t(a\varphi) \text{ for all } t \in T \text{ and } a \in A.$$

Now, again by the definition of the recognisability of $X$, the string $v$ is an element of $X$ if and only if $v\varphi$ is an element of $F$, and by construction of $\mathcal{A}$ this is the case if and only if there is a successful computation of $\mathcal{A}$ labelled by $v$.

Conversely let

$$\mathcal{A} = \left\langle Q, q_0, F, (\xrightarrow{a})_{a \in A} \right\rangle$$

be an $A$-automaton with $|\mathcal{A}| = X$.

The free monoid $A^*$ acts on the powerset $\hat{Q}$ of $Q$ by

$$P a = \left\{ q \in Q \mid p \xrightarrow{a} q,\ p \in P \right\}$$

for any set $P \in \hat{Q}$. This defines a monoid morphism $A^* \xrightarrow{\varphi} \mathcal{T}_{\hat{Q}}$ and since the set $Q$ of states is finite, the set $\hat{Q}$ is finite too. Defining $\tilde{F} \subset \mathcal{T}_{\hat{Q}}$ by

$$\tilde{F} = \left\{ f \in \mathcal{T}_{\hat{Q}} \mid q_0 f \cap F \neq \emptyset \right\},$$

the morphism $\varphi$ recognises $X$. □

Eilenberg argues that one can generalise the above definitions and results and define automata that take inputs over an arbitrary monoid $M$, but that making that exposition explicit would be "an exercise that is not very productive". We take the same position but note that we already introduced notions of rationality and recognisability in the more general setting of semigroups and monoids, and will use this generalisation in the following section. Note that it is convenient to allow for infinite $M$ as long as we can find a finite set $M_0$ that generates the submonoid of $M$ that contains $|\mathcal{A}|$.

We generalise the notion of an automaton in another direction, namely by considering finite tuples of automata which we will call *parallel automata*.

**Definition 4.1.3**

*Let $A$ be an alphabet. A* $k$-parallel $A$-automaton *is a* $k$*-tuple $\mathcal{A} = (\mathcal{A}_i)_{i \in \underline{k}}$ where $\mathcal{A}_i$ is an $A$-automaton for $i \in \underline{k}$.*

A $k$-parallel automaton $\mathcal{A} = (\mathcal{A}_i)_{i \in \underline{k}}$ accepts an input if an only if for all $i \in \underline{k}$ the automaton $\mathcal{A}_i$ accepts it. The concept of a $k$-parallel automaton is not more powerful with respect to specifying subsets of $A^*$: It follows from Kleene's theorem and the fact that the recognisable subsets of $A^*$ form a Boolean algebra that for any behaviour of a $k$-parallel $A$-automaton there exists an $A$-automaton with the same behaviour. If we consider subsets of $S \times T$ the situation becomes very different. The following section will show how this automaton model becomes useful for us.

## 4.2 Polyrational Relations

We consider relations $S \xrightarrow{\rho} T$ where $S$ and $T$ are monoids, and show that $S \xrightarrow{\rho} T$ is rational if and only if there is a finite automaton that decides the graph $\mathcal{G}_\rho$ of $S \xrightarrow{\rho} T$.

**Theorem 4.2.1**

*Let $S$ and $T$ be monoids. A relation $S \xrightarrow{\rho} T$ is rational if and only if there is a finite alphabet $A$ and an $A$-automaton $\mathcal{A}$ with $|\mathcal{A}| = \mathcal{G}_\rho$.*

*Proof.* Let $S \xrightarrow{\rho} T$ be a rational relation. Then its graph $\mathcal{G}_\rho$ is by definition a rational subset of $S \times T$, and by Theorem 3.4.3 and Lemma 3.3.4 there exists a finite alphabet $A$, a morphism $A^* \xrightarrow{\varphi} S \times T$ and a set $X \in \operatorname{Rat} A^*$ such that $\mathcal{G}_\rho = X\varphi$. Now $X$ is the behaviour of an $A$-automaton $\mathcal{A}$.

Conversely let $\mathcal{A}$ be an $S \times T$-automaton such that $|\mathcal{A}| = \mathcal{G}_\rho$. Assuming $A$ to be the set of all labels in the automaton $\mathcal{A}$, we can view $\mathcal{A}$ as an $A$-automaton that decides the subset $|\mathcal{A}|$ of $A^*$. This implies that $|\mathcal{A}|$ is rational. Using the inclusion mapping $A \xrightarrow{i} S \times T$ it follows that there exists a unique morphism $A^* \xrightarrow{\varphi} S \times T$ which extends $i$. Now $\mathcal{G}_\rho = |\mathcal{A}|\,\varphi$ and is therefore rational as the image of a rational set under a morphism. □

Extending this idea, $k$-parallel $A$-automata decide $k$-rational relations.

**Theorem 4.2.2**

*Let $S$ and $T$ be monoids. A relation $S \xrightarrow{\rho} T$ is at most $k$-rational if and only if there is a $k$-parallel $S \times T$-automaton $\mathcal{A}$ with $|\mathcal{A}| = \mathcal{G}_\rho$.*

*Proof.* A relation $S \xrightarrow{\rho} T$ is $k$-rational if and only if there are rational relations $S \xrightarrow{\rho_i} T$ for $i \in \underline{k}$ such that $\rho$ is the intersection of $\rho_i$. Applying Theorem 4.2.1, this is the case if and only if there are $S \times T$-automata $\mathcal{A}_i$ for $i \in \underline{k}$ with $|\mathcal{A}_i| = \mathcal{G}_{\rho_i}$. A pair $(s,t)$ is contained in $\mathcal{G}_\rho$ if and only if $(s,t)$ is contained in $\mathcal{G}_{\rho_i}$ for all $i \in \underline{k}$ which is the case if and only if $(s,t)$ is accepted by the $k$-parallel automaton $(\mathcal{A}_i)_{i\in\underline{k}}$. □

## 4.3 Machines

We take the time to introduce Eilenberg's concept of an X-*machine*. We will only touch on this matter in the final chapters, but find it important to introduce this concept here, since it will give the formal methods to generalise some of the results presented.

Eilenberg's machines are a very powerful generalisation of an automaton as defined in Section 4.1.

**Definition 4.3.1**
*Let* $X$, $Y$ *and* $Z$ *be sets and let* $\Phi$ *be a family of relations* $X \xrightarrow{\varphi} X$. *An* X-machine $\mathcal{M}$ of type $\Phi$ with inputs from $Y$ and outputs in $Z$ *is a tuple*

$$\mathcal{A} = \left\langle Q, q_0, F, \left(\xrightarrow{\varphi}\right)_{\varphi\in\Phi}, \alpha, \omega \right\rangle,$$

*where* $\left\langle Q, q_0, F, \left(\xrightarrow{\varphi}\right)_{\varphi\in\Phi}\right\rangle$ *is a* $\Phi$*-automaton,* $Y \xrightarrow{\alpha} X$ *is the* input encoding relation *and* $X \xrightarrow{\omega} Z$ *is the* output encoding relation.

The input encoding relation $\alpha$ converts an input into a representation suitable for the machine at hand, the output encoding relation $\omega$ converts back from an internal representation to an output. Computations are labelled by elements of $\Phi$ and via the embedding of $\Phi$ into $\mathcal{R}_X$ we assign to every computation an element of the monoid $\mathcal{R}_X$. The element of $\mathcal{R}_X$ represented by the label of a computation $\gamma$ is called the *behaviour of* $\gamma$, denoted $|\gamma|$.

We define the *behaviour* $|\mathcal{M}|$ *of* $\mathcal{M}$ by

$$|\mathcal{M}| = \{|\gamma| \mid \gamma \text{ successful}\},$$

and we say that the machine $\mathcal{M}$ *computes the relation* $\rho_{\mathcal{M}}$ given by

$$\rho_{\mathcal{M}} : Y \xrightarrow{\alpha} X \xrightarrow{|\mathcal{M}|} X \xrightarrow{\omega} Z.$$

To make clear how powerful this definition is, we now define several well-known models of computation in terms of the above definition, but leave out

detailed proofs. Let

$$\mathcal{M} = \left\langle Q, q_0, F, (\xrightarrow{\varphi})_{\varphi\in\Phi}, \alpha, \omega \right\rangle,$$

with inputs in $A^*$ and outputs in $B^*$, where

$$X = B^* \times M \times A^*$$

for a monoid $M$ and

$$\nu\alpha = (\mathbf{e}, \mathbf{e}, \nu)$$
$$(w, m, \nu)\,\omega = \begin{cases} w & \text{if } m = 1, \nu = 1 \\ \emptyset & \text{otherwise} \end{cases}.$$

Now the expressive power of the machine depends on the choices of $M$ and $\Phi$. The machine $\mathcal{M}$ is equivalent to a

- *finite automaton* if $M = \{\mathbf{e}\}$, $A = Y$ and $B = \emptyset$ and the family $\Phi$ is the family $\lambda^r_a$ for $a \in A$;

- *pushdown automaton* if $M = C^*$, where $C$ is a finite alphabet with $|C| > 1$, the set $B = \emptyset$ and the family $\Phi$ consists of relations

$$\begin{aligned} \iota\times\lambda^r_a &\qquad \text{for } a \in A \\ \rho_c\times\iota &\qquad \text{for } c \in C \\ \rho^r_c\times\iota &\qquad \text{for } c \in C \end{aligned}$$

  In the special case where $|C| = 1$, the automaton $\mathcal{A}$ is a *one-counter automaton*;

- *Turing automaton* or more commonly *Turing machine* if $M = A^*$, $B = \emptyset$ and $\Phi$ consists of the relations $\rho_a \times \iota$, $\iota \times \lambda_a$, $\rho^r_a \times \iota$ and $\iota \times \lambda^r_a$ for $a \in A$.

## 4.4 Decidability and Complexity

The two notions of a problem being *decidable* and, if so, what *complexity* it has, have been considered since Hilbert asked for a solution to the *Entscheidungsproblem*.

The Entscheidungsproblem asks for an algorithm that takes as its input a sentence in first order logic and a finite collection of axioms and outputs yes or no depending on whether the sentence is valid within the theory given by the axioms. Famously Kurt Gödel [Göd31], and later, maybe more accessibly in an algorithmic setting, Alan Turing [Tur36], proved that such an algorithm cannot exist. This gives the motivation for the following definition.

**Definition 4.4.1**
*Let* $A$ *be an alphabet. A subset* $X \subset A^*$ *is* recursively decidable *or simply* decidable *if there exists a Turing machine* $\mathcal{M}$ *with inputs in* $A^*$ *such that the relation computed by* $\mathcal{M}$ *is the characteristic function of* $X$ *in* $A^*$.

Since it is quite tedious to actually construct a Turing machine, one usually defines higher level constructs, for example programming languages, and proves the equivalence of that language to Turing machines by expressing the operations of the language in terms of operations of a Turing machine, and making sure that these operations are composable. In this setting a subset $X$ of $A^*$ is decidable if and only if there exists a procedure in the higher level language that computes the characteristic function of $X$.

For this thesis we note that the existence of an automaton that accepts $X$ proves that $X$ is a decidable subset of $A^*$.

With the definition of a Turing machine, it becomes possible to formally examine problems for their *complexity*. Complexity is a very general notion and is understood to be the amount of resources one has to use to solve a problem. In the context of theoretical computer science this has classically been *time complexity* and *space complexity*.

In the case of this thesis we might be more interested in how many states we need in an automaton or how many independent automata are needed to decide a polyrational relation. For practical purposes, for example implementing decision procedures in a computer algebra system, we will also be interested in space and time complexity.

**Theorem 4.4.2**

*Let* $A$ *and* $B$ *be alphabets and let* $\mathcal{A}$ *be a finite* $A^* \times B^*$*-automaton. Given* $(v, w) \in A^* \times B^*$*, it can be decided in time* $\mathcal{O}\Big((|v| + |w|)^2\Big)$ *and space* $\mathcal{O}(|v| + |w|)$ *whether* $\mathcal{A}$ *accepts* $(v, w)$*.*

*Proof.* Assume

$$\mathcal{A} = \left\langle Q, q_0, F, (\xrightarrow{x})_{x \in X} \right\rangle$$

to be the given finite $X$-automaton. Without loss of generality we can assume $X$ to only consist of $(a, \varepsilon)$ for $a \in A$ and $(\varepsilon, b)$ for $b \in B$ and $(\varepsilon, \varepsilon)$.

For $(x, y) \in X$ define the $(x, y)$*-follow* operation of a set of states by

$$f_{(x,y)} : \hat{Q} \longrightarrow \hat{Q},\ P \mapsto \left\{ q \in Q \mid \exists p \in P, p \xrightarrow{(x,y)} q \right\},$$

and denote by $f^+_{(\varepsilon,\varepsilon)}$ the iteration of $f_{(\varepsilon,\varepsilon)}$. The operation $f^+_{(\varepsilon,\varepsilon)}$ is sometimes called the $\epsilon$-closure operation. The iteration reaches a fixed point after finitely many iterations since the set of states is finite. We denote by $f^{\oplus}_{(x,y)}$ the composition $f_{(x,y)} f^+_{(\varepsilon,\varepsilon)}$. For $Y = A^* \times B^* \times \hat{Q}$, define the iteration $I^n$ by

$$\begin{aligned} I^0 &= \{(v, w, \{q_0\}\, \epsilon)\} \\ I^{n+1} &= \{(v, w, \bigcup P_{xv,yw} f^{\oplus}_{(x,y)}) \in Y \mid (xv, yw, P_{xv,yw}) \in I^n \text{ for } (x, y) \in X\} \end{aligned}$$

An algorithm that decides whether a given input $(v, w)$ is accepted by $\mathcal{A}$ now proceeds by iteratively computing $I^n$ for increasing $n$ until there is an element $(\varepsilon, \varepsilon, P)$ in $I^n$. Note that since we apply the $\epsilon-$closure in every step, $|v| + |w|$ is strictly decreasing for increasing $n$, and therefore this procedure will

terminate. If $P \cap F \neq \emptyset$, then $(v, w)$ is accepted, otherwise $P \cap F = \emptyset$ and $(v, w)$ is not accepted.

A tuple $(v', w', P)$ is in $I^n$ if and only if there exists a computation $q_0 \xrightarrow{(s,t)} p$ of $\mathcal{A}$ with label $(s, t)$ such that $sv' = v$ and $tw' = w$ and $p \in P$. This can be shown by induction on the iteration rule.

To estimate the runtime of this algorithm, note that $(\varepsilon, \varepsilon, P)$ will be reached after exactly $|v| + |w|$ iterations. The size of $I^n$ is bounded linearly in $n$, therefore in every iteration step we need $n$ applications of the function $f^{\oplus}_{(x,y)}$, which in this setting can be done in $\mathcal{O}(1)$. Since the size of $I^n$ is bounded linearly in $|v| + |w|$, the space requirement for this algorithm is in $\mathcal{O}(|v| + |w|)$. □

Note also that if we consider the automaton as input, the sizes of the set $Q$ and the transition relation are significant for time and memory consumption.

The two more general questions whether a rational relation is non-empty and whether a rational relation is finite are decidable.

**Theorem 4.4.3**

*Let $\mathcal{A}$ be a $A^* \times B^*$-automaton. It is decidable whether $|\mathcal{A}|$ is empty and whether $|\mathcal{A}|$ is finite. Given a rational relation $A^* \xrightarrow{\rho} B^*$ as a $A^* \times B^*$-automaton, it is decidable whether $\rho$ is the empty relation and whether $\rho$ is a finite relation.*

*Proof.* Let

$$\mathcal{A} = \left\langle Q, q_0, F, \left(\xrightarrow{x}\right)_{x \in X} \right\rangle$$

be an $A^* \times B^*$-automaton.

To decide whether $|\mathcal{A}|$ is empty, it is sufficient to apply a search algorithm to the finite graph that is defined by the states and the transition relations. If there is at least one path from $q_0$ to a state in $F$, then $|\mathcal{A}|$ is not empty. To decide whether $|\mathcal{A}|$ is finite, we consider all paths from $q_0$ to states in $F$ and check whether there exists a path that has a loop that is not labelled by $(\varepsilon, \varepsilon)$. To decide whether a rational relation $A^* \xrightarrow{\rho} B^*$ given by a $A^* \times B^*$-automaton $\mathcal{A}$ is empty, finite, or infinite, we observe that $A^* \xrightarrow{\rho} B^*$ is empty, finite or infinite if and only if $|\mathcal{A}|$ has the respective property. □

In contrast to the previous two theorems, somewhat surprisingly, many non-trivial but straightforward problems for rational relations are undecidable in general: It is undecidable whether the intersection of two rational relations is empty, whether two rational relations are equal and whether a rational relation is recognisable. It is also undecidable whether a rational relation is universal, a property which becomes decidable for rational congruences as we will show in Chapter 8. Proofs rely on the undecidable Post-Correspondence-Problem and can for example be found in [Ber79, Ch. 8].

**Theorem 4.4.4**

*Let* $A^* \xrightarrow{\rho} B^*$ *and* $A^* \xrightarrow{\sigma} B^*$ *be a rational relations. The following problems are undecidable.*

1. $\rho \cap \sigma = \emptyset$
2. $\rho \subset \sigma$
3. $\rho = \sigma$
4. $v\rho = B^*$ *for all* $v \in A^*$
5. $\rho$ *is recognisable.*

# 5

○ ⊙ ⊙

# *Examples*

This section introduces some of the semigroups that will be used in later sections along with a few properties. We introduce free commutative semigroups and transformation semigroups and then give two infinite families of infinite, finitely presented semigroups that have infinite $\mathcal{R}-$classes and an infinitely presented semigroup. These examples will serve as examples and counterexamples in later chapters.

## *5.1 Transformation Semigroups*

For any set $X$ the full transformation monoid $\mathcal{T}_X$ has already been introduced as the monoid of all maps $X \xrightarrow{f} X$ in Section 1.3 and Section 2.1. Here we introduce a way to specify elements of a full transformation monoid on a finite set and therefore generating sets of subsemigroups of the full transformation monoid on a finite set. We can specify any element $\tau \in \mathcal{T}_{\underline{n}}$ by giving the image $k\tau$ for all $k \in \underline{n}$, and for small examples this can be done in the following

tabular form.

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ 1\tau & 2\tau & \dots & n\tau \end{pmatrix}$$

The following two elements $\tau$ and $\sigma$ of $\mathcal{T}_{\underline{4}}$ shall serve as examples.

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 2 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 3 & 3 \end{pmatrix}$$

The subsemigroup of $\mathcal{T}_{\underline{4}}$ generated by $\tau$ and $\sigma$ has eight elements.

Similarly it is possible to specify elements $\tau$ of $\mathcal{T}_{\mathbb{N}}$ by specifying $n\tau$ for every $n \in \mathbb{N}$.

## 5.2 *Free Commutative Semigroups*

The free commutative semigroup of rank $k$ for any $k \in \mathbb{N}_{>0}$ can be defined by a similar universal property like the one used in the definition of a free semigroup. We specify the free commutative semigroup of rank $k$ by the following finite presentation.

$$\mathrm{CS}(k) = \mathrm{sg}\langle a_1, \dots, a_k \mid a_i a_j = a_j a_i \text{ for } 1 \leq i < j \leq k \rangle$$

We remind ourselves that $|v|_{a_i}$ denotes the number of occurrences of $a_i$ in $v$. Two strings $v$ and $w$ represent the same element of $\mathrm{CS}(k)$, if and only if $|v|_{a_i} = |w|_{a_i}$ for all $a_i$. One choice for a set of unique representatives for elements of $\mathrm{CS}(k)$ is therefore the set of strings $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_k^{\alpha_k}$ for $\alpha_i \in \mathbb{N}$ and $\sum_{i \in \underline{k}} \alpha_i > 0$.

The *free commutative monoid* of rank $k$, denoted $\mathrm{CM}(k)$ is isomorphic to $\mathrm{CS}(k)^e$.

The family of free commutative semigroups will become important in Chapters 8 and 9.

## 5.3 The Bicyclic Monoid

The bicyclic monoid is a very special monoid in many ways. It has a very simple presentation as a monoid.

$$B = \text{mon}\langle b, c \mid bc = \varepsilon \rangle$$

We will mainly use the bicyclic monoid as a counterexample. Any element of the bicyclic monoid has a representative of the form $[\mathbf{c}]^{\gamma}\,[\mathbf{b}]^{\beta}$ for $\gamma$ and $\beta$ in $\mathbb{N}$. For two elements given by the normal forms $[\mathbf{c}]^{\gamma_1}\,[\mathbf{b}]^{\beta_1}$ and $[\mathbf{c}]^{\gamma_2}\,[\mathbf{b}]^{\beta_2}$, the normal form of their product can be determined as follows.

$$([\mathbf{c}]^{\gamma_1}\,[\mathbf{b}]^{\beta_1})\,([\mathbf{c}]^{\gamma_2}\,[\mathbf{b}]^{\beta_2}) \text{ has normal form } \begin{cases} [\mathbf{c}]^{\gamma_1+\gamma_2-\beta_1}\,[\mathbf{b}]^{\beta_2} & \beta_1 \leq \gamma_2 \\ [\mathbf{c}]^{\gamma_1}\,[\mathbf{b}]^{\beta_1+\beta_2-\gamma_2} & \beta_1 > \gamma_2 \end{cases}$$

Any finite quotient of the bicyclic monoid is a group. A proof for this can be found in [CP61]. Furthermore, the bicyclic monoid is not residually finite.

**Lemma 5.3.1**

*The bicyclic monoid* B *is not residually finite.*

*Proof.* Assume for a contradiction that B is residually finite. Consider the elements $[\mathbf{cb}]\,\pi_A$ and $\mathbf{e}$ in B and note that $[\mathbf{cb}]\,\pi_A \neq \mathbf{e}$. This implies that there exists a monoid morphism $B \xrightarrow{\varphi} N$ where N is finite and such that $[\mathbf{cb}]\,\pi_A\varphi \neq \mathbf{e}\,\varphi$. Now $[\mathbf{bc}]\,\pi_A\varphi = \mathbf{e}\,\varphi$. Since N is by assumption finite, it follows that there are $i$ and $k$ in $\mathbb{N}$ such that $(b\varphi)^i = (b\varphi)^{i+k}$, and therefore $c\varphi = (b\varphi)^{k-1}$. This implies that $[\mathbf{b}]\,\pi_A\varphi$ and $[\mathbf{c}]\,\pi_A\varphi$ are in $\mathcal{U}(N)$, and mutual inverses, hence commute and therefore

$$[\mathbf{cb}]\,\pi_A\varphi = [\mathbf{bc}]\,\pi_A\varphi = \mathbf{e}_N\,.$$

This is a contradiction. □

Green's $\mathcal{R}$ and $\mathcal{L}$ relations on B are as follows. Let $s = ([\mathbf{c}]^{\gamma_1}\,[\mathbf{b}]^{\beta_1})\,\pi_A$ and $t = ([\mathbf{c}]^{\gamma_2}\,[\mathbf{b}]^{\beta_2})\,\pi_A$ be two elements of B then s and t are $\mathcal{R}$-related if and only if $\gamma_1 = \gamma_2$ and s and t are $\mathcal{L}$-related if and only if $\beta_1 = \beta_2$.

## 5.4 The Integers

The following semigroup is isomorphic to the group of integers under addition:

$$\mathrm{sg}\langle a, b \mid aab = a,\ abb = b,\ ab = ba\rangle .$$

We also show that there is a set of unique normal forms consisting of strings $[\mathbf{a}]^{\alpha}$, $[\mathbf{b}]^{\beta}$ and $[\mathbf{ab}]$ for $\alpha$ and $\beta$ in $\mathbb{N}_{>0}$.

Given a string $v$ over the generating set, by applying the relation $ab = ba$ we get the string $v' = [\mathbf{a}]^{\alpha}\,[\mathbf{b}]^{\beta}$ where $\alpha = |v|_a$ and $\beta = |v|_b$ and it holds that $v\pi_A = v'\pi_A$. By repeatedly applying the remaining relations we get either $[\mathbf{ab}]$, or $[\mathbf{a}]^{\alpha}$ or $[\mathbf{b}]^{\beta}$ for some $\alpha$ or $\beta$ in $\mathbb{N}_{>0}$ after finitely many steps.

We can also give a monoid presentation for the integers which is sometimes more convenient to work with

$$\mathrm{mon}\langle a, b \mid ab = ba = \varepsilon\rangle .$$

## 5.5 The Semigroups $\mathrm{E}(i, k)$ and $\mathrm{F}(i, k)$

The families $\mathrm{E}(i, k)$ and $\mathrm{F}(i, k)$ are two infinite families of semigroups that will serve as examples in Chapter 8. In addition to giving specifications as finite presentations we show how to determine whether two strings over the generating set represent the same element of the semigroup.

For any choice of $i$ and $k$ from $\mathbb{N}_{>0}$ let the semigroup $\mathrm{E}(i, k)$ be specified by the presentation

$$\mathrm{E}(i, k) = \mathrm{sg}\left\langle a, b \mid a^{i+k} = a^{i}, ba = a\right\rangle .$$

We want to show that for $\mathrm{E}(i, k)$ we can find an easily described set of strings that maps bijectively onto $\mathrm{E}(i, k)$, or in other words a set of normal forms.

**Lemma 5.5.1**

*The set of strings of the form* $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta}$ *with* $\alpha$ *and* $\beta$ *in* $\mathbb{N}$ *and* $0 \leq \alpha < i+k$ *and* $\alpha+\beta > 0$ *is a set of normal forms for* $E(i,k)$.

*Proof.* We show that we can obtain from any given string $v \in \{a,b\}^+$ a unique element of the set of representatives.

We proceed by induction to show that for any string $v \in \{a,b\}^+$ we can find a normal form of the desired shape. Assume we have already computed the representative $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta}$ for a string $v \in \{a,b\}^+$ of length $n$. Then

$$\begin{aligned} v[\mathbf{a}] &\text{ has representative } [\mathbf{a}]^{\alpha'} \\ v[\mathbf{b}] &\text{ has representative } [\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta+1}, \end{aligned}$$

where $\alpha' = \alpha+1$ if $0 \leq \alpha < i+k-1$ and $\alpha' = i$ if $\alpha = i+k-1$. This results in a representative of the form $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta}$ with $\alpha, \beta \in \mathbb{N}$ and $0 \leq \alpha < i+k$ and $\alpha+\beta > 0$ for every element of $E(i,k)$.

To show that this form is unique we show that two distinct strings

$$v = [\mathbf{a}]^{\alpha_1}[\mathbf{b}]^{\beta_1}, \qquad w = [\mathbf{a}]^{\alpha_2}[\mathbf{b}]^{\beta_2}$$

represent distinct elements of the semigroup.

Assume for a contradiction that this is not the case and $v\pi_A = w\pi_A$ but $\alpha_1 \neq \alpha_2$ or $\beta_1 \neq \beta_2$. Since $v$ and $w$ cannot be shortened further by applying relations, there has to be a string $u$ such that $u$ reduces to $v$ and to $w$.

Now if $0 \leq \alpha_1 < \alpha_2 < i+k$, and $\alpha_1 < i$, this would yield a contradiction, since we cannot replace any $[\mathbf{a}]^i$ by $[\mathbf{a}]^{i+k}$ in $v$. If $\alpha_1 \geq i$, but $\alpha_1 \neq \alpha_2$ we get a contradiction since $i+lk+\alpha_1 \neq i+l'k+\alpha_2$ for any choice of $l$ and $l'$ in $\mathbb{N}$. We deduce that $\alpha_1 = \alpha_2$. If $0 \leq \beta_1 < \beta_2$ we cannot apply any relation to get $u$ so we deduce $\beta_1 = \beta_2$. This contradicts the assumption that $\alpha_1 \neq \alpha_2$ or $\beta_1 \neq \beta_2$. □

It also follows that all semigroups $E(i,k)$ are infinite, since $[\mathbf{b}]^{\beta}$ is a normal form for every $\beta \in \mathbb{N}_{>0}$.

Computing a representative for the product of two elements with normal forms $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta}$ and $[\mathbf{a}]^{\alpha'}[\mathbf{b}]^{\beta'}$ is done as follows: If $\alpha' = 0$ then the representative is $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta+\beta'}$. If $\alpha' > 0$ then the representative is $[\mathbf{a}]^{\gamma}[\mathbf{b}]^{\beta'}$, where, if $\alpha+\alpha' \leq i$, then $\gamma$ is equal to $\alpha+\alpha'$, otherwise $\gamma$ is determined by the equation $\alpha + \alpha' = \gamma + qk$ for some $q \in \mathbb{N}$ such that $\gamma \in \underline{i+k-1}$.

Any semigroup $E(i,k)$ contains an infinite $\mathcal{R}$-class that contains all elements with normal forms $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta}$ for $\alpha \geq i$ and $\beta$ arbitrary. To see this, let $[\mathbf{a}]^{\alpha}[]\,b]^{\beta}$ and $[\mathbf{a}]^{\alpha'}[\mathbf{b}]^{\beta'}$ be two representatives with $\alpha = i+k_1$ and $\alpha' = i+k_2$ where $0 \leq k_1, k_2 < k$. Then

$$([\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta})\,\pi_A\,([\mathbf{a}]^{\gamma}[\mathbf{b}]^{\beta'})\,\pi_A = ([\mathbf{a}]^{\alpha'}[\mathbf{b}]^{\beta'})\,\pi_A$$

for

$$\gamma = \begin{cases} k_1 - k_2 & k_1 > k_2 \\ k_1 - k_2 + k & k_1 \leq k_2 \end{cases}.$$

The result follows by symmetry.

We can also deduce that all other elements are not $\mathcal{R}$-related and therefore $E(i,k)$ contains exactly one $\mathcal{R}-$class that is infinite. To see this consider two elements $[\mathbf{b}]^{\beta_1}$ and $[\mathbf{b}]^{\beta_2}$, where without loss of generality $\beta_1 < \beta_2$. Then $[\mathbf{b}]^{\beta_1}[\mathbf{b}]^{\beta_2-\beta_1}$ has representative $\left[\mathbf{b}^{\beta_2}\right]$, but there does not exist an element $x$ of $E(i,k)$ such that $[\mathbf{b}]^{\beta_2}x$ has representative $[\mathbf{b}]^{\beta_1}$ since multiplying by $b$ increases $\beta$, and multiplying by $a$ yields a normal form starting with $a$.

Turning to $\mathcal{L}$-classes, we see that any two elements $[\mathbf{a}]^{\alpha}[\mathbf{b}]^{\beta}$ and $[\mathbf{a}]^{\alpha'}[\mathbf{b}]^{\beta}$ where $\alpha = i + k_1$ and $\alpha' = i + k_2$ with $0 \leq k_1, k_2 < k$, are also $\mathcal{L}$-related and all other elements are not $\mathcal{L}$-related.

If we consider the semigroups $E(1,k)$, then it holds that $E(1,k)^2 = E(1,k)$ which will be of use in Section 8.6 on direct products of semigroups.

The family $F(i,k)$ of semigroups is specified by the presentation

$$F(i,k) = sg\left\langle a, b, x \mid a^{i+k} = a^i, xa = ax, ba = a, bx = x \right\rangle.$$

As above, we want to argue that every element of $F(i,k)$ has a unique representative of the form $[\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta}$ where $0 \leq \alpha < i+k$ and $\xi$ and $\beta$ are elements of $\mathbb{N}$ as well as $\alpha+\xi+\beta > 0$.

We do this by induction. Assume that for a string $\nu \in \{a,b,x\}^{+}$ of length $n$ we have computed a normal form $[\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta}$. We multiply on the right by the generators. This yields

$$\begin{aligned}
\nu\,[\mathbf{a}] &\text{ has representative } [\mathbf{a}]^{\alpha'}[\mathbf{x}]^{\xi}\\
\nu\,[\mathbf{b}] &\text{ has representative } [\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta+1}\\
\nu\,[\mathbf{x}] &\text{ has representative } [\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi+1}
\end{aligned}$$

where in the first equation $\alpha' = \alpha+1$ if $0 \leq \alpha < i+k-1$ and $\alpha' = i$ if $\alpha = i+k-1$.

Showing uniqueness of these representatives is similar to the case of $E(i,k)$. For assume that there are two distinct strings $[\mathbf{a}]^{\alpha_1}[\mathbf{x}]^{\xi_1}[\mathbf{b}]^{\beta_1}$ and $[\mathbf{a}]^{\alpha_2}[\mathbf{x}]^{\xi_2}[\mathbf{b}]^{\beta_2}$, in other words $\alpha_1 \neq \alpha_2$ or $\xi_1 \neq \xi_2$ or $\beta_1 \neq \beta_2$, such that

$$([\mathbf{a}]^{\alpha_1}[\mathbf{x}]^{\xi_1}[\mathbf{b}]^{\beta_1})\,\pi_A = ([\mathbf{a}]^{\alpha_2}[\mathbf{x}]^{\xi_2}[\mathbf{b}]^{\beta_2})\,\pi_A,$$

then it follows again that in fact $\alpha_1 = \alpha_2$, $\xi_1 = \xi_2$ and $\beta_1 = \beta_2$ and therefore a contradiction.

For any given $\xi \in \mathbb{N}$ all elements with normal forms $[\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta}$ where $\alpha = i+k_1$ with $0 \leq k_1 < k$ and $\beta \in \mathbb{N}$ are in the same $\mathcal{R}$-class, since for $[\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta}$ and $[\mathbf{a}]^{\alpha'}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta'}$, where $\alpha = i+k_1$ and $\alpha' = i+k_2$,

$$\left([\mathbf{a}]^{\alpha}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta}[\mathbf{a}]^{\gamma}[\mathbf{b}]^{\beta'}\right)\pi_A = \left([\mathbf{a}]^{\alpha'}[\mathbf{x}]^{\xi}[\mathbf{b}]^{\beta'}\right)\pi_A$$

for

$$\gamma = \begin{cases} k_1 - k_2 & k_1 > k_2 \\ k_1 - k_2 + k & k_1 \leq k_2 \end{cases}.$$

The result again follows by symmetry.

## 5.6 Finitely Generated, Infinitely Presented Semigroups

In this section we introduce a very simple example of a semigroup that is finitely generated but does not have a finite presentation. Consider the semigroup P specified by

$$P = sg\left\langle a, b \mid (ab^n a = aba)_{n\geq 2} \right\rangle.$$

This semigroup is infinite, finitely generated, cannot be finitely presented, as we will show in the following.

First we establish when two strings $v$ and $w$ over the generating set $\{a, b\}$ represent the same element of P. Consider

$$v = \prod_{i\in\underline{k}} [\mathbf{a}]^{\alpha_i} [\mathbf{b}]^{\beta_i}, \qquad w = \prod_{i\in\underline{k'}} [\mathbf{a}]^{\alpha'_i} [\mathbf{b}]^{\beta'_i},$$

where $\alpha_i$, $\alpha'_i$, $\beta'_i$ and $\beta'_i$ for $i \in \underline{k}$ are elements of $\mathbb{N}_{>0}$, with the exception of $\alpha_1$, $\alpha'_1$, $\beta_k$, and $\beta'_{k'}$, which are elements of $\mathbb{N}$. Note also that if $k$ or $k'$ is equal to one, then $\alpha_1$ and $\beta_1$ cannot both be zero, and the same holds for $\alpha'_1$ and $\beta'_1$. In this representation, the equality $v\pi_A = w\pi_A$ holds if and only if

- $k = k'$, and
- $\alpha_i = \alpha'_i$ for all $i \in \underline{k}$, and
- if $\alpha_1 = \alpha'_1 = 0$ then $\beta_1 = \beta'_1$, and
- $\beta_k = \beta'_k$.

Note that the remaining $\beta_i$ and $\beta'_i$ are arbitrary in $\mathbb{N}_{>0}$ subject to the conditions given above.

The central result required to prove Lemma 5.6.2 is is the following.

**Proposition 5.6.1**

*Let S be a semigroup that admits a finite presentation. For any presentation*

$$\mathrm{sg}\langle A \mid R\rangle$$

*of S where A is finite, there exists a finite subset* $R' \subset R$*, such that*

$$\mathrm{sg}\langle A \mid R'\rangle$$

*is a finite presentation of S.*

This proposition is valid in general abstract algebra. For groups this is attributed to B.H. Neumann by Baumslag in [Bau93, Chapter III, Theorem 12]. The relevant result for semigroups can be found in [Rus95, Proposition 1.3.1].

We show that P is infinite and does not admit a finite presentation.

**Lemma 5.6.2**

*The semigroup* P *is infinite and there does not exist a finite presentation for* P*.*

*Proof.* Firstly P is infinite, since by the results of the above paragraph the subsemigroup generated by $a$ is infinite. Secondly, P cannot be finitely presented. For this first note that if a semigroup is finitely presented with respect to some generating set, then it is finitely presented with respect to all generating sets. We can therefore consider the generating set $\{a, b\}$. We apply Proposition 5.6.1 for a contradiction. Assume that there is a finite set $X \subseteq \{ab^n a = aba \mid n \geq 2\}$ such that $P \cong \mathrm{sg}\langle a, b \mid X\rangle$.

This means that there is an $n_0 \in \mathbb{N}$ such that for all $k > n_0$ the equality

$$([\mathbf{a}]\,[\mathbf{b}]^k\,[\mathbf{a}])\,\pi_A = [\mathbf{aba}]\,\pi_A$$

can be deduced in finitely many steps from relations in X. This is impossible since we cannot apply any equality resulting from X, since each relation in X has the form

$$([\mathbf{a}]\,[\mathbf{b}]^n\,[\mathbf{a}])\,\pi_A = [\mathbf{aba}]\,\pi_A$$

for some $n < k$. □

## 5.7 An Extension of Finite Green Index and Infinite Rees Index

We give an example of a semigroup $M$ that has a subsemigroup $N$ of finite Green index but infinite Rees index. Let

$$M = \mathrm{mon}\Big\langle a, b, c, d \mid \begin{array}{l} ac = ca = c^2,\ ad^2 = d^2a = d \\ bd = db = d^2,\ bc^2 = c^2b = c \\ dc^2 = c,\ cd^2 = d,\ cd = dc \end{array} \Big\rangle$$

and let $N$ be the submonoid of $M$ generated by $a$ and $b$. Observe that $N$ is isomorphic to the free monoid on $\{a, b\}$.

The complement $Z = M \backslash N$ is an infinite group. To see this note that the subsemigroup generated by $c$ and $d$ has the presentation

$$Z = \mathrm{sg}\Big\langle c, d \mid dc^2 = c,\ cd^2 = d,\ cd = dc \Big\rangle,$$

and is therefore isomorphic to the group of integers.

It follows that all elements in $Z$ can be represented by strings of the form $[\mathbf{c}]^i$, $[\mathbf{d}]^i$ and the string $[\mathbf{cd}]$.

We want to show that all elements in $Z$ are $\mathcal{H}^N$-related and therefore the Green index of $N$ in $M$ is 2.

For this we show that every $x \in Z$ is $\mathcal{R}^N$-related to $[\mathbf{cd}]\,\pi_A$, that is there exist $v$ and $w$ in $N$ such that $xv = [\mathbf{cd}]\,\pi_A$ and $[\mathbf{cd}]\,\pi_A w = x$. We can assume $x$ to be represented by a string in normal form, that is $x = [\mathbf{cd}]\,\pi_A$, $x = [\mathbf{c}]^i\,\pi_A$ or $x = [\mathbf{d}]^i\,\pi_A$. If $x = [\mathbf{cd}]\,\pi_A$ then it is immediate that $x$ and $[\mathbf{cd}]\,\pi_A$ are $\mathcal{R}^N$-related. If $x = [\mathbf{c}]^i\,\pi_A$, then $v = [\mathbf{b}]^i\,\pi_A$ and $w = [\mathbf{a}]^i\,\pi_A$ have the desired properties, and if $x = [\mathbf{d}]^i\,\pi_A$ then $v = [\mathbf{a}]^i\,\pi_A$ and $w = [\mathbf{b}]^i\,\pi_A$ have the desired properties. Symmetric arguments yield that every $x$ in $Z$ is $\mathcal{L}^N$-related to $[\mathbf{cd}]\,\pi_A$. This shows that all elements in $Z$ are $\mathcal{H}^N$-related, and therefore that $N$ has finite Green index in $M$.

## 5.8 A semigroup with undecidable word problem

For completeness we give a semigroup that has undecidable word problem. We give an example constructed by Tzeitin [G S58].

Let

$$\begin{aligned} T = \mathrm{mon}\Big\langle a, b, c, d, e \mid\ & ac = ca,\ ad = da,\ bc = cb,\ bd = db \\ & eca = ce,\ edb = de,\ cdca = cdcae \\ & ca^3 = a^3,\ da^3 = a^3 \Big\rangle \end{aligned}$$

This semigroup has undecidable word problem. Moreover, there is no Turing machine that decides whether a given string $v$ over the generating set represents the same element as [**aaa**]. While the presentation of this semigroup has a very small number of generators and relations there are semigroups with undecidable word problem that have finite presentations with as little as two generators and three relations. The construction of such a semigroup can be found in [Mat95]. One of the relations in the two generator and three relator semigroup has a total of 912 letters: 304 for the left hand side and 608 for the right hand side and arguably the example given above is smaller.

# 6

○ ● ⊙

# *Word Problems and Coword Problems*

We give a short historical motivation starting from group theory and a natural way of defining the *word problem* and the *coword problem* for semigroups. Solving the word problem for a finitely generated semigroup is deciding whether two strings over the generating set represent the same element of the semigroup.

We further generalise the notion of word problem to arbitrary relations over finitely generated semigroups and give a quick survey of possible encodings of semigroup word problems as strings.

## *6.1 Dehn's Identitätsproblem*

The *word problem* of a finitely generated group has first been recognised as one of the central problems in the theory of infinite finitely presented groups by

Max Dehn in 1911 in [Deh11]. Dehn himself attributes the definition of groups by generators and relations to Dyck. Quoting from [Deh11]

> Die allgemeine Theorie derartig definierter Gruppen, sofern sie unendlich sind, scheint bisher sehr wenig entwickelt zu sein. Hier sind es vor allem *drei fundamentale Probleme,* deren Lösung sehr wichtig und wohl nicht ohne eindringliches Studium der Materie möglich ist.

The author's translation of the preceding quote into English is as follows.

> The general theory of groups defined in that way, as long as they are infinite, seems to be not well understood yet. There are *three fundamental problems* whose solution is very important and probably not possible without close study of the topic.

Dehn then goes on to define the "Identitätsproblem" as the first of the three fundamental problems in the theory of finitely presented, infinite groups. We quote again:

> *Das Identitätsproblem*: Irgend ein Element der Gruppe ist durch seine Zusammensetzung aus den Erzeugenden gegeben. Man soll eine Methode angeben, um mit einer endlichen Anzahl von Schritten zu entscheiden, ob dies Element der Identität gleich ist oder nicht.

Which translates into English as follows.

> *The Identitätsproblem*: Some element of the group is given by a composition of the generating elements. Give a method that decides, using only a finite amount of steps, whether this element is equal to the identity or not.

The Identitätsproblem is today commonly known in the English speaking mathematics community as the *word problem*. The other two fundamental problems are the conjugacy problem and the isomorphism problem. We note that Max Dehn stated these problems before any rigorous theory of computation was developed. What he calls "a method" would today be translated as *an algorithm*.

We translate Dehn's definition into our formal language as follows. The *Identitätsproblem* or *word problem* of a group $G$ which is finitely generated as a monoid by a set $A$ is the set

$$W_G(A) = \{v \in A^* \mid v\pi_A = \mathbf{e}_G\} \tag{6.1}$$

of all the representatives of the identity element.

Given $W_G(A)$ and two representatives $v$ and $w$ in $A^*$, one important question we asked earlier is testing whether the equation $v\pi_A = w\pi_A$ holds, or in other words, whether they are *identical*. In the case of groups this can be done by deciding whether $vw'$ is an element of $W_G(A)$, where $w'$ is a representative of $(w\pi_A)^{-1}$. In the theory of finitely presented groups we usually have an effective way of determining $w'$, because it is commonly assumed that for every generator $a \in A$ there is also a generator $a' \in A$ such that $[\mathbf{aa}']\,\pi_A = \mathbf{e}$. Determining $w'$ is then done by replacing every letter $a$ in $w$ by $a'$ and then reversing the resulting string.

The dual question to the word problem is stated in the *coword problem*.

$$\mathrm{CoW}_G(A) = \{v \in A^* \mid v\pi_A \neq \mathbf{e}_G\}. \tag{6.2}$$

The coword problem of groups has only recently attracted some attention. In their paper "Groups with context-free coword problem" [Hol+05], Holt, Rees, Röver and Thomas examine properties of groups $G$ such that $\mathrm{CoW}_G(A)$ can be decided by a pushdown automaton. They also show that polycyclic groups and Baumslag solitar groups have context-free coword problem if and only if they are virtually abelian. Lehnert and Schweitzer show in [LS07] that the

coword problem of the Higman-Thompson group is context-free. It is shown in [MS83; MS85] that the word problem of a group is context free if and only if the group is virtually free.

The word problem and the coword problem are *decision problems*: the problem is to decide whether a string over an alphabet is a member of a particular subset of the set of all strings. The word problem and the coword problem of a group are defined in terms of representatives of the identity element.

## 6.2 The Identitätsproblem for Semigroups

We generalise the notion of the Identitätsproblem to semigroups in a way that is consistent with the definition for groups. In the process we will have to abandon the notion of finding representatives of the identity, because it is a special property of groups that the set of representatives of the identity already contains all the information about equality. We will see that the notion of identity still exists in the definition.

To find a natural definition for semigroups, we realise that we want to decide for two strings $v$ and $w$ over the generating set whether the *equality* $v\pi_A = w\pi_A$ holds, in other words $v$ is in the same equivalence class of the kernel of $\pi_A$ as $w$.

We define the monoid word problem of a group G generated as a monoid by a set A to be the relation

$$\iota_G(A) : A^* \longrightarrow A^*, v \mapsto v\pi_A\pi_A^{-1} \tag{6.3}$$

which can also be written as the following composition of relations

$$A^* \xrightarrow{\pi_A} G \xrightarrow{\iota_G} G \xrightarrow{\pi_A^r} A^*,$$

and has the graph

$$\mathcal{G}_{\iota_G(A)} = \{(v, w) \in A^* \times A^* \mid v\pi_A = w\pi_A\}.$$

The *relation* $\iota_G(A)$ is an equivalence equation and a congruence, namely the kernel of the monoid morphism $A^* \xrightarrow{\pi_A} G$. We can find $W_G(A)$ as the equivalence class of the identity element of G. We also note that the equivalence relation $\iota_G(A)$ is the lift of the the *equality relation* of G to the set of all strings over the generating set, and that the equality relation is itself the *identity map* of the set G interpreted as a relation.

The definition given in 6.3 does not depend on G being a group anymore, and therefore we can generalise to any semigroup $S$ generated by a set $A$ and say that

$$\iota_S(A) : A^+ \longrightarrow A^+, \nu \mapsto \nu\pi_A\pi_A^{-1} \tag{6.4}$$

is the *semigroup word problem of S with respect to the generating set* A. Note again the factorisation

$$A^* \xrightarrow{\pi_A} S \xrightarrow{\iota_S} S \xrightarrow{\pi_A^r} A^*$$

of $\iota_S(A)$. We also note that we can define the word problem of $S$ to be a relation on $A^*$. If S is not a monoid then this relation is not total anymore and therefore not an equivalence relation. Since we can always make a semigroup S into a monoid by adding an identity and since the notions of interest for us will be invariant under this operation, we will usually choose to view the word problem as a relation over $A^*$.

The preceding definition also allows for a straightforward definition of the *semigroup coword problem of S with respect to the generating set* A as

$$\bar{\iota}_S(A) : A^+ \longrightarrow A^+, \nu \mapsto A^+ \backslash \nu\pi_A\pi_A^{-1}.$$

The coword problem, as opposed to the word problem, is not an equivalence relation or a congruence relation.

## 6.3 The Word Problem for Relations

We now extend the notion of the Identitätsproblem to relations over semigroups. In this general setting we will refer to the relation defined over strings to the *word problem of the relation over the generating set*. We will still call the word problem of the identity relation the word problem if no ambiguity arises.

We saw in Section 6.2 that the definition of the word problem involves the equality relation on a finitely generated semigroup $S$ which is lifted to strings over the generating set. Our definition did not depend on any properties of the equality relation and therefore we make the following definition. Let $S$ be a semigroup, finitely generated by $A$, and let $S \xrightarrow{\rho} S$ be a relation on $S$. We define the *word problem* $A^+ \xrightarrow{\rho(A)} A^+$ of $\rho$ with respect to the generating set $A$ by the composition

$$A^+ \xrightarrow{\pi_A} S \xrightarrow{\rho} S \xrightarrow{\pi_A^r} A^+.$$

Relations of particular interest will be Green's $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, $\mathcal{D}$ and $\mathcal{J}$ relations with respect to a generating set $A$.

Note that the above definition includes the choice of a generating set. One might be tempted to choose two generating sets and have the equivalent of a basis change in linear algebra. We choose to not pursue this path here, since all properties of interest are invariant under the choice of generating set.

## 6.4 Encodings

The generalised notion of word problem introduced in Sections 6.2 and 6.3 has a natural encoding in terms of pairs of strings or as a relation, but not as a single string as it is the case in 6.1. Sometimes it is desirable to encode pairs as single strings as inputs for some models of computation, therefore we define the following two ways to do so.

We define the *one-tape encoded semigroup word problem* ${}_1\iota_S(A)$ to be the set

$$ {}_1\iota_S(A) = \left\{ v\#w^r \in A^+\#A^+ \mid v\pi_A = w\pi_A \right\} \subseteq (A \cup \{\#\})^* , $$

where # is a new symbol that is not an element of $A$. It will become clear in Chapter 10, where we discuss the relationships between one-tape encoded and two-tape word problems, why we reverse the second string.

The *two-tape padded semigroup word problem* is defined as

$$ \iota_S^{\square}(A) = \left\{ (v, w)^{\square} \in \left(A^{\square} \times A^{\square}\right)^+ \mid v\pi_A = w\pi_A \right\}, $$

where for an alphabet $A$ and a *padding symbol* $\square$ not contained in $A$ we define $A^{\square} = A \cup \{\square\}$ and $(v, w)$ in $A^+ \times A^+$ with $|v| = k$ and $|w| = n$ we define

$$ (v, w)^{\square} = \begin{cases} \begin{bmatrix} v_1 \\ w_1 \end{bmatrix} \cdots \begin{bmatrix} v_k \\ w_k \end{bmatrix} \begin{bmatrix} \square \\ w_{k+1} \end{bmatrix} \cdots \begin{bmatrix} \square \\ w_n \end{bmatrix} & k < n \\ \begin{bmatrix} v_1 \\ w_1 \end{bmatrix} \cdots \begin{bmatrix} v_k \\ w_k \end{bmatrix} & k = n \, . \\ \begin{bmatrix} v_1 \\ w_1 \end{bmatrix} \cdots \begin{bmatrix} v_n \\ w_n \end{bmatrix} \begin{bmatrix} v_{n+1} \\ \square \end{bmatrix} \cdots \begin{bmatrix} v_k \\ \square \end{bmatrix} & k > n \end{cases} $$

# 7

○●●

# *Recognisable Word Problem*

Following the structure of Chapter 3, we first analyse semigroups that have recognisable word problem.

## *7.1 Anisimov's Theorem*

One of the first results that links word problems to formal language theory is Anisimov's theorem in [Ani71]. We restate Anisimov's theorem in the language introduced in Chapters 6 and 3.

**Theorem 7.1.1**

*Let* $G$ *be a group finitely generated as a monoid by* $A$*. Then* $W_G(A)$ *is a recognisable subset of* $A^*$ *if and only if* $G$ *is finite.*

*Proof.* Let $G$ be a group finitely generated as a monoid by $A$. The monoid morphism $A^* \xrightarrow{\pi_A} G$ maps strings over the generating set to elements of $G$.

If $G$ is finite, then $A^* \xrightarrow{\pi_A} G$ recognises $W_G(A)$ because $W_G(A) = \mathbf{e}_G\varphi^{-1}$.

Conversely, assume that there exists a morphism $A^* \xrightarrow{\varphi} T$ where $T$ is finite and $F \subset T$ such that $W_G(A) = F\varphi^{-1}$. We want to show that there is a surjective morphism $T \xrightarrow{\psi} G$. Observe that by assumption $v\varphi \in F$ if and only if $v\pi = \mathbf{e}_G$ and that for any $v \in A^*$ there exists a $v' \in A^*$ such that $vv'\varphi \in F$. Assume now $w \in v \ker \varphi$, so $v\varphi = w\varphi$. There exists $v' \in A^*$ such that $vv'\varphi \in F$ and hence $wv'\varphi \in F$ because $vv'\varphi = wv'\varphi$. It follows that $vv'\pi = wv'\pi$ from which we conclude $v\pi = w\pi$, which means that $w \in v \ker \pi$. It follows by the second isomorphism theorem for semigroups that there is a surjective morphism $T \xrightarrow{\psi} G$. This means that $G$ is a quotient of $T$ and hence finite. such that $A \xrightarrow{\varphi} T$ recognises $W_G(A)$. □

The family $\operatorname{Rec} A^*$ of recognisable subsets of $A^*$ is a Boolean algebra and therefore we get the following theorem.

**Theorem 7.1.2**

*Let $G$ be a group finitely generated as a monoid by $A$. Then the following statements are equivalent.*

1. $G$ *is finite.*
2. $W_G(A)$ *is a recognisable subset of* $A^*$.
3. $\mathrm{Co}W_G(A)$ *is a recognisable subset of* $A^*$.

*Proof.* The equivalence of 1 and 2 is exactly the statement of Theorem 7.1.1. The equivalence of 2 and 3 follows from the fact that the family of recognisable subsets of $A^*$ is a Boolean algebra. □

## 7.2 An Analogue of Anisimov's Theorem for Semigroups

In Chapter 6 we defined word problems and coword problems for groups and semigroups, and we have seen when the word problem of a group is a

recognisable subset of the set of all strings over the generating set. We now show that a similar result can be shown for the word problem of a semigroup $S$. This characterises all semigroups with recognisable word problem.

**Theorem 7.2.1**

*Let $S$ be a semigroup generated by the finite set $A$. Then $\iota_S(A)$ is recognisable if and only if $S$ is finite.*

*Proof.* Let $\iota_S(A)$ be recognisable. Note that without loss of generality we can consider $\mathcal{G}_{\iota_S(A)}$ to be a subset of $A^* \times A^*$, as $A^+ \times A^+$ is a recognisable subset of $A^* \times A^*$ and recognisable subsets of monoids are closed under intersection. Proposition 3.6.2 allows us to write

$$\mathcal{G}_{\iota_S(A)} = \bigcup_{i \in \underline{n}} X_i \times Y_i,$$

where $X_i$ and $Y_i$ are recognisable subsets of $A^*$ for all $i \in \underline{n}$.

Now if $w \in \nu\iota_S(A)$, then by the above $Y_i \subseteq \nu\iota_S(A)$. This implies that each equivalence class is a union of sets $Y_i$ for $i \in I \subseteq \underline{n}$. Therefore there are only finitely many equivalence classes, hence $S$ is finite.

Conversely let $S$ be finite. Then $S^e \times S^e$ is finite and recognises $\mathcal{G}_{\iota_S(A)}$ via

$$\varphi : A^* \times A^* \to S^e \times S^e : (v, w) \mapsto (v\pi_A, w\pi_A)$$

and $F = \{(s, s) \in S^e \times S^e \mid s \in S\}$. □

Therefore Theorem 7.1.2 naturally generalises to semigroups.

**Theorem 7.2.2**

*Let $S$ be a semigroup finitely generated by a set $A$. Then the following statements are equivalent.*

1. *$S$ is finite.*
2. *$\iota_S(A)$ is recognisable.*
3. *$\bar{\iota}_S(A)$ is recognisable.*

The above theorem also motivates the following question. As shown above, the direct product of two copies of the semigroup in question recognises the word problem, but in the case of a finite group, the group itself suffices.

**Open Question 7.2.1**

*Let $S$ be a finite semigroup and let $A$ be a finite generating set for $S$. Applying Theorem 7.2.1 yields that $\iota_S(A)$ is recognisable, that is there is a semigroup morphism $A^* \times A^* \xrightarrow{\varphi} T$ where $T$ is finite and a subset $F \subset T$ such that $\mathcal{G}_{\iota_S(A)} = F\varphi^{-1}$. Describe the structure of the syntactic quotient of $T$ that recognises $\iota_S(A)$. Is there a characterisation of minimal semigroups recognising word problems?*

## 7.3 *Changing the Encoding*

In Section 7.2 we we have characterised the class of semigroups with recognisable word problem. Now we consider the free semigroup on a generating set $A$ and the padded representation of pairs. The padded semigroup word problem of $A^+$ is a recognisable subset of $(A \times A)^\square$. Changing the generating set of $A^+$ to anything containing an additional generator, the padded word problem is not recognisable anymore. In general the following theorem holds.

**Theorem 7.3.1**

*Let $S$ be a finitely generated semigroup. Then $\iota_S^\square(A)$ is recognisable for all possible choices of finite generating sets $A$ if and only if $S$ is finite.*

*Proof.* Let $S$ be a finite semigroup and let $A$ be any generating set for $S$. Consider the semigroup morphism

$$\left(A^\square \times A^\square\right)^* \xrightarrow{\varphi} S^e \times S^e,$$

defined by the map

$$f : A^\square \longrightarrow S^e,\ x \mapsto \begin{cases} x\pi_A & x \in A \\ 1 & x = \square \end{cases}$$

extended to a morphism on pairs. With the choice

$$F = \{(s, s) \in S^e \times S^e \mid s \in S\}$$

the morphism $\varphi$ recognises strings over $(A \times A)^\square$ that represent pairs of equal elements of S. If we intersect $F\varphi^{-1}$ with the recognisable set

$$(A \times A)^+ \left( (\{\square\} \times A)^* \cup (A \times \{\square\})^* \right),$$

then we get $\iota_S^\square(A)$, which is recognisable as an intersection of recognisable sets.

To prove the converse we apply Theorem 8.3.4 which is proven in a later chapter. Assume that S is infinite. If there does not exist a finite generating set for which $\iota_S^\square(A)$ is recognisable we are done. In the case that there exists some generating set A such that $\iota_S^\square(A)$ is recognisable, by Theorem 8.3.4 there exists $s \in S$ such that the subsemigroup generated by s is infinite. We form a new generating set B by adding two generators a and b with $a\pi_B = s$ and $b\pi_B = s^2$. Applying iteration lemma given in Theorem 3.2.4 to the pair $\left(a^{2n}, b^n\right)$ yields that $\iota_S^\square(B)$ is not recognisable. □

We note that every semigroup S such that there exists a finite generating set A for S such that the padded semigroup word problem of S is recognisable has rational word problem in the sense introduced in Chapter 8. The following lemma shows that there does not exist a finite generating set for the semigroup P, defined in Section 5.6 such that the padded two tape semigroup word problem of P is a recognisable subset of $(A \times A)^\square$.

**Lemma 7.3.2**

*There does not exist a finite generating set A for P such that $\iota_P^\square(A)$, as defined in 5.6 is recognisable.*

*Proof.* We first show that for the generating set $A = \{a, b\}$ given in Section 5.6 the word problem $\iota_P^\square(A)$ is not recognisable. For a contradiction assume that

there is a finite state automaton that recognises $\iota_P^{\square}(A)$ with $n_0$ states. Choose $n > n_0$ and consider the pair

$$\left([\mathbf{ab}]^n [\mathbf{a}] [\mathbf{b}]^{2n} [\mathbf{a}], [\mathbf{a}] [\mathbf{b}]^{2n} [\mathbf{ab}]^n [\mathbf{a}]\right).$$

Since $n > n_0$ there are natural numbers $i$ and $j$ with $i < j$ such that after reading $([\mathbf{ab}]^i, [\mathbf{a}] [\mathbf{b}]^{2i-1})$ and after reading $([\mathbf{ab}]^j, [\mathbf{a}] [\mathbf{b}]^{2j-1})$ the automaton is in the same state from which it can reach an accept state by reading $([\mathbf{a}] [\mathbf{b}]^{2i-3} [\mathbf{a}], [\mathbf{ab}]^{i-1} [\mathbf{a}])$. This implies that the automaton also accepts

$$\left([\mathbf{ab}]^j [\mathbf{a}] [\mathbf{b}]^{2i-3} [\mathbf{a}], [\mathbf{a}] [\mathbf{b}]^{2j-1} [\mathbf{ab}]^{i-1} [\mathbf{a}]\right),$$

which would imply that $[\mathbf{ab}]^{j+1} [\mathbf{a}] \pi_A$ is equal to $[\mathbf{ab}]^{i+1} [\mathbf{a}] \pi_A$ which is a contradiction to $i < j$.

Since every generating set for P has to contain representatives for $a\pi_A$ and $b\pi_A$, the same argument can be applied to any finite generating set P. □

For the remainder of this work, we want to insist on notions to be invariant under choice of finite generating sets and will therefore consider rational relations in the following chapters. We close this section with the following question.

**Open Question 7.3.1**

*Characterise the class of semigroups S such that there exists a finite generating set A for S such that the padded semigroup word problem of S is a recognisable subset of* $(A \times A)^{\square}$.

# 8

○ ● ○

# *Rational Word Problem*

This chapter will treat semigroups with rational word problem. The goal is to find a description of as many properties as possible of semigroups that have rational word problem. One of the main goals of this theory is characterising all semigroups with rational word problem, which is unfortunately not achieved.

In Section 8.1 we will show that if the word problem of any relation $S \xrightarrow{\rho} S$ on a finitely generated semigroup $S$ is rational for one finite generating set of $S$, then the word problem of $\rho$ is rational with respect to any choice of finite generating set.

In Section 8.2 we will show that the family of semigroups with rational word problem contains some of the semigroups introduced in Chapter 5 by giving automata that decide the respective word problems. We will also show that some of the examples introduced in Chapter 5 do not have rational word problem.

In the following section we show that a semigroup $S$ has rational word

problem if and only if $S^e$ has rational word problem, and if and only if $S^z$ has rational word problem.

In a more general setting, in Section 8.5, we show that rational word problem is closed under subsemigroups of finite Rees index and extensions of finite Rees index and under subsemigroups of finite Green index. We also give an example of a semigroup that has a subsemigroup of finite Green index with rational word problem, but does not have rational word problem itself.

In Section 8.4 we show that Kleene's Theorem holds in semigroups with rational word problem, and in particular that the preimage of a rational subset of a semigroup with rational word problem is a rational subset of the set of all strings over the generating set.

Following that we continue in Section 8.6 to examine under which of the product constructions, namely direct product, semigroup free product and monoid free product, rational word problem is preserved. A consequence of this will also be that semigroups with rational word problem are residually finite.

Green's relations are then examined in Section 8.7. We show properties of the $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{H}$ relations on semigroups with rational word problem. An infinite semigroup with rational word problem has infinitely many $\mathcal{R}-$classes and infinitely many $\mathcal{L}$-classes, and $\mathcal{H}$-classes are finite and therefore subgroups of semigroups with rational word problem are finite. We also show that for semigroups with rational word problem $\mathcal{J} = \mathcal{D}$ holds.

Sections 8.8 then considers decidability of the property of a semigroup having rational word problem, and the decidability of different questions for semigroups with rational word problem. In Section 8.9 we give a bound for the time and space complexity of the word problem of a semigroup with rational word problem. We also note that specifying a rational relation, either in form of a rational expression or in the form of an automaton is an efficient and effective way of specifying infinite semigroups, in particular some semi-

groups which are not finitely presented.

Some of the results in this chapter have been submitted as a research paper [NPR11], which is awaiting referee's feedback and is available on the arXiv.

## 8.1 Rational Relations and Change of Generators

For a semigroup $S$ finitely generated by $A$ we now consider relations $S \xrightarrow{\rho} S$ such that $A^+ \xrightarrow{\rho(A)} A^+$ is a rational relation. We show that this property of $S \xrightarrow{\rho} S$ does not depend on the choice of the generating set, as long as it is finite. We will, by slight abuse of nomenclature, call a relation $\rho$ such that $\rho(A)$ is rational a *rational relation*.

We first remove generators from a generating set.

**Lemma 8.1.1**

*Let $S$ be a semigroup and let $S \xrightarrow{\rho} S$ be a relation on $S$. If for some generating set $A$ of $S$ the relation $\rho(A)$*

$$A^+ \xrightarrow{\pi_A} S \xrightarrow{\rho} S \xrightarrow{\pi_A^r} A^+ \tag{8.1}$$

*is rational, then for any subset $B \subset A$ the restriction of $\rho$ to the subsemigroup $T$ of $S$ generated by $B$, in other words the relation $\rho(B)$*

$$B^+ \xrightarrow{\pi_B} T \xrightarrow{\rho} T \xrightarrow{\pi_B^r} B^+$$

*is rational.*

*Proof.* Let $S \xrightarrow{\rho} S$ be a relation on a semigroup $S$ which is finitely generated by $A$ and let $B \subset A$. The embedding

$$\epsilon : B^+ \longrightarrow A^+, v \mapsto v$$

is a rational relation and therefore the composition

$$B^+ \xrightarrow{\epsilon} A^+ \xrightarrow{\pi_A} S \xrightarrow{\rho} S \xrightarrow{\pi_A^r} A^+ \xrightarrow{\epsilon^r} B^+ \tag{8.2}$$

is rational given the assumption in 8.1. It remains to show that $\rho(B)$ is equal to the composition given in 8.2. We note that $\pi_B = \epsilon\pi_A$ and therefore conclude for $v$ and $w$ from $B^+$ that $w \in v\rho(B)$ if and only if $w\pi_B \in (v\pi_B)\,\rho$, which is the case if and only if $w\epsilon\pi_A \in (v\epsilon\pi_A)\,\rho$. This concludes the proof. □

Adding generators also does not change the property of a relation being rational.

**Lemma 8.1.2**

*Let $S$ be a semigroup and let $S \xrightarrow{\rho} S$ be a relation on $S$. If for some generating set $A$ of $S$ the relation $\rho(A)$*

$$A^+ \xrightarrow{\pi_A} S \xrightarrow{\rho} S \xrightarrow{\pi_A^r} A^+ \tag{8.3}$$

*is rational, then for any finite generating set $B \supset A$ the relation $\rho(B)$*

$$B^+ \xrightarrow{\pi_B} S \xrightarrow{\rho} S \xrightarrow{\pi_B^r} B^+$$

*is rational.*

*Proof.* Since $A$ is a generating set for $S$, we can choose $v_b \in b\pi_B\pi_A^{-1}$ for all $b \in B\backslash A$ and define

$$f : B \longrightarrow A^+,\ x \mapsto \begin{cases} x & x \in A \\ v_x & x \in B\backslash A \end{cases}$$

which by Definition 2.7.1 uniquely extends to a semigroup morphism $B^+ \xrightarrow{\varphi} A^+$. The morphism $\varphi$ can be regarded as a rational relation, because its graph is a rational subset of $B^+ \times A^+$ defined by the rational expression

$$\left(\bigcup_{b\in B} (b, b\varphi)\right)^+.$$

The composition

$$B^+ \xrightarrow{\varphi} A^+ \xrightarrow{\pi_A} S \xrightarrow{\rho} S \xrightarrow{\pi_A^r} A^+ \xrightarrow{\varphi^r} B^+ \tag{8.4}$$

is rational since by assumption $\rho(A)$ is rational. Denote 8.4 by $\gamma$. We show that $\gamma = \rho(B)$. For this we first observe that $\pi_B = \varphi\pi_A$ and we have

$$\begin{aligned} w \in v\gamma &\Leftrightarrow w\varphi \in v\varphi\rho(A) \\ &\Leftrightarrow w\varphi\pi_A \in v\varphi\pi_A\rho \\ &\Leftrightarrow w\pi_B \in v\pi_B\rho \\ &\Leftrightarrow w \in v\rho(B)\,. \end{aligned}$$

This concludes the proof. □

Therefore, if $\rho(A)$ is rational with respect to the generating set $A$ of $S$ then $\rho(B)$ is rational with respect to any finite generating set $B$ of $S$.

**Theorem 8.1.3**

*Let $S$ be a semigroup and let $S \xrightarrow{\rho} S$ be a relation on $S$. If for some finite generating set $A$ of $S$ the relation $\rho(A)$*

$$A^+ \xrightarrow{\pi_A} S \xrightarrow{\rho} S \xrightarrow{\pi_A^r} A^+ \tag{8.5}$$

*is rational, then for all finite generating sets $B$ of $S$ the relation*

$$B^+ \xrightarrow{\pi_B} S \xrightarrow{\rho} S \xrightarrow{\pi_B^r} B^+$$

*is rational.*

*Proof.* We apply Lemmas 8.1.1 and 8.1.2 . Let $S$ be a semigroup and $S \xrightarrow{\rho} S$ be a relation on $S$ such that $\rho(A)$ is rational for some finite generating set $A$. Let $B$ be any finite generating set of $S$. The union $A \cup B$ is a finite generating set of $S$ with $A \cup B \supset A$ and therefore

$$(A \cup B)^+ \xrightarrow{\pi_{A\cup B}} S \xrightarrow{\rho} S \xrightarrow{\pi_{A\cup B}^r} (A \cup B)^+$$

is rational by Lemma 8.1.2. Now $B \subset (A \cup B)$ and by Lemma 8.1.1 the claim follows. □

As a consequence of the preceding theorems we will say that a semigroup $S$ has *rational word problem* if $\iota_S(A)$ is rational for some finite generating set $A$ of $S$. We will say that a semigroup has rational $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, $\mathcal{D}$ or $\mathcal{J}$ if the respective relation $\mathcal{R}(A)$, $\mathcal{L}(A)$, $\mathcal{H}(A)$, $\mathcal{D}(A)$ or $\mathcal{J}(A)$ is rational for some finite generating set $A$ of $S$.

## 8.2 Examples

Every concept should come with a collection of examples *and* counterexamples to place it firmly within a greater picture of the surrounding theory.

We go through some of the examples presented in Chapter 5 and show whether they have rational word problem. For this we observe that we can prove rationality of relations by giving a rational expression or by giving a generalised $A^+ \times A^+$—automaton. Also we can give rational relations as compositions of other rational relations or intersections of rational relations with recognisable relations.

Firstly, by Theorem 7.2.1 every finite semigroup has recognisable word problem and therefore rational word problem.

Furthermore for a finite set $A$ the free semigroup $A^+$ is infinite and has rational word problem.

**Lemma 8.2.1**

*Let $A$ be a finite set, then $\iota_{A^+}(A)$ is rational.*

*Proof.* The relation

$$\iota_{A^+}(A) : A^+ \longrightarrow A^+, v \mapsto v$$

is the identity relation and therefore rational. A rational expression for the graph of $\iota_{A^+}(A)$ can be given as

$$\left( \bigcup_{a \in A} (a, a) \right)^+.$$

To make sure the class of semigroups with rational word problem does not consist of finite semigroups and free semigroups we show that for any choice of $i$ and $k$ in $\mathbb{N}_{>0}$ the semigroup $E(i,k)$ has rational word problem. We note that this also holds for $F(i,k)$ and the proof is very similar. This will also illustrate that it can be convenient to use automata to specify subsets of $A^+$ or relations $A^+ \xrightarrow{\rho} A^+$.

To show how word problem automata work, we start with an automaton that decides the word problem of the semigroup $E(4,5)$. The automaton depicted in Figure 8.1 decides the word problem of the semigroup $S = \mathrm{sg}\langle a \mid a^4 = a^9 \rangle$, which is isomorphic to the subsemigroup of $E(4,5)$ generated by $a$. Note the similarity to the Cayley graph of $S$.

To decide the full word problem of $E(4,5)$, we add in states to deal with reading $b$ and the relation $ba = a$. The resulting automaton is shown in Figure 8.2. To make this illustration complete for $E(i,k)$ we give the specification of a finite automaton $\mathcal{A}$ that decides $\iota_{E(i,k)}(\{a,b\})$. For

$$X = \{(a,\varepsilon), (b,\varepsilon), (\varepsilon,a), (\varepsilon,b)\}$$

we specify the $X$−automaton

$$\mathcal{A} = \left\langle Q, q_0, F, (\xrightarrow{x})_{x\in X} \right\rangle$$

where $Q = \{q_0\} \cup \{a_0, ..., a_{i+k-1}\} \cup \{a_0^l, ..., a_{i+k-1}^l\} \cup \{a_0^r, ..., a_{i+k-1}^r\} \cup \{b_0, b_1\}$

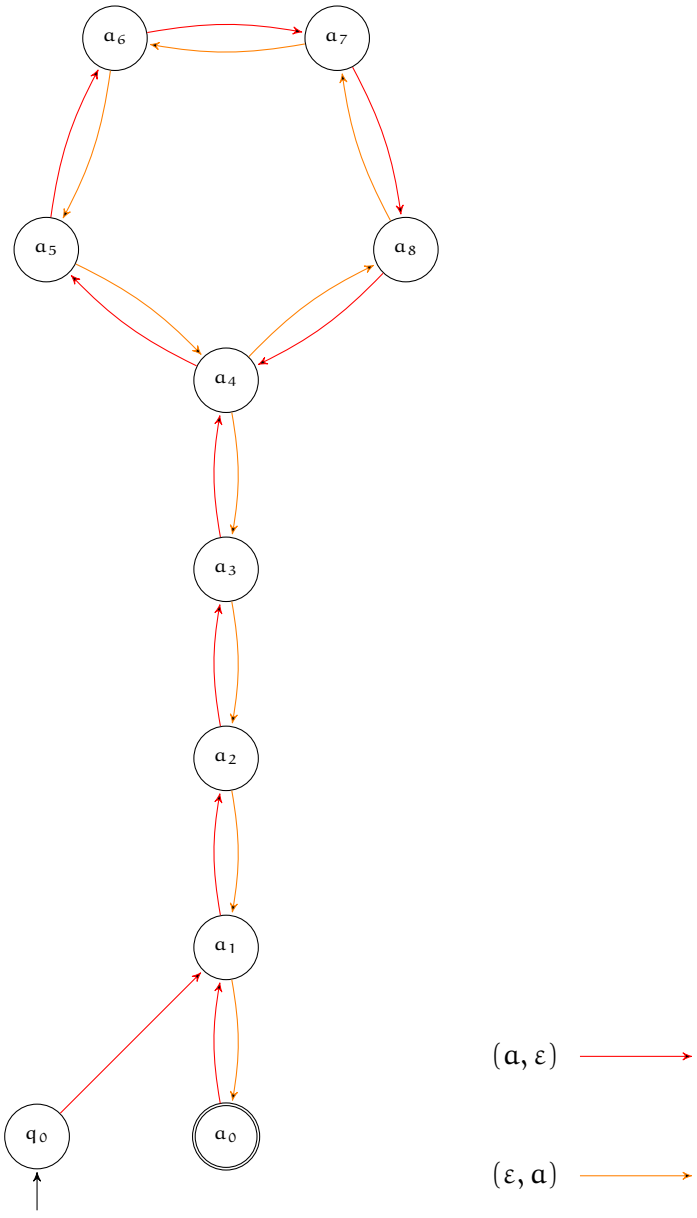



Figure 8.1: Automaton for $\iota_S(A)$ where $S = sg\langle a \mid a^4 = a^9 \rangle$

and $F = \{a_0, b_0\}$ and transitions given by the following table

| | $(a, \varepsilon)$ | $(\varepsilon, a)$ | $(b, \varepsilon)$ | $(\varepsilon, b)$ | |
|---|---|---|---|---|---|
| $q_0$ | $a_1$ | | $a_0^l, b_1$ | | |
| $b_0$ | | | $b_1$ | | |
| $b_1$ | | | | $b_0$ | |
| $a_0$ | $a_1$ | | $a_0^l, b_1$ | | |
| $a_j$ | $a_{j+1}$ | $a_{j-1}$ | $a_j^l$ | $a_j^r$ | for $i < j < i + k$ |
| $a_i$ | $a_{i+1}$ | $a_{i-1}$, $a_{i+k-1}$ | $a_i^l$ | $a_i^r$ | |
| $a_j^l$ | $a_{j+1}$ | | $a_j^l$ | | |
| $a_j^r$ | | $a_{j-1}$ | | $a_j^r$ | |
| $a_{i+k-1}$ | $a_i$ | $a_{i+k-2}$ | $a_{i+k-1}^l$ | $a_{i+k-1}^r$ | |

To show that the automaton decides $\iota_{E(i,k)}(A)$, we have to show that for any computation $q_0 \xrightarrow{(v,w)} a_0$ or $q_0 \xrightarrow{(v,w)} b_0$ it holds that $v\pi_A = w\pi_A$ and that if given a pair $(v, w)$ of strings with $v\pi_A = w\pi_A$ then there exists an accepting computation labelled by $(v, w)$.

Firstly, the given automaton decides the word problem of the subsemigroup

$$S = sg\left\langle a \mid a^i = a^{i+k} \right\rangle$$

of $E(i, k)$. For all computations $q_0 \xrightarrow{(a^\alpha, a^\beta)} a_m$ it holds that $|\alpha - \beta| = m + lk$ for $m \in \{0, \ldots, i + k - 1\}$ and some $l \in \mathbb{N}$. Conversely, it holds that for any pair $(a^\alpha, a^\beta)$ there is a computation $q_0 \xrightarrow{(a^\alpha, a^\beta)} a_m$ if $|\alpha - \beta| = m + lk$. Since $a^\alpha\pi_A = a^\beta\pi_A$ if and only if $|\alpha - \beta| = 0 + lk$ for some $l \in \mathbb{N}_{>0}$ the claim follows.

Now, for any computation $q_0 \xrightarrow{(v,w)} a_m$ it holds that $||v|_a - |w|_a| = m + kl$ for some $l \in \mathbb{N}$, and if $(va, wa)$ is a pair of strings over the generating set with $(va)\,\pi_A = (wa)\,\pi_A$, then there is a computation $q_0 \xrightarrow{(va,wa)} a_0$. It is immediate that there are computations $q_0 \xrightarrow{(b^\alpha, b^\beta)} b_0$ and computations $a_0 \xrightarrow{(b^\alpha, b^\beta)} b_0$

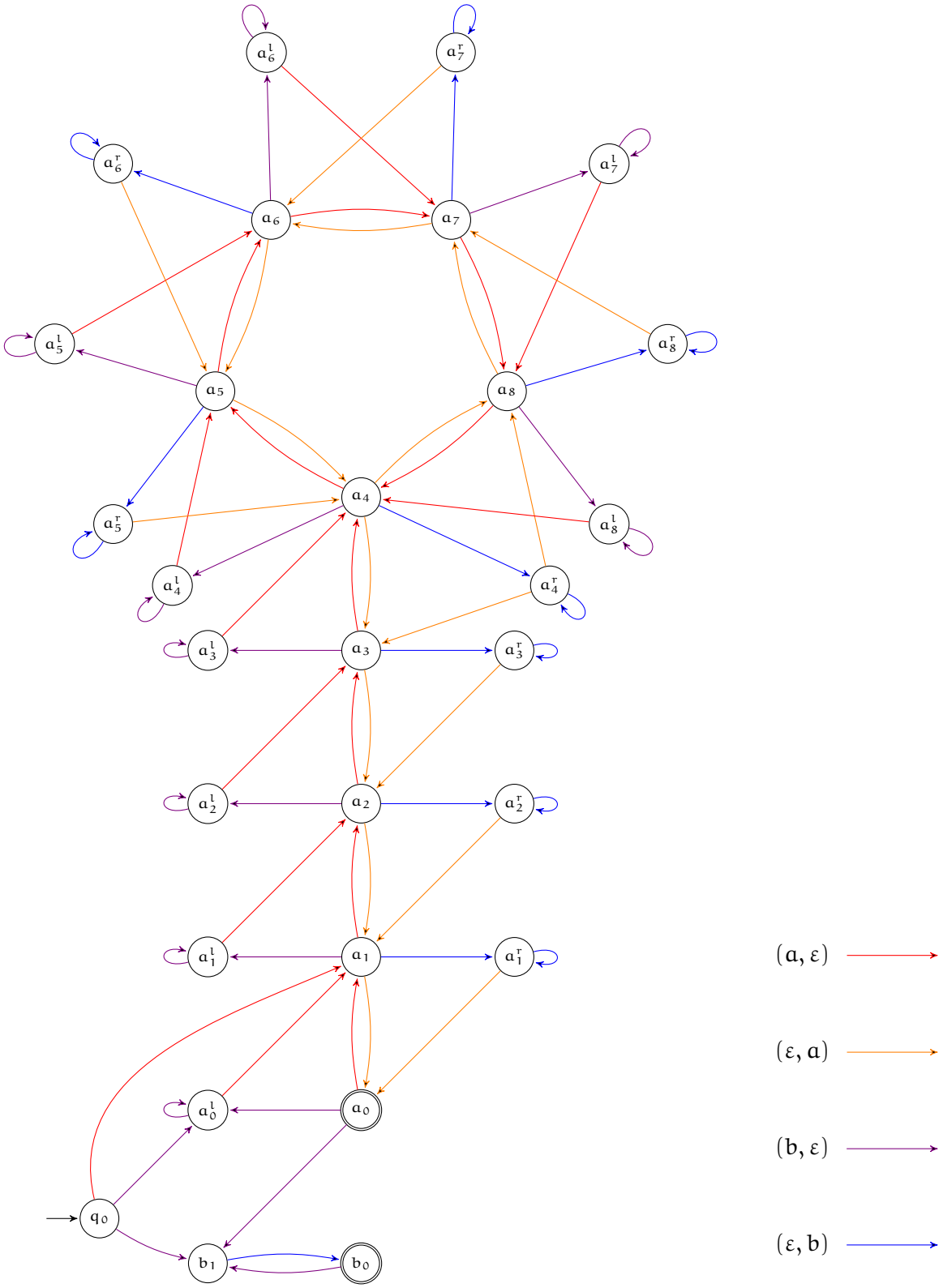



Figure 8.2: Automaton for $\iota_{E(4,5)}(\{a, b\})$

if and only if $\alpha = \beta$. Therefore it holds that any accepting computation labelled by a pair $(v, w)$ has $v\pi_A = w\pi_A$ by results from Section 5.5 and if $(v, w)$ is a pair with $v\pi_A = w\pi_A$ then there is an accepting computation.

Next we show that the automaton depicted in Figure 8.3 decides $\iota_P(\{a, b\})$. Recall that P was specified by the presentation

$$P = sg\left\langle a, b \mid (ab^n a = aba)_{n\geq 2} \right\rangle.$$

It follows that semigroups with rational word problem are not finitely presented in general.

Again, we show that the automaton shown in Figure 8.3 accepts a pair $(v, w)$ if and only if $v\pi_A = w\pi_A$. For this we take the viewpoint introduced in Section 5.6, namely consider

$$v = \prod_{i\in\underline{k}} [\mathbf{a}]^{\alpha_i} [\mathbf{b}]^{\beta_i}, \qquad w = \prod_{i\in\underline{k'}} [\mathbf{a}]^{\alpha'_i} [\mathbf{b}]^{\beta'_i},$$

for parameters as defined in Section 5.6.

A pair of this form is accepted by the automaton. After reading the pair $\left([\mathbf{a}]^{\alpha_1} [\mathbf{b}]^{\beta_1}, [\mathbf{a}]^{\alpha'_1} [\mathbf{b}]^{\beta'_1}\right)$ the automaton reaches one of $q_4$, $q_2$, or $q_3$. The next factor is started by reading $(a, a)$ and reaching $q_1$. From there the automaton can read each of the $k-1$ factors and accepts by reaching $q_1$ or $q_2$.

Assume now that the pair $(v, w)$ labels an accepting computation. We define factors of $(v, w)$ based on when a transition of the form $q \xrightarrow{(a,a)} q_1$ occurs. It now follows that $v$ and $w$ are of the form above and therefore $v\pi_A = w\pi_A$.

For the semigroups $CS(k)$ the relation $\iota_{CS(k)}(A)$ are not rational if $k > 1$. We will show this by applying the iteration lemma for rational relations. In Chapter 9 we will consider $CS(k)$ for $k > 1$ and show that $\iota_{CS(k)}(A)$ is polyrational.

**Theorem 8.2.2**

*Let* $CS(k)$ *be a free commutative semigroup of rank* $k > 1$*, generated by* $A = \{a_1, \ldots, a_k\}$*. Then* $\iota_{CS(k)}(A)$ *is not rational.*

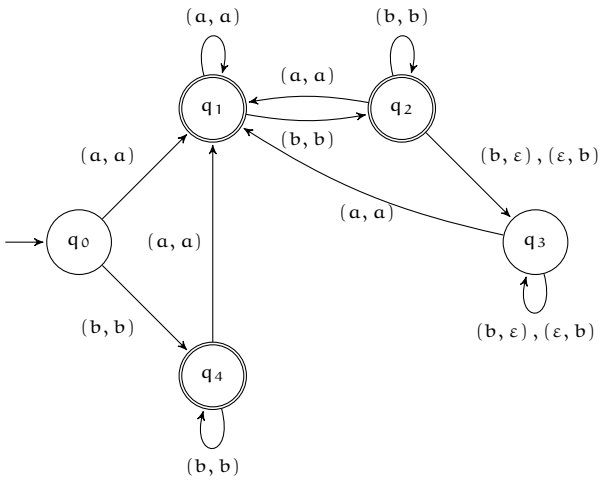



Figure 8.3: Automaton that decides $\iota_P(\{a, b\})$

*Proof.* We apply Proposition 3.7.6. Let for some $k > 1$ the semigroup $CS(k)$ be generated by $A = \{a_1, \ldots, a_k\}$.

The equation $v\pi_A = w\pi_A$ holds if and only if $|v|_a = |w|_a$ for all $a \in A$, therefore $w \in v\iota_{CS(k)}(A)$ if and only if $|v|_a = |w|_a$ for all $a \in A$.

Assume for a contradiction that $\iota_{CS(k)}(A)$ is rational. The iteration lemma 3.7.6 implies the existence of $n_0 \in \mathbb{N}$ such that for any pair $(v, w) \in \iota_{CS(k)}(A)$ with $|v| + |w| \geq n_0$ the strings $v$ and $w$ can be factorised into $v = x_1u_1z_1$ and $w = x_2u_2z_2$ such that $0 < |u_1| + |u_2| \leq n_0$ and $\left(x_1u_1^iz_1, x_2u_2^iz_2\right) \in \iota_{CS(k)}(A)$ for all $i \in \mathbb{N}$.

Let $n > n_0$ and consider the strings

$$v = [\mathbf{a_1^n a_2^n}], \qquad w = [\mathbf{a_2^n a_1^n}].$$

Then $w \in v\iota_{CS(k)}(A)$ and by the iteration lemma, as stated above, there are $m_1$ and $m_2$ in $\mathbb{N}$ where $0 \leq m_1, m_2 \leq n$ and $m_1 + m_2 > 0$ such that

$$v = \left[\mathbf{a_1^{n-m_1} a_1^{m_1} a_2^n}\right], \qquad w = \left[\mathbf{a_2^{n-m_2} a_2^{m_2} a_1^n}\right]$$

and the pairs

$$\left(\left[\mathbf{a_1^{n-m_1} a_1^{im_1} a_2^n}\right], \left[\mathbf{a_2^{n-m_2} a_2^{im_2} a_1^n}\right]\right)$$

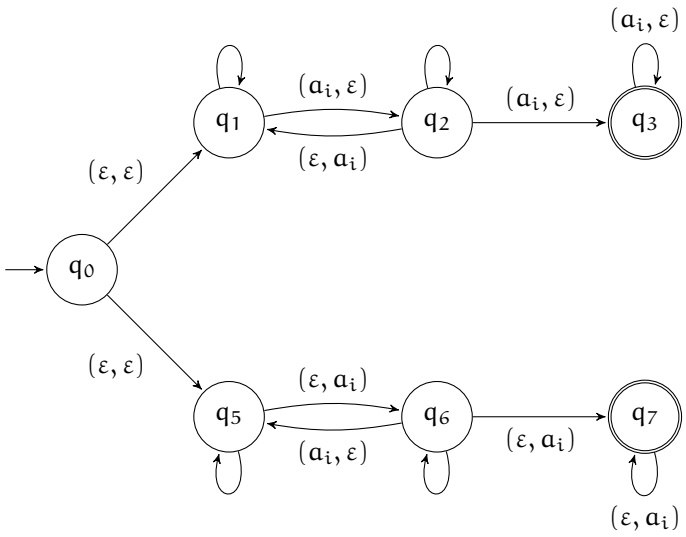



Figure 8.4: Automaton $\mathcal{A}_i$.

are elements of $\iota_{CS(k)}(A)$ for all $i \in \mathbb{N}$, which is a contradiction since for instance $[\mathbf{a_1^{n-m_1}a_2^n}]\,\pi_A \neq [\mathbf{a_2^{n-m_2}a_1^n}]\,\pi_A$, because $m_1 + m_2 > 0$. □

To not ignore the coword problem entirely we show the following result, which will become particularly interesting in Chapter 10.

**Theorem 8.2.3**

*Let $k$ be in $\mathbb{N}_{>0}$ and let $A = \{a_1, \ldots, a_k\}$. Then the coword problem $\bar{\iota}_{CS(k)}(A)$ is rational.*

*Proof.* Let $k$ be in $\mathbb{N}_{>0}$. We note that $w \in v\bar{\iota}_{CS(k)}(A)$ if and only if there exists an $a_i \in A$ such that $|v|_{a_i} \neq |w|_{a_i}$. The automaton $\mathcal{A}_i$ depicted in Figure 8.4, where all loops have additional labels $(a_j, \varepsilon)$ and $(\varepsilon, a_j)$ for $i \neq j$, accepts a pair $(v, w)$ of strings if and only if $|v|_{a_i} \neq |w|_{a_i}$ for a fixed $a_i \in A$. Denote the rational relation computed by $\mathcal{A}_i$ by $\rho_i$, then

$$\bar{\iota}_{CS(k)}(A) = \bigcup_{i \in \underline{k}} \rho_i,$$

and is therefore rational as a finite union of rational relations. □

In a very similar fashion as in the proof of Theorem 8.2.2 we can prove that the bicyclic monoid does not have rational word problem. We will give an alternative proof of this fact using Corollary 8.4.6 in Corollary 9.5.3.

**Theorem 8.2.4**

*The word problem of the bicyclic monoid* B *is not rational.*

*Proof.* We apply Proposition 3.7.6 once more.

Assume for a contradiction that $\iota_B(\{b, c\})$ is rational. Then there exists $n_0 \in \mathbb{N}$ such that for any pair $(v, w) \in \iota_B(\{b, c\})$ with $|v| + |w| \geq n_0$ the strings $v$ and $w$ can be factorised into $v = x_1u_1z_1$ and $w = x_2u_2z_2$ such that

$$0 < |u_1| + |u_2| \leq n_0,$$

and

$$\left(x_1u_1^iz_1, x_2u_2^iz_2\right) \in \iota_B(\{b, c\}) \text{ for all } i \in \mathbb{N}.$$

Let $n > n_0$ and consider $v = [\mathbf{b^n c^n}]$ and $w = \varepsilon$. Now by Proposition 3.7.6 as stated above there is $m \in \mathbb{N}$ with $m > 0$ such that $\left(\left[\mathbf{b^{n-m}b^{mi}c^n}\right], \varepsilon\right)$ is in $\iota_B(\{b, c\})$. This is a contradiction since for example

$$\left[\mathbf{b^{n-m}c^n}\right]\pi_A = [\mathbf{c^m}]\,\pi_A \neq \varepsilon\pi_A.$$

Therefore $\iota_B(\{b, c\})$ is not rational. □

## 8.3 Elements

It is a straightforward corollary of Proposition 3.7.7 that for a semigroup with rational word problem finitely generated by a set A we can find a recognisable subset D of $A^+$ such that D contains only finitely many representatives for each element of S.

**Theorem 8.3.1**

*Let S be a semigroup finitely generated by* A*. If* $\iota_S(A)$ *is rational, then there exists a recognisable subset* $D \subset A^+$ *such that* $(v\rho) \cap D$ *is finite for any* $v \in A^+$*.*

*Proof.* Since $\iota_S(A)$ is a congruence on $A^+$, it is in particular an equivalence relation on $A^+$, and therefore we can apply Proposition 3.7.7 to get the result.□

The above theorem only yields that D contains finitely many representatives for each element of S. It does not put a global bound on how many representatives there are in D for each element. In particular there are rational equivalence relations $A^+ \xrightarrow{\sigma} A^+$ and choices for D compatible with the statement of Proposition 3.7.7 such that there is no bound $n \in \mathbb{N}$ such that for all $v \in A^+$ it holds that $|(v\sigma \cap D)| < n$. As an example consider a finite alphabet A with more than one element and the equivalence relation $v \sim w$ if and only if $|v| = |w|$. A choice for D which is compatible with Proposition 3.7.7 is $A^+$.

The above is related to the following open question and with Open Question 3.7.1.

**Open Question 8.3.1**

*Given a semigroup S finitely generated by A such that $\iota_S(A)$ is a rational relation. Does there exist a recognisable subset $D \subset A^+$ such that for every $v \in A^+$ it holds that $|(v\iota_S(A)) \cap D| = 1$, in other words D is a recognisable set of unique representatives.*

Strictly speaking, the following theorem is a special case of Theorem 8.5.4, but since adding a zero or an identity is a very common construction in semigroups, we show that for any semigroup S the semigroups $S^z$ and $S^e$ have rational word problem if and only if S has rational word problem.

**Theorem 8.3.2**

*Let S be a finitely generated semigroup. Then the following statements are equivalent.*

1. *S has rational word problem.*
2. *$S^z$ has rational word problem.*
3. *$S^e$ has rational word problem.*

*Proof.* Let $S$ be a semigroup finitely generated by $A$ and such that $\iota_S(A)$ is rational.

The semigroup $S^z$ is generated by $B = A \cup \{z\}$. For two strings $v$ and $w$ in $B^+$ the equality $v\pi_B = w\pi_B$ holds if and only if either $v$ and $w$ are elements of $A^+$ and $v\pi_A = w\pi_A$ or both are elements of $B^*zB^*$ and hence $v\pi_B = w\pi_B = \mathbf{z}$, therefore

$$\iota_{S^z}(B) = \iota_S(A) \cup \mu_{B^*zB^*},$$

where $\mu_{B^*zB^*}$ is the universal relation on $B^*zB^*$. The above relation is rational as a union of a rational relation and a recognisable relation.

Conversely if $S^z$ has rational word problem we just remove $z$ from the generating set and apply Lemma 8.1.1.

The semigroup $S^e$ can be generated by $B = A \cup \{e\}$. Let

$$\iota : B \longrightarrow A^*, x \mapsto \begin{cases} \varepsilon, & x = e \\ x, & x \in A \end{cases}$$

then $B^* \xrightarrow{\iota} A^*$ is a rational relation and so is $\iota^r$, and the composition

$$B^* \xrightarrow{\iota} A^* \xrightarrow{\iota_S(A)} A^* \xrightarrow{\iota^r} B^*$$

is rational as well.

For two strings $v$ and $w$ in $B^+$ the equality $v\pi_B = w\pi_B$ holds if and only if either $v$ and $w$ are both in $\{e\}^+$ or $w \in v\rho$, in other words $v\iota\pi_A = w\iota\pi_A$ and therefore

$$\iota_{S^e}(B) = \rho \cup \mu_{e^+},$$

which is rational as a union of a rational relation and a recognisable relation.

Conversely if $S^e$ has rational word problem we remove $e$ from the generating set and apply Lemma 8.1.1. □

The following theorems treat the subsemigroups of a semigroup that are generated by single elements. For any element $s$ of a semigroup $S$ the set $s^+$ is either finite, and there are $i \in \mathbb{N}_{>0}$ and $k \in \mathbb{N}_{>0}$ with $s^{i+k} = s^i$, or $s^+$ is infinite.

We conjecture that for a given semigroup $S$ with rational word problem there is a constant $n_0 \in \mathbb{N}_{>0}$ such that for all $s \in S$ it holds that if $s^+$ is finite, then $|s^+| < n_0$.

**Open Question 8.3.2**

*Let $S$ be a semigroup with rational word problem. Prove that there is a constant $n_0 \in \mathbb{N}_{>0}$ such that for any $s \in S$ with $s^+$ finite it follows that $|s^+| < n_0$.*

We prove the partial result that there is $n_0 \in \mathbb{N}_{>0}$ such that if $s^{i+k} = s^i$ for $i$ and $k$ minimal, then $k \leq n_0$.

**Theorem 8.3.3**

*Let $S$ be a semigroup with rational word problem. There exists $n_0 \in \mathbb{N}_{>0}$ such that for any $s \in S$ with $s^{i+k} = s^i$, where $i \in \mathbb{N}$ and $k \in \mathbb{N}$ are minimal, the period $k$ is bounded above by $n_0$.*

*Proof.* Let $S$ be a semigroup with rational word problem finitely generated by $A$ and let $s \in S$ such that there are $i \in \mathbb{N}_{>0}$ and $k \in \mathbb{N}_{>0}$ with $s^{i+k} = s^i$. Assume $i$ and $k$ to be minimal, and choose $w \in A^+$ with $w\pi_A = s$. An automaton deciding $\iota_S(A)$ accepts $\left(w^i, w^m\right)$ if and only if $m = i + kl$ with $l \in \mathbb{N}$. Let $n_0$ be the number of states of such an automaton. For a contradiction suppose that $k > n_0$. For some $l_0 \in \mathbb{N}_{>0}$ we have $i + kl_0 > (i|w| + 1)(n_0 + 1)$. This means while reading the input $\left(w^i, w^{i+kl_0}\right)$, the automaton reads a substring of $w^{i+kl_0}$ of length greater than $|w|(n_0 + 1)$ while not reading anything from $w^i$. This means that the automaton reads $(\varepsilon, w^p)$ for some $0 < p \leq n_0 < k$, because starting from some state $q$ it reads some remainder $w'$ of $w$ and reaches a state $q'$. Reading $w$, it reaches states $q_i$, and enters a computation starting in $q_i$ and ending in $q_i$ labelled by $(\varepsilon, w^p)$, where $0 < p \leq n_0 < k$. Therefore it also accepts $\left(w^i, w^{i+kl_0-p}\right)$. Since $0 < p \leq n_0 < k$ the automaton accepts $\left(w^i, w^m\right)$ with $m = i + kl_0 - p$ and $p$ is not a multiple of $k$. This is a contradiction. □

An infinite semigroup with rational word problem contains an element of infinite order.

**Theorem 8.3.4**

*Let $S$ be a finitely generated infinite semigroup with rational word problem. Then there exists $s \in S$ such that the subsemigroup generated by $s$ is infinite.*

*Proof.* Proposition 3.7.7 ensures existence of a recognisable set $D \subset A^+$ such that for all $s \in S$ the intersection $s\pi^{-1} \cap D$ is finite and non-empty. Since $D$ is recognisable there exists an $n_0 \in \mathbb{N}$ such that we can factor any string of length greater than $n_0$ according to Theorem 3.2.4. Since $S$ is by assumption infinite, $D$ must be infinite, so there exists an element $v \in D$ of length greater than $n_0$ with a factorisation $v = xuy$ and $xu^iy \in D$ for all $i \in \mathbb{N}$, therefore $u\pi_A$ must have infinite order. □

Applying Theorems 8.2.2 and 8.5.1 yields that if a semigroup contains a subsemigroup isomorphic to a free commutative semigroup of rank bigger than one, then the semigroup does not have rational word problem. This also provides a tool to show that a semigroup does not have rational word problem.

**Theorem 8.3.5**

*Let $S$ be a finitely generated semigroup such that $S$ has a subsemigroup $T$ which is isomorphic to a free commutative semigroup of rank $k$ with $k \geq 2$. Then $S$ does not have rational word problem.*

*Proof.* Assume that $S$ is generated by $A$ and let $T$ generated by $B$ be a subsemigroup of $S$ isomorphic to $CS(k)$ for some $k \geq 2$. If $\iota_S(A)$ was rational then by Theorem 8.5.1 the set $\iota_T(B)$ would be rational in contradiction with Theorem 8.2.2. □

## 8.4 Rational Subsets and Kleene's Theorem

We show that if a semigroup $S$ has rational word problem, then the set of all representatives for a rational subset of $S$ is rational. We also show that the *pre*image of a rational subset of a semigroup with rational word problem is a rational subset of $A^+$ where $A$ is a finite generating set for $S$. It follows that semigroups with rational word problem are residually finite and Kleene semigroups.

We also note that the property that preimages of rational subsets are rational is a finiteness condition. It is a stricter finiteness condition than residual finiteness in that it demands rational subsets be separable from their complement by a finite semigroup quotient of $S$. Residual finiteness only demands elements to be separable by a finite quotient of $S$.

We have the condition that for any subset $X$ of $S$ which is rational, a finite quotient of $S$ can distinguish between $X$ and $S\backslash X$.

**Theorem 8.4.1**
*Let $S$ be a finitely generated semigroup with rational word problem. Then for any $X \in \operatorname{Rat} S$ the set $X\pi_A^{-1}$ is an element of $\operatorname{Rat} A^+$.*

*Proof.* Let $S$ be finitely generated by $A$, the relation $\iota_S(A)$ be rational, and let $A^+ \xrightarrow{\pi} S$ be the canonical morphism. We proceed by induction.

- Let $s \subset S$. For any choice of $v \in A^+$ with $v\pi_A = s$

$$s\pi_A^{-1} = v\iota_S(A)\,.$$

  and by Theorem 3.7.3 this set is a rational subset of $A^+$, because $\iota_S(A)$ is rational.

- Let $X$ and $Y$ be subsets of $S$ such that $X\pi_A^{-1}$ and $Y\pi_A^{-1}$ are rational subsets of $A^+$. Then $\left(X\pi_A^{-1}\right) \cup \left(Y\pi_A^{-1}\right)$ is a rational subset of $A^+$ and $(X \cup Y)\,\pi_A^{-1} = X\pi_A^{-1} \cup Y\pi_A^{-1}$, therefore $(X \cup Y)\pi_A^{-1}$ is rational.

- Let $X$ and $Y$ be subsets of $S$ such that $X\pi_A^{-1}$ and $Y\pi_A^{-1}$ are rational subsets of $A^+$. Then $\left(X\pi_A^{-1}\right)\left(Y\pi_A^{-1}\right)$ is a rational subset of $A^+$ and

$$\begin{aligned} z \in (XY)\,\pi_A^{-1} &\Leftrightarrow z\pi_A = xy \text{ for } x \in X \text{ and } y \in Y \\ &\Leftrightarrow z\pi_A = (v\pi_A)\,(w\pi_A) \text{ for } v \in X\pi_A^{-1} \text{ and } w \in Y\pi_A^{-1} \\ &\Leftrightarrow vw \in z\iota_S(A) \text{ for } vw \in \left(X\pi_A^{-1}\right)\left(Y\pi_A^{-1}\right) \end{aligned}$$

  Therefore $(XY)\,\pi_A^{-1}$ is a rational subset of $A^+$ by Theorem 3.7.3, because it is the image of a rational subset of $A^+$ under a rational relation.

- Let $X$ be a subset of $S$ such that $X\pi_A^{-1}$ is rational. Then $\left(X\pi_A^{-1}\right)^+$ is a rational subset of $A^+$ and

$$\begin{aligned} z \in \left(X^+\right)\pi_A^{-1} &\Leftrightarrow z\pi_A = x_1x_2\cdots x_n \text{ for } x_i \in X \\ &\Leftrightarrow v \in z\iota_S(A) \text{ for } v \in \left(X\pi_A^{-1}\right)^+ \end{aligned}$$

  Therefore $(X^+)\,\pi_A^{-1}$ is a rational subset of $A^+$, because it is the image of a rational subset of $A^+$ under a rational relation.

Therefore by induction on the structure of a rational subset $X$ of $S$, its preimage $X\pi_A^{-1}$ is rational. □

The following lemma characterises the recognisable subsets of any finitely generated semigroup by rational subsets of the free semigroup over the generating set. This is a finiteness condition in the sense that certain subsets can be recognised by a finite quotient of $S$.

**Lemma 8.4.2**

*Let $S$ be a semigroup finitely generated by $A$. For $X \subset S$ it holds that*

$$X\pi_A^{-1} \in \operatorname{Rat} A^+ \textit{ if and only if } X \in \operatorname{Rec} S.$$

*Proof.* Let $X \subset S$ such that $X\pi_A^{-1} \in \operatorname{Rat} A^+$. Kleene's Theorem states that $X\pi_A^{-1} \in \operatorname{Rec} A^+$ and therefore there exists a morphism $A^+ \xrightarrow{\varphi_X} T_X$, where $T_X$ is the quotient of $A^+$ by the syntactic congruence of $X\pi_A^{-1}$ as defined in 3.1.1, and a subset $F_X \subset T_X$ such that $X\pi_A^{-1} = F_X\varphi_X^{-1}$. We show that $\ker \pi_A \subset \ker \varphi_X$.

$$\begin{aligned} w \in v \ker \pi_A &\Rightarrow v\pi_A = w\pi_A \\ &\Rightarrow (\forall x, y \in A^*)\ (xvy)\,\pi_A = (xwy)\,\pi_A \\ &\Rightarrow (\forall x, y \in A^*)\ (xvy)\,\pi_A\pi_A^{-1} = (xwy)\,\pi_A\pi_A^{-1} \\ &\Rightarrow (\forall x, y \in A^*)\ xvy \in X\pi_A^{-1} \Leftrightarrow xwy \in X\pi_A^{-1} \\ &\Rightarrow w \in v \ker \varphi_X \end{aligned}$$

As justification for the last step refer to the definition of the syntactic congruence in 3.1.1. Applying the second isomorphism theorem for semigroups, there is now a morphism $S \xrightarrow{\psi_X} T_X$ with the property that $v\pi\psi_X = v\varphi_X$ for any $v \in A^+$. The definition of $\varphi_X$ ensures that for any $v \in A^+$ the image $v\varphi_X$ is an element of $F_X$ if and only if $v\pi_A \in X$. This shows that $\psi_X$ recognises the subset $X$ of $S$.

Conversely let $X \in \operatorname{Rec} S$. Since recognisability is closed under preimages by Theorem 3.2.2, the set $X\pi^{-1}$ is a recognisable subset of $A^+$, and by Kleene's Theorem a rational subset of $A^+$. □

It follows that if the preimage of any rational subset of a semigroup $S$ is rational, then Kleene's theorem holds in $S$.

**Corollary 8.4.3**

*Let $S$ be a semigroup finitely generated by $A$ such that for every $X \in \operatorname{Rat} S$ the preimage $X\pi^{-1}$ is in $\operatorname{Rat} A^+$. Then $\operatorname{Rat} S = \operatorname{Rec} S$.*

*Proof.* This follows directly from Lemma 8.4.2 □

It follows from the preceding lemmas that Kleene's Theorem holds in semigroups with rational word problem, in other words rational subsets of semi-

groups with rational word problem are recognisable. This is not true anymore for the class of semigroups with polyrational word problem introduced in Chapter 9, in particular for $\mathrm{CS}(k)$.

**Theorem 8.4.4**

*Let S be a semigroup with rational word problem. Then* $\operatorname{Rat} S = \operatorname{Rec} S$.

*Proof.* Let $S$ be a semigroup finitely generated by $A$ with rational word problem. Applying Theorem 8.4.1 yields that preimages under $\pi_A$ of rational subsets of $S$ are rational. Applying Corollary 8.4.3 now yields the result. □

It is still an open problem to characterise the class of semigroups in which Kleene's Theorem holds. We have shown that all semigroups with rational word problem are Kleene semigroups, but we do not have a proof that the converse holds. This question is also interconnected with an open question which is asked in a later chapter, namely whether the class of semigroups with rational word problem is the same class as the class of semigroups that are rational in the sense of Sakarovitch: The authors of the paper [PS90] construct a semigroup that is not rational but in which Kleene's theorem holds.

**Open Question 8.4.1**

*Let S be a semigroup with* $\operatorname{Rat} S = \operatorname{Rec} S$. *Does this imply that S has rational word problem?*

A further application of the above results is the following, which is valid in more general classes of semigroups than just semigroups with rational word problem.

If a semigroup $S$ is finitely generated by $A$, and for all elements $s \in S$ the set $s\pi_A^{-1}$ is a rational subset of $A^+$, then $S$ is residually finite. We will extend this result in Chapter 9 to include semigroups with polyrational word problem in Theorem 9.5.2.

**Theorem 8.4.5**

*Let $S$ be a semigroup finitely generated by $A$. If for all $s \in S$ the preimage $s\pi^{-1}$ is a rational subset of $A^+$, then $S$ is residually finite.*

*Proof.* Let $s$ and $t$ be elements of $S$ with $s \neq t$. Since $s$ is a rational subset of $S$, and by assumption $s\pi^{-1}$ is in Rat $A^+$, we conclude, using Corollary 8.4.3 that the set $s$ is a recognisable subset of $S$. This means that there is a morphism $S \xrightarrow{\varphi_s} T$, where $T$ is finite, and $F \subset T$ such that $s = F\varphi_s^{-1}$. Since $t \neq s$, applying $\varphi_s$ to $t$ yields that $t\varphi_s \in T \backslash F$, and in particular $s\varphi_s \neq t\varphi_s$. Therefore $S$ is residually finite. □

We conclude that semigroups with rational word problem are residually finite.

**Corollary 8.4.6**

*Let $S$ be a semigroup with rational word problem. Then $S$ is residually finite.*

*Proof.* Let $S$ be a semigroup finitely generated by $A$ with rational word problem. Then, by applying Theorem 8.4.1, for any $s \in S$ the preimage $s\pi_A^{-1}$ is a recognisable language. Applying Theorem 8.4.5 now proves the claim. □

## 8.5 Subsemigroups

It is a consequence of the theorems in Section 8.1 that finitely generated subsemigroups of a semigroup with rational word problem have rational word problem.

**Theorem 8.5.1**

*Let $S$ be a semigroup with rational word problem. Then any finitely generated subsemigroup of $S$ has rational word problem.*

*Proof.* Let $S$ be a semigroup with rational word problem and let $A$ be a finite generating set for $S$. Let $T$ be a finitely generated subsemigroup of $S$ and let $B$ be a generating set for $T$. Then $A \cup B$ is a generating set for $S$ and by

Theorem 8.1.3 S has rational word problem with respect to this generating set. Applying Lemma 8.1.1 now proves our claim. □

The notion of index of a subsemigroup T of a semigroup S is used to measure the relative size of T in S. If T has finite index in S, then the structural differences between S and T should also be small. The most restrictive notion of index is the Rees index: The Rees index of a subsemigroup T of a semigroup S is defined to be $|S\backslash T|$.

We want to show that if T is a subsemigroup of S of finite Rees index, then T has rational word problem if and only if S has rational word problem. Theorems 2.4.2 and 8.5.1 imply that subsemigroups of finite Rees index of a semigroup with rational word problem have rational word problem themselves.

We will show that, if S is a semigroup, and T is a subsemigroup of S of finite Rees index with rational word problem, then S has rational word problem.

Let in the following S be a semigroup and $T \subset S$ a subsemigroup of S. Let T have finite Rees index in S, and let T have rational word problem. Let B be a generating set for T and let $C = S\backslash T$. Note that C is finite and that that $A = B \cup C$ therefore is a finite generating set for S.

The proof will proceed in three steps.

We first show that for $v \in A^+$ with $v\pi_A \in S\backslash T$ we can compute a $c \in C$ with $c\pi_A = v\pi_A$ using a rational relation.

We then use a theorem from [Cam+95] to get a finite generating set D for T and a rational relation that rewrites any $v \in A^+$ with $v\pi_A \in T$ to an element $w \in D^+$ with $v\pi_A = w\pi_D$.

In a final step we put together the first two steps in Theorem 8.5.4 to show that S has rational word problem.

We note that from an element $t \in T$ the only way to get an element $t' \in S\backslash T$ is by multiplying by an element of $S\backslash T$, because T is a subsemigroup of S. In

contrast, the product of two elements in $S\backslash T$ can be any element of $S$, and the same holds for product of an element of $T$ and an element of $S\backslash T$.

Denote by $U$ the set of strings $u \in A^+$ with $u = [\mathbf{ac}]$ or $u = [\mathbf{ca}]$ for $a \in A$ and $c \in C$, and with $u\pi_A \in T$. For $u \in U$ we choose $w_u \in B^+$ with $u\pi_A = w_u\pi_B$. We denote the set of all such $w_u$ by $W$. Note that $W$ is a finite set.

We denote by $\mathcal{P}_C$ the monoid of partial transformations on $C$, and we denote undefined values by $\perp$. Let for all $a$ in $A$

$$\varphi_a : C \longrightarrow C,\ c \mapsto \begin{cases} c', & \text{if } c'\pi_A = (ac)\,\pi_A \\ \perp, & \text{otherwise} \end{cases}.$$

and define $A^* \xrightarrow{\varphi} \mathcal{P}_C$ by

$$a\varphi = \varphi_a.$$

The following lemma is the first step: There is a rational relation that for $v \in A^+$ with $v\pi_A \in S\backslash T$ computes $c \in C$ with $c\pi_A = v\pi_A$.

**Lemma 8.5.2**

*There is a rational relation* $A^+ \xrightarrow{\sigma} A^+$ *such that for any* $v \in A^+$*, if* $v\pi_A \in S\backslash T$*, then* $c = v\sigma$ *with* $v\pi_A = c\pi_A$*.*

*Proof.* Define an automaton $\mathcal{H} = \langle Q, A, A, q_0, F, \Delta\rangle$ such that the following hold, if if $v \in A^+$ with $v\pi_A \in S\backslash T$, then there is an accepting computation labelled by $(v, c)$ with $c \in C$ such that $v\pi_A = c\pi_A$.

For this let $Q = \mathcal{P}_C \cup C \cup \{f\}$ with $q_0 = \iota_C$ and $F = \{f\}$ and the following transitions

| | |
|---|---|
| $(\alpha, a, \varepsilon, \alpha \circ (a\varphi))$ | for $a \in A$ and $\alpha \in \mathcal{P}_C$ |
| $(\alpha, a, \varepsilon, a\alpha)$ | for $a \in A$ with $a\alpha \in C$ |
| $(c, a, \varepsilon, c')$ | for $a \in A$ and $c' \in C$ with $c'\pi_A = (ca)\,\pi_A$ |
| $(c, a, \varepsilon, w_{[\mathbf{ca}]}\varphi)$ | for $a \in A$ and $w_{[\mathbf{ca}]} \in W$ |
| $(c, \varepsilon, c, f)$ | for $c \in C$ |

We show that for any $v \in A^+$ there is a computation $\gamma : q_0 \xrightarrow{(v,\varepsilon)} c$ if and only if $v\pi_A = c\pi_A$. For this we first note that any computation of the form

$$\alpha \xrightarrow{(w,\varepsilon)} \beta \xrightarrow{(x,\varepsilon)} c$$

where all states up to $\beta$ are elements of $\mathcal{P}_C$ have the property that there is $u \in B^*$ such that $(uwx)\,\pi_A = c\pi_A$. In particular if $\alpha = q_0$ then $u = \varepsilon$ and $(vx)\,\pi_A = c\pi_A$. Note that $c(a\varphi) = w_{ac}$ implies $w_{ac}\pi_A = (c\,(a\varphi))\,\pi_A$ and therefore $(c\,(a\varphi))\,\pi_A = (ac)\,\pi_A$ if $v\varphi$ is defined then $(vc)\pi_A = (c(v\varphi))\pi_A$.

Conversely let $vx \in B^*C$ with $(vx)\pi_A \in S\backslash T$. In this case $v\varphi$ is defined, because if $v = v_1 \dots v_n \in B^*$ and $(v_1 \dots v_n x)\pi_A \in S\backslash T$ then $(v_1 \dots v_i)\pi_A \in T$ and therefore $(v_{i+1} \dots v_n x)\pi_A \in S\backslash T$ for any $1 \leq i < n$. By the definition of $\mathcal{H}$ there exists a computation

$$q_0 \xrightarrow{(v,\varepsilon)} v\varphi \xrightarrow{(x,\varepsilon)} x(v\varphi)$$

and $(x(v\varphi))\pi_A = (vx)\pi_A$.

Now let $\gamma : q_0 \xrightarrow{(v,\varepsilon)} c$ with $c \in C$ be a computation. We show that $v\pi_A = c\pi_A$.

The computation $\gamma$ can be factorised into partial computations of the form

$$\alpha_i \xrightarrow{(v_i,\varepsilon)} \beta_i \xrightarrow{(x_i,\varepsilon)} c_i \xrightarrow{(w_i,\varepsilon)} d_i \xrightarrow{(y_i,\varepsilon)} \alpha_{i+1}$$

for $1 \leq i < k$ for some $k \in \mathbb{N}$ and

$$\alpha_k \xrightarrow{(v_k,\varepsilon)} \beta_k \xrightarrow{(x_k,\varepsilon)} c_k \xrightarrow{(w_k,\varepsilon)} c$$

where for all $1 \leq i \leq k$ the states $\alpha_i$ and $\beta_i$ and all states that are visited in between are elements of $\mathcal{P}_C$, and $c_i$ and $d_i$ and all states that are visited in between are elements of $C$. Furthermore $v_i \in B^+$, $w_i \in A^+$ and $x_i$ and $y_i$ are in $C$.

We observe that $\alpha_{i+1} = w_{d_i y_i}\varphi$ and therefore by induction on $k$ the equation $v\pi_A = c\pi_A$ holds.

We can factor a given string $v \in A^+$ with $v\pi_A \in S\backslash T$ into

$$v = u_1 \dots u_k$$

where $u_i = v_i x_i w_i y_i$ for $1 \leq i < k$ and $u_k = v_k x_k w_k$ and $v_i \in B^*$, $w_i \in A^+$ and $x_i, y_i \in C$ such that there are computations

$$\alpha_i \xrightarrow{(v_i,\varepsilon)} \beta_i \xrightarrow{(x_i,\varepsilon)} c_i \xrightarrow{(w_i,\varepsilon)} d_i \xrightarrow{(y_i,\varepsilon)} \alpha_{i+1}$$

and

$$\alpha_k \xrightarrow{(v_k,\varepsilon)} c_k \xrightarrow{(w_k,\varepsilon)} d_k$$

by construction of $\mathcal{H}$ and by induction on $k$ it follows that $d_k\pi_A = v\pi_A$.

In conclusion, if $v\pi_A \in S\backslash T$, then there is an accepting computation of $\mathcal{H}$ labelled by $(v, c)$. This concludes the proof. □

For the second step, we use a result from [Cam+95]. Consider the set

$$D = \{d_{x,a,z} \mid x, z \in C \cup \{\varepsilon\}, a \in A, \text{ and } (xa)\pi_A, (xaz)\pi_A \in T\}$$

Let $w \in A^+$ with $w\pi_A \in T$. The authors prove in [Cam+95] that $D$ is a finite generating set for $T$, see also Theorem 2.4.2. They also prove that the following partial function rewrites any string $w$ into $w' \in D^+$ with $w\pi_A = w'\pi_D$. Let $w = w'aw''$ such that $w'a$ is of minimal length with the property that $(w'a) \in T$. Let also $x \in C$ with $x\pi_A = w'\pi_A$, if $w' \in A^+$ and $x = \varepsilon$ if $w' = \varepsilon$, and $z \in C$ with $z\pi_A = w''\pi_A$.

$$w\tau = \begin{cases} d_{x,a,z}, & \text{if } w''\pi_A \in S\backslash T \\ d_{x,a,\varepsilon}(w''\tau), & \text{if } w''\pi_A \in T \end{cases}$$

We show that $\tau$ is a rational relation.

**Lemma 8.5.3**

*The partial function* $A^+ \xrightarrow{\tau} D^+$ *is a rational relation.*

*Proof.* Define a finite automaton $\mathcal{T}$ as follows. The state set of the automaton is

$$Q = \{q_0, f\} \cup C \cup (C \times A \times \mathcal{P}_C \times (C \cup \{\varepsilon\}))\,.$$

We define the following transitions for all $a, a' \in A$, $b \in B$, $c, c', c'' \in C$, and $\alpha \in \mathcal{P}_C$, subject to the additional conditions given in the second column.

| | |
|---|---|
| $(q_0, b, d_{\varepsilon,b,\varepsilon}, q_0)$ | |
| $(q_0, c, \varepsilon, c)$ | |
| $(c, a, \varepsilon, c')$ | $(ca)\,\pi_A = c'\pi_A$ |
| $(c, a, d_{c,a,\varepsilon}, q_0)$ | $(ca)\,\pi_A \in T$ |
| $(c, a, \varepsilon, (c, a, \iota_C, \varepsilon))$ | $(ca)\,\pi_A \in T$ |
| $((c, a, \alpha, \varepsilon), a', \varepsilon, (c, a, \alpha \circ (a'\varphi), \varepsilon))$ | |
| $((c, a, \alpha, \varepsilon), a', \varepsilon, (c, a, \perp, a'\alpha))$ | $a'\alpha \in C$ |
| $((c, a, \perp, c'), a', \varepsilon, (c, a, \perp, c''))$ | $c''\pi_A = (c'a)\,\pi_A$ |
| $((c, a, \perp, c'), a', \varepsilon, (c, a, \left(w_{[\mathbf{c'a}]}\right)\varphi, \varepsilon))$ | if $c'a\pi_A \in T$ |
| $((c, a, \perp, c'), \varepsilon, d_{c,a,c'}, f)$ | |

The initial state is $q_0$, accepting states are $q_0$ and $f$.

We show by induction that the graph of $\tau$ is computed by $\mathcal{T}$. For this we first consider computations $q_0 \xrightarrow{(w, d_{x,a,z})} q_0$. Let $w \in A^+$. Starting from $q_0$, the automaton computes the shortest prefix $w'a$ of $w$ such that $(w'a)\,\pi_A \in T$ and either outputs $d_{x,a,\varepsilon}$, and continues on the remainder of the input, or computes $z \in C$ and outputs $d_{x,a,z}$. This conforms exactly to the definition of $\tau$. □

The previous two lemmas are now used to prove the following result about subsemigroups of finite Rees index.

**Theorem 8.5.4**

*Let $S$ be a finitely generated semigroup and let $T$ be a subsemigroup of $S$ of finite Rees index. Then $S$ has rational word problem if and only if $T$ has rational word problem.*

*Proof.* Let S be a finitely generated semigroup and let T be a subsemigroup of S of finite Rees index.

If S has rational word problem, applying Theorem 2.4.2 yields that T is finitely generated and by Theorem 8.5.1 the subsemigroup T has rational word problem.

If T has rational word problem, then by Theorem 8.1.3 it follows that $\iota_T(D)$, for D as defined above, is rational. Also, the relation $A^+ \xrightarrow{\rho} A^+$

$$A^+ \xrightarrow{\tau} D^+ \xrightarrow{\iota_T(D)} D^+ \xrightarrow{\tau^r} A^+$$

is rational as a composition of rational relations.

From Lemma 8.5.2 we get a rational relation $A^+ \xrightarrow{\sigma} A^+$ with the properties described. The relation $A^+ \xrightarrow{\rho'} A^+$ defined by the composition

$$A^+ \xrightarrow{\sigma} A^+ \xrightarrow{\iota_C} A^+ \xrightarrow{\sigma^r} A^+$$

is also rational as a composition of rational relations. Now the relation $(\rho \cup \rho')$ is rational as a union of rational relations, and it is the word problem of S. □

The above theorem does by no means tell the whole story: If we let $S = \{a, b\}^+$ and the subsemigroup $T = \{a\}^+$, then S as well as T have rational word problem, and T has infinite Rees index in S. We conjecture that the above methods can suitably be extended to extensions where the action of T on S\T and of S\T on T are rational relations.

The following theorem shows how the situation is for some extensions of infinite Rees index. Green index is a generalisation of the notion of index proposed by Gray and Ruskuc in [GR08]. It is aimed at generalising Rees index and group index. If $T \leq S$ has finite Green index and rational word problem, then S does not necessarily have rational word problem. For consider

the monoid M introduced in Example 5.7.

$$\begin{aligned} M = \mathrm{mon}\Big\langle a, b, c, d \mid\ & ac = ca = c^2,\ ad^2 = d^2a = d \\ & bd = db = d^2,\ bc^2 = c^2b = c \\ & dc^2 = c,\ cd^2 = d,\ cd = dc \Big\rangle \end{aligned}$$

The submonoid N generated by $a$ and $b$ has finite Green index in M and N has rational word problem since it is the free monoid on $\{a, b\}$. The monoid M itself does not have rational word problem, as can be shown by applying Proposition 3.7.6 to the pair $([\mathbf{b}]^n [\mathbf{c}]^n, [\mathbf{bc}])$ for a sufficiently large $n$.

**Theorem 8.5.5**

*Let S be a finitely generated semigroup and let* T *be a subsemigroup of S of finite Green index. Then the following statements are equivalent*

1. *S has rational word problem,*
2. T *has rational word problem, and all* T*-relative Schützenberger groups are finite,*
3. T *has rational word problem, and* T *has finite Rees index in S.*

*Proof.* We first show that 1 implies 2. Assume S has rational word problem. Applying Theorem 8.7.7 yields that all $\mathcal{H}^S$-classes are finite. Since every $\mathcal{H}^S$ class is a union of $\mathcal{H}^T$ classes, it follows that all $\mathcal{H}^T$ classes are finite and therefore all T-relative Schützenberger groups are finite. It also follows that T has finite Rees index, since by assumption, if T has finite Green index, that means that there are finitely many $\mathcal{H}^T$-classes contained in $S \setminus T$, all of which are finite. Therefore T has rational word problem by Theorem 8.5.4.

For 2 implies 3, assume that T has rational word problem, and all T-relative Schützenberger groups are finite. By the assumption that T has finite Green index in S it follows that T has finite Rees index in S and again by Theorem 8.5.4 it also follows that T has rational word problem.

The final implication 3 implies 1 now follows by applying Theorem 8.5.4 S once more. □

To conclude this section we show that if M is a monoid with rational word problem, then $M \setminus \mathcal{U}(M)$ is an ideal in M. We will show in Theorem 8.7.7 and Corollary 8.7.8 that in fact the group of units has to be finite.

**Theorem 8.5.6**

*Let* M *be a finitely generated monoid with rational word problem. Then* $M \setminus \mathcal{U}(M)$ *is an ideal of* M.

*Proof.* Let M be finitely generated by A and assume that $M \setminus \mathcal{U}(M)$ is not an ideal of M. This means that there are $v$ and $w$ in $A^+$ such that $(vw)\,\pi_A = \mathbf{e}$ and $(wv)\,\pi_A \neq \mathbf{e}$. Applying Corollary 1.32 from [CP61, Ch.1, p. 45] now yields that $v\pi_A$ and $w\pi_A$ generate a submonoid of M that is isomorphic to the bicyclic monoid, which is a contradiction to the assumption that M has rational word problem. □

## 8.6 Products

This section is dedicated to showing how semigroups with rational word problem can arise as direct products, free products and zero unions.

First we will consider direct products and prove the following theorem.

**Theorem 8.6.1**

*Let* S *and* T *be finitely generated semigroups such that* $S \times T$ *is finitely generated. Then* $S \times T$ *has rational word problem if and only if* S *and* T *have rational word problem and at least one of* S *or* T *is finite.*

We establish when the direct product of two finitely generated semigroups is finitely generated. Assume that S and T are finitely generated semigroups. If S and T are monoids, then $S \times T$ is finitely generated. If for example $S = a^+$

and $T = b^+$, then $S \times T$ is not finitely generated. We state the following result from [RRW98].

**Proposition 8.6.2**

*Let $S$ and $T$ be finitely generated semigroups. Then $S \times T$ is finitely generated if and only if one of the following conditions holds.*

1. *$S$ and $T$ are both finite.*
2. *$S$ is finite and $S^2 = S$.*
3. *$T$ is finite and $T^2 = T$.*
4. *$S^2 = S$ and $T^2 = T$.*

The next step is to establish the properties of factors of direct products that have rational word problem. We first prove that if a direct product $S \times T$ is finitely generated and has rational word problem, then both factors have rational word problem. It is well-known t hat $S$ and $T$ are finitely generated if $S \times T$ is finitely generated.

**Theorem 8.6.3**

*Let $S$ and $T$ be semigroups. If $S \times T$ is finitely generated and has rational word problem then $S$ and $T$ are finitely generated and have rational word problem.*

*Proof.* Let $S \times T \xrightarrow{\pi_S} S$ be the projection onto $S$ and let $A$ be a finite generating set for $S \times T$. The set $A$ generates $S$ via the map $\pi_A \pi_S$.

Denote by $\rho$ the kernel of the map $\pi_A \pi_S$ restricted to $A$. The equivalence relation $A \xrightarrow{\rho} A$ extends to an equivalence relation on $A^+ \xrightarrow{\rho} A^+$. Consider the composition

$$A^+ \xrightarrow{\rho} A^+ \xrightarrow{\iota_{S\times T}(A)} A^+ \xrightarrow{\rho} A^+$$

which in the following we denote by $\tau$. We claim that $\tau = \iota_S(A)$.

Let $v$ and $w$ be elements of $A^+$. If $w \in v\tau$ then $w\pi_A\pi_S = v\pi_A\pi_S$hence $w \in v\iota_S(A)$.

Conversely, if $w \in v\iota_S(A)$, then $w\pi_A\pi_S = v\pi_A\pi_S$ which implies that there exist strings $w'$ and $v'$ in $A^+$ such that $w' \in w\rho$ and $v \in v'\rho$ and $w' \in v'\iota_{S\times T}(A)$, hence $w \in v\sigma$. This concludes the proof. □

For the "only if" direction of Theorem 8.6.1, we consider the three cases: Either S and T are finite, one of S or T is finite, or both S and T are infinite. In the case that S and T are finite, their direct product $S \times T$ is finite and therefore has recognisable word problem by Theorem 7.2.1. For the case that S is finite we prove the following lemma.

**Lemma 8.6.4**

*Let S be a finite semigroup and let T be a semigroup with rational word problem. If $S \times T$ is finitely generated then $S \times T$ has rational word problem.*

*Proof.* Let A be a finite generating set for $S \times T$. Since A generates S and T, the relation $A^+ \xrightarrow{\iota_S(A)} A^+$ is recognisable. By assumption the relation $A^+ \xrightarrow{\iota_T(A)} A^+$ is rational. Now

$$\iota_{S\times T}(A) = \iota_S(A) \cap \iota_T(A)\,,$$

and therefore $\iota_{S\times T}(A)$ is rational by Lemma 3.4.4. □

In the case of a direct product of two infinite semigroups with rational word problem, we get a subsemigroup which is isomorphic to the free commutative semigroup of rank two, and therefore the direct product of two infinite semigroups with rational word problem does not have rational word problem.

**Lemma 8.6.5**

*Let S and T be infinite semigroups with rational word problem. Then $S \times T$ contains a free commutative semigroup of rank two.*

*Proof.* Let S and T be infinite semigroups with rational word problem. By Theorem 8.3.4 there exist $s \in S$ and $t \in T$ such that the subsemigroups of S and T generated by s and t respectively are infinite. The elements $(s^2, t)$ and

$(s, t^2)$ commute and generate a free commutative semigroup of rank two in $S \times T$. □

We can now give the proof of Theorem 8.6.1.

**Theorem 8.6.6**

*Let $S$ and $T$ be semigroups such that $S \times T$ is finitely generated. Then $S \times T$ has rational word problem if and only if $S$ and $T$ have rational word problem and at least one of $S$ or $T$ is finite.*

*Proof.* Let $S$ and $T$ be semigroups such that $S \times T$ is finitely generated.

If $S \times T$ has rational word problem, then both $S$ and $T$ have rational word problem by Theorem 8.6.3. Assume both $S$ and $T$ to be infinite. Then $S \times T$ would not have rational word problem by Lemma 8.6.5.

Conversely, if both $S$ and $T$ are finite then $S \times T$ is finite and has rational word problem by Theorem 7.2.1. If $S$ is finite and $T$ is infinite and has rational word problem, or vice versa, then by Lemma 8.6.4 the semigroup $S \times T$ has rational word problem. □

The situation in the case of the semigroup free product is easier to describe. Note that we do not need the restriction on the groups of units of $S$ and $T$ in the case of the semigroup free product. This is because the semigroup free product of two groups is *not* a group.

**Theorem 8.6.7**

*Let $S$ and $T$ be finitely generated semigroups. Then the semigroup free product $S * T$ has rational word problem if and only if $S$ and $T$ have rational word problem.*

*Proof.* Let $S$ and $T$ be finitely generated semigroups.

If $S * T$ has rational word problem, then $S$ and $T$ are finitely generated subsemigroups of $S * T$ and therefore have rational word problem.

Conversely assume that $S$ is finitely generated by $A$ and $T$ is finitely generated by $B$. Then $C = A \cup B$ is a generating set for $S * T$. Assume that $\iota_S(A)$

and $\iota_T(B)$ are rational relations. Define the rational relation $C^+ \xrightarrow{\rho} C^+$ by

$$\rho = (\iota_S(A) \cup \iota_T(B))^+$$

The relation $C^+ \xrightarrow{\rho} C^+$ is rational and equal to $\iota_{S*T}(C)$. □

If we consider monoid free products of monoids with rational word problem we first observe that the monoid free product $C_2 * C_2$ where $C_2$ is a cyclic group of order two is an infinite group and so does not have rational word problem, as will be shown in Theorem 8.7.7 and Corollary 8.7.8. We get the following theorem that characterises monoid free products that have rational word problem.

**Theorem 8.6.8**

*Let* $M$ *and* $N$ *be finitely generated monoids. Then the monoid free product* $M * N$ *has rational word problem if and only if* $M$ *and* $N$ *have rational word problem and the group of units of* $M$ *or* $N$ *is trivial.*

*Proof.* Let $M$ be finitely generated as a monoid by $A$ and $N$ be generated as a monoid by $B$. Then $C = A \cup B$ generates $M * N$.

Assuming $\iota_{M*N}(C)$ is rational, $M$ and $N$ are finitely generated submonoids of $M * N$ and therefore have rational word problem.

If the groups $\mathcal{U}(M)$ and $\mathcal{U}(N)$ were both not trivial, then $\mathcal{U}(M) * \mathcal{U}(N)$ would be an infinite subgroup of $M * N$, in contradiction with the assumption that $M * N$ has rational word problem.

Let now without loss of generality $\mathcal{U}(M)$ be non-trivial and $\mathcal{U}(N)$ be trivial. Since $\mathcal{U}(M * N)$ is finite, the set $L = \mathbf{e}\,\pi_C^{-1}$ is a recognisable subset of $C^*$. The relation $C^* \xrightarrow{\rho} C^*$ which replaces any occurrence of an element of $L$ by $\varepsilon$ is a rational relation, since the relations $C^* \xrightarrow{\tau} C^*$ with $L\tau = \varepsilon$, and $C^* \xrightarrow{\sigma} C^*$ with $\nu\sigma = C^* \backslash C^* L C^*$ are recognisable and

$$\rho = (\iota_{C^*} \cup \tau)^* \cap \sigma.$$

Now, since

$$\mu = (\iota_M(A) \cup \iota_N(B))^*$$

is rational, we can write $\iota_{M*N}(C)$ as the composition

$$C^* \xrightarrow{\rho} C^* \xrightarrow{\mu} C^* \xrightarrow{\rho^r} C^*.$$

This concludes the proof. □

The last type of construction we consider in this section is the zero union of two semigroups as defined in Definition 2.10.5

**Theorem 8.6.9**

*Let* $U$ *be a semigroup that is a zero union of two finitely generated subsemigroups* $S$ *and* $T$. *Then* $U$ *has rational word problem if and only if* $S$ *and* $T$ *have rational word problem.*

*Proof.* Let $U$ be a zero union of $S$ and $T$ and let $C$ be a finite generating set for $U$ such that $C$ contains generating sets $A$ for $S$ and $B$ for $T$. If $U$ has rational word problem then $S$ and $T$ are finitely generated subsemigroups of $U$ and therefore have rational word problem by Theorem 8.5.1.

Conversely, assume that $\iota_S(A)$ and $\iota_T(B)$ are rational. We observe that the set

$$Z = \left\{ v \in C^+ \mid v\pi_C = \mathbf{z} \right\},$$

the set of representatives over $C$ of the zero element of $U$ is a recognisable subset of $C^+$ by Theorem 8.4.1. The equality

$$\iota_U(C) = \iota_S(A) \cup \iota_T(B) \cup (Z \times Z)$$

now shows that $\iota_U(C)$ is rational. □

## 8.7 Green's Relations

Green's relations were introduced as very important in the theory of semigroups in Chapter 2. For a finitely generated semigroup $S$ we have defined

the notion of rationality for relations $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, $\mathcal{D}$ and $\mathcal{J}$ with respect to a given generating set. This section will consider Green's relations of semigroups with rational word problem.

It does not seem to be of high value to consider semigroups with rational $\mathcal{R}$ and rational $\mathcal{L}$ alone, since any finitely generated group has rational Green's relations.

**Lemma 8.7.1**

*Let* $G$ *be a finitely generated group and* $A$ *be a finite monoid generating set for* $G$. *Then*

$$\mathcal{L}_G(A) = \mathcal{R}_G(A) = \mathcal{H}_G(A) = \mathcal{J}_G(A) = \mathcal{D}_G(A) = \mu_{A^*}$$

*and therefore all the relations are rational.*

*Proof.* For a group G Green's relations are all equal to $G \times G$ and the claim follows immediately since $A$ is a generating set. □

The bicyclic monoid B has neither rational word problem, as shown in Section 8.2, nor rational $\mathcal{R}$ nor rational $\mathcal{L}$. To illustrate this, we remind ourselves that the elements of the bicyclic monoid have representatives of the form $[\mathbf{c}]^{\gamma}[\mathbf{b}]^{\beta}$. Two such elements $[\mathbf{c}]^{\gamma_1}[\mathbf{b}]^{\beta_1}$ and $[\mathbf{c}]^{\gamma_2}[\mathbf{b}]^{\beta_2}$ are $\mathcal{R}$-related if and only if $\gamma_1 = \gamma_2$. Assume $\mathcal{R}(A)$ is rational. The element $[\mathbf{c}]\pi_B$ can be represented by the strings $[\mathbf{b}]^n[\mathbf{c}]^n c$ and $[\mathbf{c}]$ for any $n \in \mathbb{N}_{>0}$ and therefore $[\mathbf{b}]^n[\mathbf{c}]^n[\mathbf{c}] \in [\mathbf{c}]\mathcal{R}(A)$. By applying Proposition 3.7.6 we get $n_0 \in \mathbb{N}$ such that for $n > n_0$ there are $0 \leq k_1 < n_0$ and $0 \leq k_2 \leq 1$ such that $[\mathbf{b}]^{n-k_1}[\mathbf{b}]^{ik_1}[\mathbf{c}]^n[\mathbf{c}]$ and $[\mathbf{c}]^{1-k_2}[\mathbf{c}]^{ik_2}$ are $\mathcal{R}(A)$-related for all $i \in \mathbb{N}$. This shows that $\mathcal{R}$ is not rational for the bicyclic monoid.

We consider Green's relations on semigroups with rational word problem, and first get the following result. We remind ourselves that the definition of a k-rational relation as an intersection of at most k rational relations in Section 3.8.

**Lemma 8.7.2**

*Let S be a semigroup with rational word problem. Then the relations $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{J}$ are 2-rational. The relation $\mathcal{H}$ is 4-rational.*

*Proof.* Let S be a semigroup with rational word problem and let A be a generating set for S. We observe that the relation

$$\rho : A^+ \longrightarrow A^+,\ v \mapsto vA^*,$$

the relation

$$\lambda : A^+ \longrightarrow A^+,\ v \mapsto A^*v,$$

and the relation

$$\sigma : A^+ \longrightarrow A^+,\ v \mapsto A^*vA^*$$

are rational and therefore the relations $\rho\iota_S(A)$, $\lambda\iota_S(A)$ and $\sigma\iota_S(A)$ are rational by Theorem 3.7.4. The following equivalences hold for $\mathcal{R}$.

$$\begin{aligned} w \in v\mathcal{R}_S(A) &\Leftrightarrow w\pi_A \in v\pi_A\mathcal{R} \\ &\Leftrightarrow \exists x \in A^* \text{ such that } (vx)\pi_A = w\pi_A \text{ and} \\ &\quad\ \exists y \in A^* \text{ such that } (wy)\pi_A = v\pi_A \\ &\Leftrightarrow \exists x \in A^* \text{ such that } w \in (vx)\,\iota_S(A) \text{ and} \\ &\quad\ \exists y \in A^* \text{ such that } v \in (wy)\,\iota_S(A) \\ &\Leftrightarrow w \in v\rho\iota_S(A) \text{ and } v \in w\rho\iota_S(A)\,. \end{aligned}$$

This proves that $\mathcal{R}(A)$ is the intersection of the two rational relations $\rho\iota_S(A)$ and $\rho\iota_S(A)^r$. The proofs for $\mathcal{L}(A)$ and $\mathcal{J}(A)$ are very similar and therefore omitted. The claim about $\mathcal{H}(A)$ follows immediately from the results about $\mathcal{R}$ and $\mathcal{L}$ and the definition of $\mathcal{H}$. □

We observe that, if a semigroup with rational word problem has only singleton $\mathcal{R}$-classes, then $\mathcal{R}$ is rational and the same holds for $\mathcal{L}$. This is in particular true for the free semigroups on a finite generating set. If either $\mathcal{R}$ or $\mathcal{L}$ has only singleton classes then $\mathcal{H}$ classes are trivial and $\mathcal{H}$ is rational too.

It follows from Theorem 8.7.11 that $\mathcal{D}$ is 2-rational.

A slightly larger class we consider is the class of cancellative semigroups. We get that $\mathcal{R}$ and $\mathcal{L}$ are rational. It is currently an open question to characterise semigroups with rational word problem and rational $\mathcal{R}$ or $\mathcal{L}$. We will show in Theorem 8.7.7 that $\mathcal{H}-$classes have to be finite for semigroups with rational word problem in general.

**Theorem 8.7.3**

*Let S be a finitely generated, cancellative semigroup with rational word problem. Then $\mathcal{R}$ and $\mathcal{L}$ are rational.*

*Proof.* Let S be a cancellative semigroup finitely generated by A and assume $\iota_S(A)$ is rational. Without loss of generality we assume S to contain an identity element. If S would not contain an identity element we consider $S^{\mathbf{e}}$. If $w \in v\mathcal{R}_S(A)$, then there exist x and y in $A^*$ such that $vx \in w\iota_S(A)$ and $wy \in v\iota_S(S)$, or equivalently, since S is cancellative, there are x and y in $A^*$ such that $x\pi_A \in \mathcal{U}(S)$ and $y\pi_A \in \mathcal{U}(S)$ and $(xy)\,\pi_A = \mathbf{e}_S$ and $(vxy)\,\pi_A = (wy)\,\pi_A$.

For any pair $x \in A^*$ and $y \in A^*$ the relations

$$\rho_{xy} : A^* \longrightarrow A^*,\ v \mapsto vxy$$

and

$$\rho_y : A^* \longrightarrow A^*,\ w \mapsto wy$$

are rational. Define the relation $\gamma_{x,y}$ by the composition

$$A^* \xrightarrow{\rho_{xy}} A^* \xrightarrow{\iota_S(A)} A^* \xrightarrow{\rho_y^r} A^*.$$

Choosing a set $R \subset A^* \times A^*$ such that for all pairs $(g,h) \in \mathcal{U}(S)$ with $gh = \mathbf{e}_s$ there is at least one pair $(v,w) \in R$ with $v\pi_A = g$ and $w\pi_A = h$, we conclude that

$$\mathcal{R}_S(A) = \bigcup_{(x,y)\in R} \gamma_{x,y}.$$

Since $\mathcal{U}(S)$ is finite, $R$ can be chosen to be finite. All $\gamma_{x,y}$ are rational, because $\iota_S(A)$ is assumed to be rational. We therefore conclude that $\mathcal{R}_S(A)$ is rational as a finite union of rational relations. The same result holds for $\mathcal{L}$ by an analogous proof. □

We record the following open questions for later reference.

**Open Question 8.7.1**

*Give a characterisation of all semigroups with rational word problem.*

**Open Question 8.7.2**

*Give a characterisation of all semigroups with rational $\mathcal{R}$ or rational $\mathcal{L}$, in particular prove that any semigroup with rational word problem has rational $\mathcal{R}$ and rational $\mathcal{L}$ or find an example of a semigroup with rational word problem where $\mathcal{R}$ or $\mathcal{L}$ is strictly 2-rational.*

We now further examine $\mathcal{R}$ for semigroups with rational word problem. All of the results hold for $\mathcal{L}$, for example by transferring to the opposite semigroup. The following result is mainly a technical helper. It describes the structure of infinite $\mathcal{R}$-classes.

**Lemma 8.7.4**

*Let $S$ be a semigroup with rational word problem and let $R$ be a $\mathcal{R}$-class of $S$. Then for all $s \in R$ there exists a finite set $X_s \subset S^e$ such that for all $y \in R$ there is $t \in X_s$ and $x \in S^e$ such that*

$$s = yt = sxt.$$

*Proof.* Let $S$ be a semigroup with rational word problem and let $A$ be a finite generating set for $S$.

If $R$ is a finite $\mathcal{R}$-class the claim follows immediately from the definition of $\mathcal{R}$.

Assume $R$ is an infinite $\mathcal{R}$-class and choose $v \in A^+$ such that $v\pi_A \in R$. By the definition of $\mathcal{R}$, for all $w \in A^+$ such that $w\pi_A \in R$, there exists $x \in A^*$

such that $v\pi_A = (wx)\pi_A$. We show that there is a finite set $Y_v \subset A^+$ such that for all $w \in A^+$ with $w\pi_A \in R$ there is a $u \in Y_v$ such that $v\pi_A = (wu)\pi_A$. From this the claim follows.

Assume that $\mathcal{A}$ is an automaton with $n_0$ states that decides $\iota_S(A)$. For $v$ and $w$ as above, there exists $x \in A^*$ such that $\mathcal{A}$ accepts $(v, wx)$. For any computation of $\mathcal{A}$ that accepts $(v, wx)$ we can find the following factorisation

$$q_0 \xrightarrow{(v_1,w)} q \xrightarrow{(v_2,x)} q_f$$

where $v_1$ and $v_2$ are in $A^*$. Now the length of $x$ in the computation from $q$ to $q_f$ is bounded from above by $|v|\, n_0 + n_0$, since we can assume that there is a shortest computation from $q$ to $q_f$ which is labelled by $(v_2, x)$. Therefore the set $Y_v$ of all possible such computations has at most $|A|^{|v|n_0+n_0}$ elements.

Since $Y_v$ is finite, the set $X_s = Y_v\pi_A$ is finite, which proves the existence and finiteness of $X_s$.

By assumption $v\pi_A = s$ and $w\pi_A = y$ where $y \in R$ arbitrary. By the above there is $t \in X_s$ such that $s = yt$ and by definition of $\mathcal{R}$ there is $x \in S^e$ with $y = sx$ and therefore the claim follows. □

The previous lemma allows us to prove that in a semigroup with rational word problem the intersection of a monogenic subsemigroup and any $\mathcal{R}-$class is finite.

**Theorem 8.7.5**

*Let $S$ be an infinite semigroup with rational word problem and let $R$ be an infinite $\mathcal{R}-$class of $S$. For any $s \in S$ such that the subsemigroup $s^+$ is infinite the intersection $s^+ \cap R$ is finite.*

*Proof.* Suppose $S$ is an infinite semigroup with rational word problem which has an infinite $\mathcal{R}$-class $R$. Let $s \in S$ such that $s^+$ is infinite. Choose $r \in R$. By Lemma 8.7.4 there exists a finite set $X_r$ such that for any $x \in R$ there is $t \in X_r$ such that $xt = r$. Assume for a contradiction that for infinitely many $k \in \mathbb{N}$ the power $s^k \in R$. Then there exist $i, j \in \mathbb{N}$ with $i < j$ and $t \in X_r$ such that

$s^i \in R$ and $s^j \in R$ and $r = s^i t = s^j t$. Since $R$ is an $\mathcal{R}$-class there is $x \in S$ such that $rx = s^i$. This yields $s^i tx = rx = s^i$, and by left multiplication by $s^{j-i}$ it follows that $s^{j-i}s^i = s^{j-i}s^i tx$. Therefore $s^j = s^j tx$ and also $s^j tx = rx = s^i$, hence $s^i = s^j$, which is a contradiction. □

We can now conclude, employing Theorem 8.3.4, that any infinite semigroup with rational word problem has infinitely many $\mathcal{R}-$classes.

**Theorem 8.7.6**

*Let $S$ be an infinite semigroup with rational word problem. Then $S$ has infinitely many $\mathcal{R}-$classes.*

*Proof.* By Theorem 8.3.4 there exists $s \in S$ such that $s^+$ is infinite. Every element of $s^+$ lies in exactly one $\mathcal{R}$-class of $S$, but only finitely many elements of $s^+$ lie in any given $\mathcal{R}$-class. Therefore $S$ has infinitely many $\mathcal{R}$-classes. □

Having covered some properties of $\mathcal{R}$- and $\mathcal{L}$- classes, we now move on to $\mathcal{H}$-classes. We first show that $\mathcal{H}$-classes of a semigroup with rational word problem have to be finite.

**Theorem 8.7.7**

*Let $S$ be a semigroup with rational word problem. Then all $\mathcal{H}$-classes of $S$ are finite.*

*Proof.* Let $S$ be a semigroup with rational word problem and let $A$ be a finite generating set for $S$. Let furthermore $n_0 \in \mathbb{N}$ be the number of states in some finite automaton that decides $\iota_S(A)$.

Assume for a contradiction that $S$ has an infinite $\mathcal{H}$ class $H$. Choose $h \in H$ and $v \in A^+$ with $v\pi_A = h$. Since we assumed $H$ to be infinite, $\mathcal{T}_S(H)$ is an infinite group by Theorem 2.9.3. Hence there exists $g \in \mathcal{T}_S(H)$ represented by $w \in A^+$ as an element of $S$ such that the shortest string $w' \in A^+$ with $(vww')\,\pi_A = h$ satisfies $|w'| > (|v| + 1)\,n_0 + |v|$, or in other words $ww'$ is a representative of the identity element of the group $\mathcal{T}_S(H)$.

Since $(vww')\,\pi_A = v\pi_A$ the finite automaton that decides $\iota_S(A)$ will accept the pair $(vww', v)$, and by the choice of length of $w'$ there is a factorisation of $w'$ into strings $x$,$u$ and $y$ in $A^*$ with $|u| > 0$ such that the automaton also accepts $\left(vwxu^i y, v\right)$ for all $i \in \mathbb{N}$. In particular, $(vwxy, v)$ is accepted and $(vwxy)\pi_A = v\pi_A$ contradicting the choice of $w'$ to be of minimal length.

Therefore any $\mathcal{H}$ class $H$ has to be finite, since $\mathcal{T}_S(H)$ has to be a finite group and by Theorem 2.9.3 $|H| = |\mathcal{T}_S(H)|$. □

Since maximal subsemigroups of semigroups that are groups are exactly the $\mathcal{H}$-classes that contain an idempotent, we have the following corollary.

**Corollary 8.7.8**

*Let $S$ be a semigroup with rational word problem. Every subsemigroup $G$ of $S$ that is a group is finite.*

*Proof.* The maximal subgroups of $S$ are exactly the $\mathcal{H}$-classes of $S$ that contain an idempotent. For a proof of this we refer to [How95, Theorem 2.2.5]. The result follows from 8.7.7. □

For completeness we present the following theorem. In the case where $S$ is a group and has rational word problem, $S$ has to be finite. The class of groups with rational word problem is no greater than the class of groups with recognisable word problem in the sense of Definition 6.1. This is a direct consequence of Corollary 8.7.8.

**Theorem 8.7.9**

*Let $G$ be a finitely generated semigroup that is a group. Then $G$ has rational word problem if and only if $G$ is finite.*

*Proof.* Since if $G$ is finite, $G$ has recognisable word problem by Theorem 7.2.1 and therefore rational word problem.

Conversely, by Corollary 8.7.8, all finitely generated subgroups of $G$ have to be finite. This includes $G$ itself. □

We have shown in Theorem 8.7.7 that $\mathcal{H}$-classes of semigroups with rational word problem are finite. We are conjecturing that there is a bound $n_0 \in \mathbb{N}$ such that for any $\mathcal{H}$-class H the size $|H| \leq n_0$. We also conjecture that there is a bound $n_0 \in \mathbb{N}$ such that if a $\mathcal{L}$, $\mathcal{R}$, or $\mathcal{J}$-class C is finite, then $|C| < n_0$. Note that such a bound for $\mathcal{L}$ and $\mathcal{R}$ implies the bound for $\mathcal{H}$.

**Open Question 8.7.3**

*Let S be a semigroup with rational word problem. Does there exist an $n_0 \in \mathbb{N}$ such that any $\mathcal{R}$—class, $\mathcal{L}$—class or $\mathcal{H}$— which is finite contains at most $n_0$ elements?*

A further finiteness condition on semigroups is $\mathcal{J} = \mathcal{D}$. Unsurprisingly, semigroups with rational word problem fulfil this property. We use weak stability as introduced in Section 2.9. This employs a similar idea to the proof of the same theorem for rational semigroups as can be found in [Sak87].

**Theorem 8.7.10**

*Let S be a semigroup with rational word problem. Then S is weakly stable.*

*Proof.* Let S be a semigroup with rational word problem, and let $T = S^e$. Let T be generated by A and let $\mathcal{A}$ be an automaton that decides $\iota_T(A)$.

Let $a$ and $b$ be elements of T with $aT \subset baT$. It follows that

$$TaT \subset TbaT \subset TaT$$

and therefore $a\mathcal{J} = ba\mathcal{J}$. The goal is to show that $aT = baT$, hence T is right stable.

Choose representatives $v$ and $w$ from $A^*$ with $v\pi_A = a$ and $w\pi_A = ba$. By assumption there exist strings $x$,$y$ and $z$ in $A^*$ with $(wy)\,\pi_A = a$ and $(xvz)\,\pi_A = ba$. We can replace $v$ by $wy$ and $w$ by $xvz$ and iterate that process,

$$ba = (xvz)\,\pi_A = (xwyz)\,\pi_A = (xxvzyz)\,\pi_A = (xxwyzyz)\,\pi_A = \ldots$$

and it follows that $(x^n w\,(yz)^n)\,\pi_A = ba$. The automaton $\mathcal{A}$ therefore accepts the pair $(w, x^n w\,(yz)^n)$ for every $n \in \mathbb{N}_{>0}$.

Let $n_0$ be the number of states of $\mathcal{A}$. If $n > |w|(2n_0 + 1)$, the automaton $\mathcal{A}$ must read $(\varepsilon, u)$ where $u$ is a substring of $(yz)^n$ of length at least $2n_0 + 1$. Therefore for some $m \in \mathbb{N}$ it reads $(\varepsilon, (yz)^m)$ in a loop, and hence also accepts $\left(w, x^n w (yz)^{n+m}\right)$. We get

$$\begin{aligned} ba = w\pi_A &= (x^n w (yz)^{n+m})\,\pi_A = (x^n w (yz)^n yz (yz)^{m-1})\,\pi_A \\ &= (x^n w (yz)^n y)\,\pi_A\,(z (yz)^{m-1})\,\pi_A = (wy)\,\pi_A\,(z (yz)^{m-1})\,\pi_A \\ &= ap \end{aligned}$$

for some $p \in T$. Therefore implies $ba \in aT$, hence $aT = baT$. We have shown that $T$ is right stable. An analogous argument shows that $T$ is also left stable and therefore stable.

It follows that if $S$ is weakly stable. □

The fact that for semigroups with rational word problem $\mathcal{J} = \mathcal{D}$ is now a corollary of Theorem 8.7.10.

**Theorem 8.7.11**

*Let $S$ be a semigroup with rational word problem. Then $\mathcal{J} = \mathcal{D}$.*

*Proof.* By Theorem 8.7.10 a semigroup with rational word problem is weakly stable. Applying Theorem 2.9.6 now proves the claim. □

We close this section with two open questions about $\mathcal{D}$-classes. Note that an infinite semigroup with rational word problem has infinitely many $\mathcal{R}$-classes and infinitely many $\mathcal{L}$-classes.

**Open Question 8.7.4**

*Does there exist a semigroup with rational word problem that has a $\mathcal{D}$-class that contains infinitely many $\mathcal{R}$-classes and infinitely many $\mathcal{L}$-classes?*

The following question was suggested by Abdullahi Umar. It is known [How95, Proposition 2.1.5] that if a semigroup $S$ satisfies $\min_L$ and $\min_R$, then $\mathcal{J} = \mathcal{D}$. The conditions $\min_L$ and $\min_R$ are conditions on the partial order on

$\mathcal{L}$-classes and $\mathcal{R}$-classes. A semigroup satisfies $\min_L$ if every non-empty set of $\mathcal{L}$ classes has a minimal element.

**Open Question 8.7.5**

*Let S be a semigroup with rational word problem. Does S have* $\min_L$ *and* $\min_R$*?*

## 8.8 Decidability

We consider the notion of decidability of properties of semigroups with rational word problem. Note that we assume to have the semigroup specified as a finite automaton that decides the word problem.

Firstly all the Green's relations are decidable.

**Theorem 8.8.1**

*Let S be a semigroup given by a finite automaton $\mathcal{A}$ that decides $\iota_S(A)$ for some generating set A. Then the word problems $\iota_S(A)$, $\mathcal{R}_S(A)$, $\mathcal{L}_S(A)$, $\mathcal{H}_S(A)$, $\mathcal{J}_S(A)$ and $\mathcal{D}_S(A)$ are decidable.*

*Proof.* Let S be given as the automaton $\mathcal{A}$ that accepts a pair $(v, w) \in A^+ \times A^+$ if and only if $(v, w) \in \iota_S(A)$. By the definition of decidability introduced in 4.4 and the definition of the word problem this means that the word problem of S is decidable.

By Lemma 8.7.2 the Green relations $\mathcal{R}$ and $\mathcal{L}$ are at most 2-rational and $\mathcal{H}$ is at most 4-rational. The construction of automata for $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{H}$ from $\mathcal{A}$ is effective: Constructing an automaton for the rational relations

$$\rho : A^+ \longrightarrow A^+, v \mapsto vA^*,$$

and

$$\lambda : A^+ \longrightarrow A^+, v \mapsto A^*v$$

and

$$\beta : A^+ \longrightarrow A^+, v \mapsto A^*vA^*$$

and the compositions of $\rho\iota_S(A)$, $\lambda\iota_S(A)$ and $\beta\iota_S(A)$ is effective. Now deciding whether $(v, w) \in A^+ \times A^+$ is in $\mathcal{R}_S(A)$ is done by deciding whether $(v, w)$ *and* $(w, v)$ are accepted by the automaton for $\rho\iota_S(A)$. Deciding whether $(v, w) \in A^+ \times A^+$ is in $\mathcal{L}_S(A)$ is done by deciding whether $(v, w)$ and $(w, v)$ are accepted by the automaton for $\lambda\iota_S(A)$.

Since $\mathcal{H}$ is the intersection of $\mathcal{R}$ and $\mathcal{L}$, deciding whether $(v, w) \in \mathcal{H}_S(A)$ is a matter of checking whether $(v, w)$ and $(w, v)$ are accepted by the automata for $\rho\iota_S(A)$ and $\lambda\iota_S(A)$. □

The following theorem shows how strong the property of having rational word problem is. It is undecidable in general whether a finitely presented semigroup is trivial, finite or infinite. For semigroups with rational word problem we get the following theorem.

**Theorem 8.8.2**

*Let S be a semigroup with rational word problem. Then given a finite automaton that decides $\iota_S(A)$ for some generating set A of S, it is decidable whether*

1. *S is trivial,*
2. *S is finite, or*
3. *S is infinite.*

*Proof.* Assume S has rational word problem, is finitely generated by A and $\mathcal{A}$ is an automaton that decides $\iota_S(A)$.

The semigroup S is trivial if and only if

- for all $a \in A$ it holds that $[\mathbf{aa}]\,\pi = [\mathbf{a}]\,\pi$, and
- for all $a, b \in A$ it holds that $[\mathbf{a}]\,\pi = [\mathbf{b}]\,\pi$.

This is decidable using the finite automaton given as input.

Determining the recognisable language $D \subset A^+$ in the proof of Proposition 3.7.7 is constructive. Since D only contains finitely many representatives

for each element of S, it follows that S is finite if and only if D is finite. Therefore it is decidable whether S is finite or infinite. □

It follows that we can also decide whether a semigroup with rational word problem has recognisable word problem. Note here that it is in general undecidable whether a rational relation is recognisable.

**Corollary 8.8.3**

*Let S be a semigroup with rational word problem. Then given a finite automaton that decides $\iota_S(A)$ for some finite generating set A of S it is decidable whether $\iota_S(A)$ is recognisable.*

*Proof.* The word problem $\iota_S(A)$ is recognisable if and only if S is finite, as shown in Theorem 7.2.1. This is decidable by Theorem 8.8.2. □

And from the preceding corollary we deduce that we can decide whether a semigroup with rational word problem is a group.

**Corollary 8.8.4**

*Let S be a semigroup with rational word problem. Then given a finite automaton that decides $\iota_S(A)$ for some generating set A of S it is decidable whether S is a group.*

*Proof.* It follows from Theorem 8.8.2 that it is decidable whether S is finite and by Theorem 8.7.9 any semigroup with rational word problem that is a group has to be finite. A decision procedure first decides whether S is finite, if it is not, it gives a negative answer, if S is finite the decision procedure determines whether S is a group by checking whether there is an identity element and whether every element has a uniquely determined inverse by brute force. □

We show, by employing a well-known method, for which a proof can for example be found in [BO93], that it is *un*decidable whether a semigroup given by a suitable finite specification has rational word problem.

**Theorem 8.8.5**

*Let $S = \mathrm{sg}\langle A \mid R\rangle$ be a finitely presented semigroup. It is undecidable whether S has rational word problem.*

*Proof.* Suppose for a contradiction that there exists a Turing machine $\mathcal{M}$ that decides, given a finite monoid presentation for $M = \mathrm{mon}\langle A \mid R\rangle$ as its input, whether $M$ has rational word problem.

Let $S = \mathrm{mon}\langle A_1 \mid R_1\rangle$ be a finitely presented monoid with rational word problem and let $T = \mathrm{mon}\langle A_2 \mid R_2\rangle$ be finitely presented monoid with undecidable word problem. Let $A = A_1 \cup A_2$ and $R = R_1 \cup R_2$. For any $u$ and $v$ from $A_2^*$ define

$$T_{u,v} = \mathrm{mon}\langle A, c, d \mid R, (cud, \varepsilon), (acvd, cvd) \text{ for all } a \in A \cup \{c, d\}\rangle \qquad (8.6)$$

It holds that if $u\pi_{A_2} = v\pi_{A_2}$ then $T_{u,v}$ is trivial, otherwise $T_{u,v}$ has undecidable word problem. Now the monoid free product $S * T_{u,v}$ has rational word problem if and only if $u\pi_{A_2} = v\pi_{A_2}$.

The Turing machine $\mathcal{M}$ now decides given as input $S * T_{u,v}$ whether it has rational word problem, or equivalently whether $u\pi_{A_2} = v\pi_{A_2}$, hence the word problem of $T$, which is undecidable by assumption. This is a contradiction.□

From a list in [CM09] we deduce a list of questions whose decidability should be considered in the future. This list does not claim to be complete, or a list of hard problems.

**Open Question 8.8.1**

*Let $S$ be a semigroup with rational word problem. Is it decidable, given a finite automaton $\mathcal{A}$ that decides $\iota_S(A)$ for some generating set $A$ of $S$, whether*

1. *$S$ is cancellative,*
2. *$S$ is left- or right-stable,*
3. *$S$ contains an idempotent,*
4. *$S$ is a one-relator semigroup,*
5. *$S$ has an identity,*

6. *$S$ has a zero,*
7. *$S$ has a non-trivial subgroup,*
8. *$S$ is a direct product,*
9. *$S$ is a free product.*
10. *given a semigroup $T$ with rational word problem, $S \cong T$.*

Note that point 1 of Open Question 8.8.1 is already answered for finite semigroups in Corollary 8.8.4 because a finite semigroup is cancellative if and only if it is a finite group. Also note that for automatic semigroups cancellativity is undecidable, this was shown by Alan Cain in [Cai06]. An answer to Open Question 8.10.1 would conceivably help answering this particular question.

Maybe more generally we want to ask the following question, to which without a doubt there exists some answer.

**Open Question 8.8.2**

*Let $S$ be a semigroup with rational word problem. Find an undecidable problem.*

**Open Question 8.8.3**

*Let $S$ and $T$ be semigroups with rational word problem. Given automata that decide $\iota_S(A)$ and $\iota_T(B)$, is there an algorithm that decides whether $S$ and $T$ are isomorphic?*

In the book [Eps+92a] the authors show that there exists an algorithm that, given a finite group presentation as input, computes an automatic structure for the group specified by the presentation if it exists. This algorithm heavily relies on axiom checking on finite state automata. There are implementations of the algorithm, but they are restricted to subclasses of the class of automatic groups. Even if we give such an implementation a presentation of a group, it might run out of memory or take far too long to be useful.

It might not be possible to find such an algorithm for rational word problem semigroups, since the problems involved are undecidable in general for rational congruences.

Preliminary work by Mark Kambites in [Kam09a; Kam09b] and independently by the author hints at the possibility that an algorithm that given a semigroup presentation as input computes a finite state automaton that decides $\iota_S(A)$ if it exists. We state the following open problem or project task. It is a consequence of Theorem 8.8.5 that we cannot hope for an algorithm that terminates on all inputs and computes a correct automaton if and only if the presentation given as input specifies a semigroup with rational word problem.

**Open Question 8.8.4**

*Does there exist an algorithm that, given a semigroup presentation* $S = \mathrm{sg}\langle A \mid R\rangle$ *as input, computes a finite automaton that decides* $\iota_S(A)$*?*

## 8.9 Complexity

We have shown that rational word problem semigroups have decidable word problem given an effective specification of the rational relation. We have also shown that finiteness and triviality are decidable in that case. This immediately yields that the decision problem whether a semigroup has rational word problem must be undecidable. We will also briefly discuss the time and space complexity of the word problem and related problems, in particular we will show that the word problem is decidable in time quadratic in the sum of the length of the input strings.

**Theorem 8.9.1**

*Let* $S$ *be a semigroup specified by a finite automaton deciding* $\iota_S(A)$ *for some generating set* $A$ *of* $S$*. Given* $(v, w)$ *it can be decided in time* $\mathcal{O}\left((|v| + |w|)^2\right)$ *and space* $\mathcal{O}((|v| + |w|))$ *whether* $(v, w) \in \iota_S(A)$*.*

*Proof.* This follows directly from Theorem 4.4.2. □

The complexities of the Green relations all depend on the constructions of the automaton for the word problem.

## 8.10 Further Questions

The following conjecture states that for semigroups that are cancellative we can find a deterministic automaton that decides the word problem. For finite semigroups this is true, since for finite semigroups we have recognisable word problem.

**Open Question 8.10.1**

*Is a semigroup with rational word problem is cancellative if and only if* $\iota_S(A)$ *is a deterministic rational relation?*

Another relative of groups in semigroups are the inverse semigroups. The following question was asked by Stuart Margolis.

**Open Question 8.10.2**

*Does there exist an infinite inverse semigroup with rational word problem?*

# 9

⊙ ● ○

# *Polyrational Word Problem*

In this chapter we generalise the notion of rational word problem to polyrational word problem. We remind ourselves of the definition of polyrational relations as given in Section 3.8. Let $S$ be a semigroup finitely generated by $A$ and let $S \xrightarrow{\rho} S$ be a relation. Then $A^+ \xrightarrow{\rho(A)} A^+$ is $k$-*rational* if it is an intersection of $k$ rational relations, more formally

$$\rho(A) = \bigcap_{i \in \underline{k}} \rho_i(A)\,,$$

and $\rho_i(A)$ are rational relations for $i \in \underline{k}$.

We call a relation that has $k$-rational word problem for some $k \in \mathbb{N}_{>0}$ a $k$-rational relation, again by slight abuse of nomenclature. If we just want to say that there exists some $k \in \mathbb{N}$ such that $\rho(A)$ is $k$-rational we also say that $\rho(A)$ is polyrational.

A relation being polyrational is in line with the concept of an effectively and easily soluble word problem: Deciding the word problem of an intersection involves deciding a finite number of rational relations which can be

done effectively, because the word problem of a rational relation is effectively decidable.

## 9.1 Generators

We extend the results of Section 8.1 to polyrational relations.

**Theorem 9.1.1**

*Let $S$ be a semigroup and $S \xrightarrow{\rho} S$ be a relation on $S$ such that*

$$\rho = \bigcap_{i \in \underline{k}} \rho_i$$

*for $k$ relations $S \xrightarrow{\rho_i} S$ with $\rho_i(A)$ rational for all $i \in \underline{k}$ for some finite generating set $A$ of $S$. Then*

$$\rho(A) = \bigcap_{i \in \underline{k}} \rho_i(A)$$

*and for any finite generating set $B$ of $S$ the relation $\rho(B)$*

$$B^+ \xrightarrow{\pi_B} S \xrightarrow{\rho} S \xrightarrow{\pi_B^r} B^+$$

*has the property that*

$$\rho(B) = \bigcap_{i \in \underline{k}} \rho_i(B)$$

*for the rational relations $B^+ \xrightarrow{\rho_i(B)} B^+$.*

*Proof.* Let $v$ and $w$ be in $A^+$ then

$$\begin{aligned} w \in v\rho(A) &\Leftrightarrow w\pi_A \in v\pi_A\rho \\ &\Leftrightarrow w\pi_A \in v\pi_A\rho_i \text{ for all } i \in \underline{k} \\ &\Leftrightarrow w \in v\rho_i(A) \text{ for all } i \in \underline{k}. \end{aligned}$$

Let now $B$ be another finite generating set for $S$. Then $\rho_i(B)$ is rational by Theorem 8.1.3, and for $v$ and $w$ in $B^+$ we have $w \in v\rho(B)$ if and only if $w\pi_B \in v\pi_B\rho$. □

For completeness we also give the following two lemmas. The proofs are the same as the proofs of Lemma 8.1.1 and 8.1.2 and are therefore omitted. Note that the proofs rely on Theorems 3.8.2 and 3.8.3.

**Lemma 9.1.2**

*Let* $S$ *be a semigroup finitely generated by* $A$ *and let* $S \xrightarrow{\rho} S$ *be a* $k$*-rational relation. Then for any subset* $B \subset A$ *the restriction* $T \xrightarrow{\rho} T$ *of* $\rho$ *to the subsemigroup generated by* $B$ *is a* $k$*-rational relation.*

**Lemma 9.1.3**

*Let* $S$ *be a semigroup finitely generated by* $A$ *and let* $S \xrightarrow{\rho} S$ *be a* $k$*-rational relation. Then for any superset* $B \supset A$ *the relation* $\rho(B)$ *is* $k$*-rational.*

We conclude from the preceding lemmas that finitely generated subsemigroups of semigroups with polyrational word problem have polyrational word problem. Again the proof is identical to the proof of Theorem 8.5.1.

**Corollary 9.1.4**

*Let* $S$ *be a semigroup finitely generated by* $A$ *and let* $T$ *be a finitely generated subsemigroup of* $S$*. If* $S$ *has* $k$*-rational word problem then* $T$ *has* $k$*-rational word problem.*

## 9.2 *The Polyrational Hierarchy*

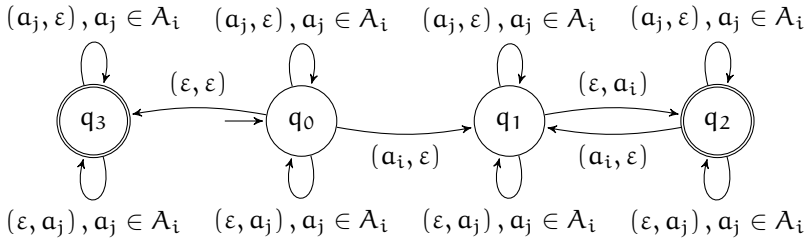
We prove a hierarchy theorem which establishes that for $k \in \mathbb{N}_{>0}$ the semigroup $CS(k)$ with respect to the generating set $A = \{a_1, \ldots, a_k\}$ has strictly $k$-rational word problem.

This ensures the existence of an infinite hierarchy of semigroups with increasing word problem complexity. The class of semigroups with rational word problem is naturally contained in the class of semigroups with polyrational word problem.

**Theorem 9.2.1**

*Let* $k \in \mathbb{N}$*. The semigroup* $CS(k)$ *has* $k$*-rational word problem.*

*Proof.* Let $A = \{a_1, \ldots, a_k\}$ be a generating set for $CS(k)$ and let $A_i = A \setminus \{a_i\}$. For $1 \leq i \leq k$ define the rational relation $\rho_i(A)$ by the automaton $\mathcal{A}_i$.




A string $w$ is in $v\rho_i$ if and only if $|v|_{a_i} = |w|_{a_i}$ and therefore

$$\iota_{CS(k)}(A) = \bigcap_{i \in \underline{k}} \rho_i(A),$$

since $v$ and $w$ represent the same element of $CS(k)$ if and only if $|v|_{a_i} = |w|_{a_i}$ for all $i \in \underline{k}$ which is the case if and only if $w \in v\rho_i(A)$ for all $i \in \underline{k}$. This shows that $CS(k)$ has $k$-rational word problem with respect to the generating set $A$ and therefore with respect to any finite generating set. □

Note that all $\rho_i(A)$ used in the proof of Theorem 9.2.1 are rational *congruences*. In fact ${}^{A^+}/_{\rho_i(A)}$ and ${}^{CS(k)}/_{\rho_i}$ are isomorphic to the free monogenic monoid, and $CS(k)^{\mathbf{e}}$ is isomorphic to the direct product of $k$ monogenic monoids.

In Theorem 9.2.1 it is only shown that $\iota_{CS(k)}(A)$ is *at most* $k$-rational, to make the bound strict we prove the following theorem. The proof is another application of the iteration lemma 3.7.6. We have to take care that we can pump all involved relations at the same time.

**Theorem 9.2.2**

*The free commutative semigroup* $CS(k)$ *for* $k > 1$ *does not have* $(k-1)$*-rational word problem.*

*Proof.* Assume for a contradiction that $\iota_{CS(k)}(A)$ is $(k-1)$-rational and note that we can without loss of generality assume $k > 2$ since the case $k = 2$ is proven in Theorem 8.2.2.

By the definition of a k-rational relation it holds that

$$\iota_{CS(k)}(A) = \bigcap_{i \in \underline{k-1}} \rho_i,$$

where $A^+ \xrightarrow{\rho_i} A^+$ are rational relations. The relation

$$\tau : A^+ \longrightarrow A^+,\ a_k^+ a_{k-1}^+ \cdots a_1^+ \mapsto a_1^+ a_2^+ \cdots a_k^+$$

is recognisable by Theorem 3.6.2. For any choice of j and j′ from $\underline{k}$ with $j < j'$ the relation

$$\sigma_{j,j'} : A^+ \longrightarrow A^+,\ a_j^+ a_{j'}^+ \mapsto a_{j'}^+ a_j^+$$

is recognisable, again by Theorem 3.6.2.

Therefore, the relations $\tau_i = \rho_i \cap \tau$ and $\tau_i \cap \sigma_{j,j'}$ are rational by Lemma 3.4.4, and the relation

$$\theta = \iota_{CS(k)}(A) \cap \tau = \bigcap_{l \in \underline{k-1}} \tau_i$$

is $(k-1)$-rational.

There exists an $n_0 \in \mathbb{N}$ such that for i,j and j′ and all $\alpha$, $\beta$, $\alpha'$ and $\beta'$ greater than $n_0$, if a pair $(v, w)$ with

$$v = a_{j'}^{\alpha'} a_j^{\alpha} \text{ and}$$
$$w = a_j^{\beta} a_{j'}^{\beta'}$$

is contained in the graph $\mathcal{G}_{\tau_i \cap \sigma_{j,j'}}$, then the following cases can occur. Either $\alpha = \beta$ and $\alpha'$ and $\beta'$ are arbitrary elements of $\mathbb{N}$ greater than $n_0$, or $\alpha' = \beta'$ and $\alpha$ and $\beta$ are arbitrary elements of $\mathbb{N}$ greater than $n_0$ or $\alpha, \beta, \alpha'$ and $\beta'$ are arbitrary elements of $\mathbb{N}$ greater than $n_0$.

It follows from the iteration lemma that $\alpha = \beta$ and $\alpha' = \beta'$ cannot occur.

Note that $\tau_i \cap \sigma_{j,j'}$ has to contain all pairs with $\alpha = \beta$ and $\alpha' = \beta'$. If $\alpha = \beta$ for all $\alpha > n_0$, it follows by applying the iteration lemma, that $\alpha'$ and $\beta'$ can be chosen arbitrarily, and the same holds for the case where $\alpha' = \beta'$ for all $\alpha' > n_0$.

If neither $\alpha = \beta$ nor $\alpha' = \beta'$ then $\alpha$, $\beta$, $\alpha'$ and $\beta'$ are arbitrary.

We can therefore find a letter $a_j$ and relation $\tau_i$ such that the graph of $\tau_i$ consists of pairs $(v', w')$ where

$$v' = a_k^{\alpha_k} \cdots a_j^{n_j} \cdots a_1^{\alpha_1}, \qquad w' = a_1^{\beta_1} \cdots a_j^{n_j} \cdots a_k^{\beta_k}$$

and $\alpha_l$ and $\beta_l$ arbitrary greater than $n_0$.

We now proceed by induction. For assume that $CS(k)$ had $(k-1)$-rational word problem. Then $\theta$ is $(k-1)$-rational and we find $\tau_i$ and $a_j$ as above and form the relation

$$\theta' = \bigcap_{\substack{l \in \underline{k-1} \\ l \neq i}} \tau_i$$

which is $(k-2)$-rational. Applying induction, it follows that there are $j$ and $j'$ such that the graph of the rational relation $\iota_{CS(2)}(A) \cap \sigma_{j,j'}$ precisely consists of pairs $(v'', w'')$ where

$$v'' = a_{j'}^{\alpha'} a_j^{\alpha},$$
$$w'' = a_j^{\beta} a_{j'}^{\beta'}$$

such that $\alpha = \beta$ and $\alpha' = \beta'$ for $\alpha$ and $\alpha'$ arbitrary greater than $n_0$. This concludes the proof.

We have thus shown that there is at least one semigroup with strictly $k$-rational word problem for every $k \in \mathbb{N}$. We have established an infinite hierarchy of semigroups with increasing complexity of the word problem. We will detail this hierarchy in Chapter 10.

Furthermore, applying the above theorems gives the following.

**Theorem 9.2.3**

*Let $S$ be a semigroup and let $\iota_S(A)$ be $k$-rational. Then the maximal rank of a free commutative subsemigroup of $S$ is $k$.*

*Proof.* Assume for a contradiction that $S$ is a semigroup with $k$-rational word problem and that $T$ is a subsemigroup of $S$ which is free commutative of rank $l$ with $l > k$. Applying Corollary 9.1.4 yields that $T$ has at most $k$-rational word problem. This contradicts Theorem 9.2.2. □

## 9.3 Counterexamples

We show that the class of semigroups with polyrational word problem does not contain the bicyclic monoid or the integers.

**Theorem 9.3.1**

*The bicyclic monoid* $B$ *does not have polyrational word problem.*

*Proof.* Assume for a contradiction that $\iota_B(A)$ is $k$-rational for some $k \in \mathbb{N}_{>0}$ and the generating set $A = \{b, c\}$ as given in Section 5.3.

Let $\mathcal{A}_i$ for $i \in \underline{k}$ be automata with behaviour $\rho_i(A)$ such that

$$\iota_B(A) = \bigcap_{i \in \underline{k}} \rho_i(A)\,.$$

Applying the iteration lemma 3.7.6 to each $\mathcal{A}_i$ yields an $n_0 \in \mathbb{N}_{>0}$ with the property that each $\mathcal{A}_i$ accepts the pair $(b^{n_0}c^{n_0}, \varepsilon)$ and the pair $\left(b^{n_0+n_i l}c^{n_0}, \varepsilon\right)$ for $n_i \in \mathbb{N}_{>0}$ and all $l \in \mathbb{N}$. This implies that $(b^{n_0+n}c^{n_0}, \varepsilon)$ is accepted by $\mathcal{A}_i$ for all $i \in \underline{k}$, where

$$n = \operatorname{lcm}\{n_i \mid i \in \underline{k}\}\,.$$

Hence $\iota_B(A)$ is not $k$-rational. Since $k$ was chosen arbitrarily this shows that $\iota_B(A)$ is not $k$-rational for any $k \in \mathbb{N}$. □

In very much the same way we show that the integers do not have polyrational word problem.

**Lemma 9.3.2**

*The integers do not have polyrational word problem.*

*Proof.* Assume for a contradiction that the monoid word problem $\iota_{\mathbb{Z}}(A)$ is $k$-rational for some $k \in \mathbb{N}_{>0}$ and the monoid generating set $A = \{a, b\}$ given in Section 5.4.

Let $\mathcal{A}_i$ for $i \in \underline{k}$ be automata with behaviour $\rho_i(A)$ such that

$$\iota_{\mathbb{Z}}(A) = \bigcap_{i \in \underline{k}} \rho_i(A) .$$

Applying the iteration lemma 3.7.6 to each $\mathcal{A}_i$ yields some $n_0 \in \mathbb{N}_{>0}$ with the property that each $\mathcal{A}_i$ accepts the pair $(a^{n_0} b^{n_0}, \varepsilon)$ and the pair $\left(a^{n_0+n_i l} b^{n_0}, \varepsilon\right)$ for $n_i \in \mathbb{N}_{>0}$ and all $l \in \mathbb{N}$.

This implies that $(a^{n_0+n} b^{n_0}, \varepsilon)$ is accepted by all $\mathcal{A}_i$, where

$$n = \operatorname{lcm}\{n_i \mid i \in \underline{k}\} .$$

Hence $\iota_{\mathbb{Z}}(A)$ is not $k$-rational. Since $k$ was chosen arbitraily this shows that $\iota_{\mathbb{Z}}(A)$ is not $k$-rational for any $k \in \mathbb{N}$. □

Answering the following question in the positive would also, just as in Chapter 8, establish that the class of semigroups with polyrational word problem does not contain any infinite group.

**Open Question 9.3.1**

*Let $S$ be a semigroup with polyrational word problem. If $H$ is an $\mathcal{H}$-class of $S$, is $H$ necessarily finite?*

## 9.4 Direct Products

In the proof of Theorem 9.2.1 we defined congruences $\rho_i$ such that ${}^{A^+}/_{\rho_i}$ was isomorphic to a monogenic monoid and such that

$$\mathrm{CS}(k)^{\mathbf{e}} \cong {}^{A^+}/_{\rho_1} \times \cdots \times {}^{A^+}/_{\rho_k} .$$

We first extend our results about direct products by showing that the class of semigroups with polyrational word problem is closed under taking finite direct products. The class of semigroups with polyrational word problem thus

contains the closure of the class of semigroups with rational word problem under taking finite direct products.

We prove first that if a direct product of two semigroups has polyrational word problem, then the factors have polyrational word problem. Also compare the proof to that of Theorem 8.6.3.

**Theorem 9.4.1**

*Let* $S$ *and* $T$ *be semigroups. If* $S \times T$ *is finitely generated and has polyrational word problem, then* $S$ *and* $T$ *have polyrational word problem.*

*Proof.* Let $S \times T \xrightarrow{\pi_S} S$ be the projection onto $S$ and let $A$ be a finite generating set for $S \times T$. Denote by $\sigma$ the kernel of the map $\pi_A\pi_S$ restricted to $A$. The equivalence relation $A \xrightarrow{\sigma} A$ extends to an equivalence relation $A^+ \xrightarrow{\sigma} A^+$. Consider the composition

$$A^+ \xrightarrow{\sigma} A^+ \xrightarrow{\iota_{S\times T}(A)} A^+ \xrightarrow{\sigma^r} A^+,$$

which we denote by $\tau$. We claim that $\tau = \iota_S(A)$.

Let $v$ and $w$ be elements of $A^+$. If $w \in v\tau$ then $w\pi_A\pi_S = v\pi_A\pi_S$, hence $w \in v\iota_S(A)$.

Conversely, if $w \in v\iota_S(A)$, then $w\pi_A\pi_S = v\pi_A\pi_S$, which implies that there exist strings $w'$ and $v'$ in $A^+$ such that $w' \in w\sigma$ and $v \in v'\sigma$ and $w' \in v'\iota_{S\times T}(A)$ and hence $w \in v\tau$. This concludes the proof. □

We show that the class of semigroups with polyrational word problem is closed under taking direct products. More precisely we show that if the direct product of a semigroup with $k$-rational word problem and a semigroup with $l$-rational word problem is finitely generated, then it has $(k+l)$-rational word problem.

**Theorem 9.4.2**

*Let* $S$ *and* $T$ *be semigroups. If* $S$ *has* $k$*-rational word problem,* $T$ *has* $l$*-rational word problem and* $S \times T$ *is finitely generated, then* $S \times T$ *has* $(k+l)$*-rational word problem.*

*Proof.* Let $S$ be a semigroup with $k$-rational word problem and $T$ be a semigroup with $l$-rational word problem and let $S_1 \times S_2$ be finitely generated by $A$.

Then $A$ also generates $S$ and $T$ via $\pi_A\pi_S$ and $\pi_A\pi_T$ where $S \times T \xrightarrow{\pi_S} S$ and $S \times T \xrightarrow{\pi_T} T$ are the projections onto the factors.

Since the relation $\iota_S(A)$ is $k$-rational and the relation $\iota_T(A)$ is $l$-rational by assumption, the relation

$$\rho = \iota_S(A) \cap \iota_T(A)\,,$$

is $(k+l)$-rational.

It holds that $w \in \nu\rho$ if and only if $w \in \nu\iota_S(A)$ and $w \in \nu\iota_T(A)$, which is the case if and only if $w\pi_A\pi_S = \nu\pi_A\pi_S$ and $w\pi_A\pi_T = \nu\pi_A\pi_T$, which is the case if and only if $w \in \nu\iota_{S\times T}(A)$.

It follows that $\rho = \iota_{S\times T}(A)$ and therefore $\iota_{S\times T}(A)$ is $(k+l)$-rational and the proof is complete. □

The previous two theorems can also be stated as the following characterisation of direct products of semigroups with polyrational word problem.

**Theorem 9.4.3**

*Let $S$ and $T$ be semigroups such that $S \times T$ is finitely generated. The direct product $S \times T$ has polyrational word problem if and only if $S$ and $T$ have polyrational word problem.*

*Proof.* This follows by applying Theorem 9.4.1 and 9.4.2. □

We give a partial converse to the above theorem. We cannot conclude that a $k$-rational congruence decomposes into $k$ rational congruences: If we consider the congruence $\mathcal{D}$, we have only shown that it is polyrational and from all we know the relations making up the intersection are not congruences.

**Theorem 9.4.4**

*Let $S$ be a semigroup finitely generated by $A$ with polyrational word problem such that*

$$\iota_S(A) = \rho_1(A) \cap \rho_2(A)$$

*where $\rho_1(A)$ and $\rho_2(A)$ are polyrational congruences and such that the smallest congruence on $A^+$ that contains $\rho_1(A)$ and $\rho_2(A)$ is the universal congruence. Then*

$$S \cong {}^{A^+}\!/_{\rho_1(A)} \times {}^{A^+}\!/_{\rho_2(A)},$$

*and therefore $S$ is isomorphic to a direct product of two semigroups with polyrational word problem. Furthermore, if $\iota_S(A)$ is $k$-rational, then $\rho_1$ is $k_1$-rational and $\rho_2$ is $k_2$-rational, then $k = k_1 + k_2$.*

*Proof.* This follows from Theorem 2.10.3. □

Note that the above theorem does *not* imply that every semigroup with $k$-rational word problem is a direct product of at most $k$ semigroups with rational word problem. It is not clear that that we can decompose any $k$-rational congruence into rational congruences, much to the opposite we conjecture that this is not possible in general.

Also, we have shown that $\mathrm{CS}(k)$ has $k$-rational word problem, but $\mathrm{CS}(k)$ is only a subsemigroup of finite Rees index of a direct product of $k$ monogenic monoids and not itself a direct product.

However, we can conclude that if a semigroup with $k$-rational word problem is a direct product, there are at most $k$ infinite factors involved.

**Open Question 9.4.1**

*Does there exist a semigroup with polyrational word problem that is not a subsemigroup of a direct product of semigroups with rational word problem?*

## 9.5 Rational Subsets and Kleene's Theorem

If a semigroup S has k-rational word problem for $k > 1$, then S is in general not a Kleene semigroup. The free commutative monoid of rank 2 has 2-rational word problem and Kleene's theorem does not hold, for if $a_1$ and $a_2$ are two generators for the free commutative semigroup of rank two, then the set $(a_1a_2)^+$ is rational but not recognisable.

**Lemma 9.5.1**

*Let* $A = \{a_1, a_2\}$, $S = CS(A)$, *and* $X$ *be the rational subset of* $S$ *given by the rational expression* $(a_1a_2)^+$. *Then* $X$ *is not in* $\operatorname{Rec} S$.

*Proof.* Assume for a contradiction that $X \in \operatorname{Rec} S$. There is a semigroup morphism $CS(A) \xrightarrow{\varphi} T$ with $T$ finite and a subset $F \subset T$ such that $X = F\varphi^{-1}$.

Now consider the semigroup morphism $A^+ \xrightarrow{\pi_A} CS(A)$ and the concatenation $\pi_A\varphi$. This concatenation recognises the subset

$$F(\pi_A\varphi)^{-1} = \left\{ v \in A^+ \mid |v|_{a_1} = |v|_{a_2} \right\}.$$

Now applying the iteration lemma 3.2.4 yields that this is a contradiction. □

For a semigroup S finitely generated by A we proved that if S has rational word problem, then the preimage of a rational subset X of S under $\pi_A$ is a rational subset of $A^+$ in Section 8.4. We have shown that the congruence $\iota_S(A)$ is compatible with the rational constructions from Definition 3.3.1. By extension, if $\iota_S(A)$ is polyrational, then the congruence classes are intersections of congruence classes of the rational relations involved.

We show that semigroups with polyrational word problem are residually finite. This follows from our results in Section 8.4.

**Theorem 9.5.2**

*Let* $S$ *be a finitely generated semigroup with polyrational word problem. Then* $S$ *is residually finite.*

*Proof.* Let $S$ be generated by a finite set $A$ and let

$$\iota_S(A) = \bigcap_{i \in \underline{k}} \rho_i.$$

Then for $v \in A^*$ the set $v\rho_i$ is a recognisable subset of $A^*$ and $v\iota_S(A)$ is an intersection of $k$ recognisable subsets of $A^*$, and therefore a recognisable subset of $A^*$. Since $v\iota_S(A) = v\pi_A\pi_A^{-1}$, by applying Theorem 8.4.5 it follows that $S$ is residually finite. □

We can now give an alternative proof for Lemma 9.3.1, the bicyclic monoid does not have polyrational word problem, because it is not residually finite.

**Corollary 9.5.3**

*The bicyclic monoid* $B$ *does not have polyrational word problem.*

*Proof.* If for some generating set $A$ for the bicyclic monoid $B$ the word problem $\iota_B(A)$ was rational, then $B$ would be residually finite by Theorem 9.5.2, which contradicts Lemma 5.3.1. □

## 9.6 Green's Relations

In this section we show that Lemma 8.7.2 naturally extends to semigroups with polyrational word problem. Compare the proof also with the proof of Lemma 8.7.2.

We also emphasise that the Green's relations of a semigroup with polyrational word problem are decidable.

**Lemma 9.6.1**

*Let $S$ be a semigroup with polyrational word problem. Then the relations $\mathcal{L}$, $\mathcal{R}$, $\mathcal{D}$, $\mathcal{J}$ and $\mathcal{H}$ are polyrational.*

*Proof.* The relations $A^+ \xrightarrow{\rho} A^+$, $A^+ \xrightarrow{\lambda} A^+$ and $A^+ \xrightarrow{\sigma} A^+$ as defined in the proof of Lemma 8.7.2 and rational.

Applying Theorems 3.8.2 and 3.8.3 yields that the relations $\rho\iota_S(A)$, $\lambda\iota_S(A)$ and $\sigma\iota_S(A)$ are polyrational and the result now follows by the same argument as applied in the proof of Lemma 8.7.2 □

It should be established whether we can effectively bound the number of rational relations required to express Green's relations in a semigroup with polyrational word problem.

**Open Question 9.6.1**

*Let $S$ be a semigroup such that for a finite generating set $A$ the word problem $\iota_S(A)$ is $k$-rational. Give minimal $n_\rho \in \mathbb{N}$ for each Green relation $\rho$ among $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, $\mathcal{J}$ and $\mathcal{D}$ such that $\rho$ is $n_\rho$-rational.*

# 10

⊙ ● ⊙

# *The (Co)Word Problem Hierarchy*

This chapter will give connections from the previous chapters to related research in word problems and connections between semigroup theory and computation. We give an infinite complexity hierarchy of semigroups based on the computational complexity of their word and coword problem in the natural representation as congruences on strings. We call the collections of semigroups with a certain property *classes of semigroups*, since such collections are not sets in the sense of ZFC.

This hierarchy is inspired by hierarchies in complexity theory, for example the polynomial hierarchy. The polynomial hierarchy was introduced in [MS72], and has gained some attention in the analysis of the P vs. NP problem. Eilenberg in [Eil76a] envisioned a hierarchy of Rational phenomena and announced in Volume A that these would be treated in Volume C of his four volume monograph on automata and machines. Eilenberg never finished Vol-

ume C. There are some notes available for download from Jean Berstel that Eilenberg took in preparation for Volume C [Eil98].

We will point out on which levels we already have information about the hierarchy and on which levels future research is needed.

Figure 10.1 shows the relevant levels of the (Co)Word Problem Hierarchy. We define the top level of the presented hierarchy here. We note that the hierarchy can be extended further by using the idea of an oracle for example, but our main interest here are semigroups with decidable word problem, more specifically, semigroups with efficiently decidable word problem.

The *class of semigroups with decidable word problem* is defined as

$$\mathbf{Dec} = [\ S \mid S \text{ has decidable word problem } ],$$

and the *class of semigroups with decidable coword problem* is defined as

$$\mathbf{CoDec} = [\ S \mid S \text{ has decidable coword problem } ].$$

We note that the two classes coincide.

In the following sections we will show how some other classes of semigroups with naturally defined notions of word problem complexity fit into the hierarchy. A major question is whether it is possible to meaningfully extend the proposed hierarchy, while preserving as many nice properties as possible. A nice property is for example decidability of properties of a semigroup in a given class.

A possible step is to give automata more expressivity, for example by adding a single stack, yielding one stack pushdown automata. Note that adding two stacks would result in the full power of a Turing Machine, effectively resulting in undecidable problems. It is also possible to give the automata algebraic memory, for example the group of integers instead of a stack. A slightly different approach would be to employ Petri-net [Pet62; Pet66] counting memories. A very powerful approach from the field of complexity theory are oracles that answer well defined decision problems instantly.

This would enable defining semigroups with word problems that are decidable relative to some, possibly undecidable, decision problem.

There seems to be an abundance of possibilities which is only waiting to be explored.

## 10.1 Recognisable (Co)Word Problem

In this section we begin with the *class of semigroups with recognisable word problem*,

$$\mathbf{Rec} = [\, S \mid S \text{ is finitely generated and has recognisable word problem} \,],$$

and the *class of semigroups with recognisable coword problem*,

$$\mathbf{CoRec} = [\, S \mid S \text{ is finitely generated and has recognisable coword problem} \,].$$

By Theorem 7.2.1, the classes **Rec** and **CoRec** coincide, and characterise the class of finite semigroups. This is particularly interesting, but not necessarily surprising, since a class from group theory directly extends to semigroup theory in this case.

It is also clear that the above classes are not empty since we gave at least one example of a finite semigroup in Section 5.1.

We have shown that word problems of semigroups in this class are efficiently decidable in time $\mathcal{O}(|v| + |w|)$ by using deterministic finite state automata. We have also shown in Corollary 8.8.3 that membership in this class is decidable inside the class **Rat** of semigroups with rational word problem. This means that given a semigroup $S$ in **Rat** specified by a finite state automaton, it is decidable whether $S$ is in **Rec**.

Note that in contrast it is undecidable, as shown in [Ber79], whether a given rational relation is recognisable.

Open Question 7.2.1 asks for a characterisation of semigroups recognising word problems of semigroups.

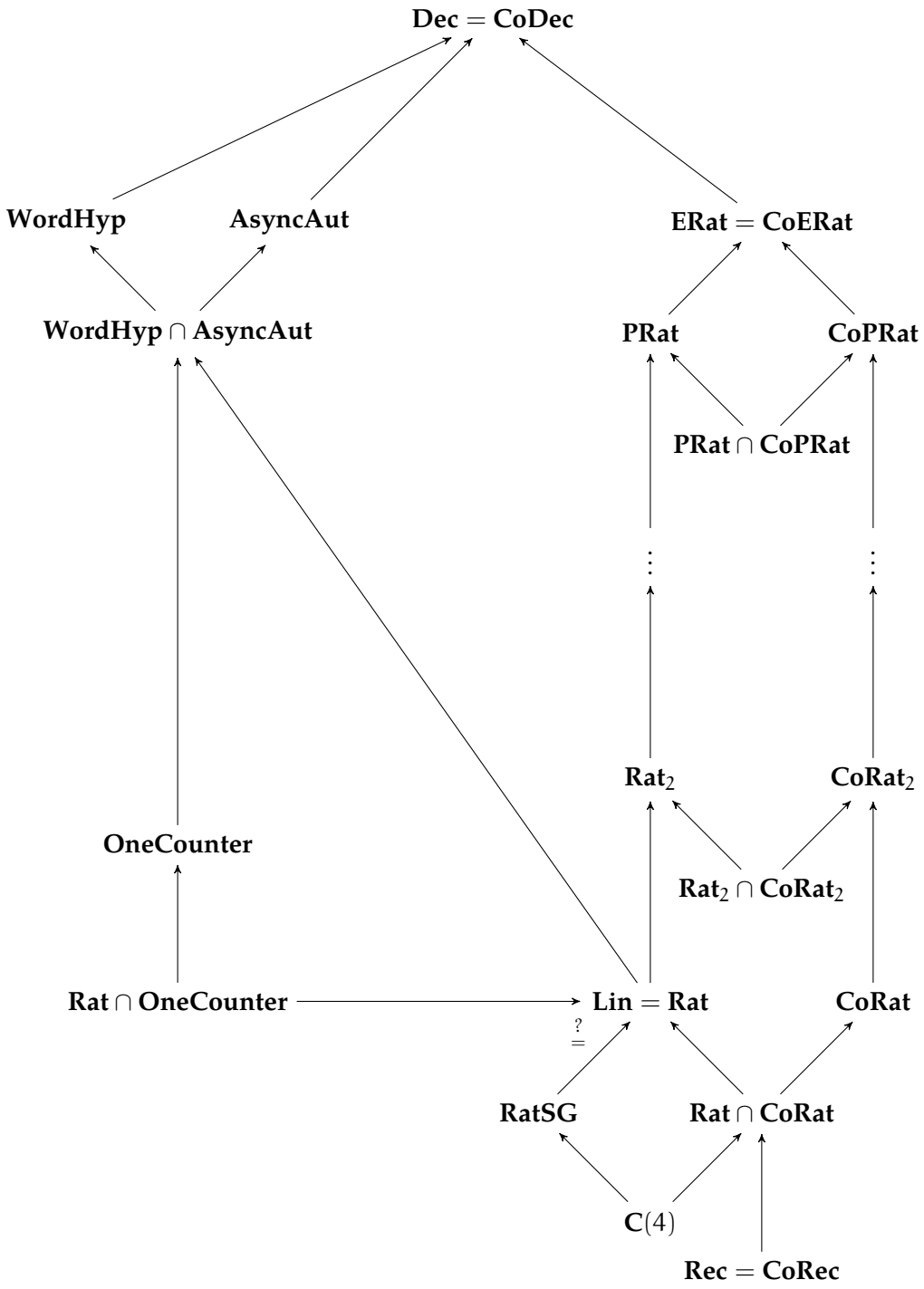



Figure 10.1: The (Co)Word Problem Hierarchy

There is a large body of research dealing with varieties of finite semigroups, described for example in [Eil76b]. Varieties are a tool to describe classes of finite semigroups and might give means to attack Open Question 7.2.1, and give finer subdivisions of the class **Rec**.

## 10.2 Rational, Polyrational and Extended Rational (Co)Word Problem

Next, we define classes of semigroups with rational, polyrational and extended rational word problem and coword problem. We developed a few results about semigroups in these classes in Chapters 7, 8, and 9.

First, we go ahead with the definitions; The *class of semigroups with rational word problem* is defined as

$$\mathbf{Rat} = [\, S \mid S \text{ is finitely generated and has rational word problem } ],$$

and the *class of semigroups with rational coword problem* is defined as

$$\mathbf{CoRat} = [\, S \mid S \text{ is finitely generated and has rational coword problem } ].$$

For $k \in \mathbb{N}_{>0}$, the *class of semigroups with* k*-rational word problem* is defined as

$$\mathbf{Rat}_k = [\, S \mid S \text{ is finitely generated and has } k\text{-rational word problem } ],$$

and the *class of semigroups with* k*-rational coword problem* is defined as

$$\mathbf{CoRat}_k = [\, S \mid S \text{ is finitely generated and has } k\text{-rational word problem } ].$$

As an upper bound for the classes defined above, we define the *class of semigroups with polyrational word problem*,

$$\mathbf{PRat} = [\, S \mid \text{ there is } k \in \mathbb{N} \text{ with } S \text{ in } \mathbf{Rat}_k \,],$$

and the *class of semigroups with polyrational coword problem*

$$\mathbf{CoPRat} = [\, S \mid \text{ there is } k \in \mathbb{N} \text{ with } S \text{ in } \mathbf{CoRat}_k \,].$$

Finally, according to the definitions in Section 3.5, we define the *class of semigroups with extended rational word problem*.

**ERat** $= [\, S \mid S$ is finitely generated and has extended rational word problem $]$.

We have thus defined infinitely many classes of semigroups. Just from the definition, it is not clear whether these classes are empty, what the relationships between these classes are, and whether any of them are distinct.

We deduce the following relationships and properties of the classes defined above results in Chapters 8 and 9.

The classes **Rat** and **CoRat** are not empty, since they both contain the free semigroup on one generator. This also implies that the class **Rat** $\cap$ **CoRat** is not empty. We can also deduce that the inclusion **Rec** $\subset$ **Rat** $\cap$ **CoRat** is proper by using Theorem 7.2.1.

A related question is whether there is a semigroup with rational word problem that does not have rational coword problem. This is also related to the question whether we can always find a deterministic automaton that decides the word problem. Note that this is a question about the relationship of **Rat** and **CoRat**: In Section 10.4 we will draw a connection between rational word problem and a different way of defining the class of semigroups with rational word problem, so called linear context-free grammars. It is known for groups that if a group has context-free word problem, then it also has context-free coword problem.

**Open Question 10.2.1**
*Does there exist a semigroup $S$ that has rational word problem but does not have rational coword problem?*

We have shown in Theorem 9.2.1 that for $k \in \mathbb{N}_{>0}$ the class $\mathbf{Rat}_k$ contains the free commutative semigroup on $k$ generators, and is therefore not empty. We have also shown in Theorem 9.2.2 that, for every $k \in \mathbb{N}_{>0}$, the inclusion

$\mathbf{Rat}_k \subset \mathbf{Rat}_{k+1}$ is strict. This means that we have defined an infinite hierarchy of classes of semigroups.

The situation for the class $\mathbf{CoRat}_k$ is not understood yet. Theorem 8.2.3 implies that the intersections $\mathbf{Rat}_k \cap \mathbf{CoRat}_1$ are not empty, but we do not have an example of a semigroup $S$ that has $k$-rational coword problem for some $k \in \mathbb{N}_{>0}$, but does not have $l$-rational coword problem for $l < k$.

**Open Question 10.2.2**

*For any given $k \in \mathbb{N}_{>0}$, is there a semigroup that has $k$-rational coword problem but does not have $l$-rational coword problem for any $l < k$?*

We have shown in Theorem 9.4.2 that the class **PRat** contains the closure of the class **Rat** under taking finite direct products. We have also shown in Theorems 9.4.1 and 9.4.4 which semigroups with polyrational word problems are isomorphic to direct products.

It will have to be established whether **PRat** contains semigroups that are not direct products of semigroups with $k$-rational word problems themselves.

**Open Question 10.2.3**

*Does there exist a semigroup with $k$-rational word problem that is not a direct product of $k$ semigroups with rational word problem?*

Should the answer to Open Question 9.4.1 be negative then semigroups with rational word problem are the only building blocks of semigroups with polyrational word problem. Should the answer be positive, semigroups with rational word problem and their direct products are still an important member of this class and therefore very interesting in this theory.

We know from Theorems 9.4.1 and 9.4.2 that **PRat** contains direct products of semigroups with rational word problem, and that finitely generated subsemigroups of direct products of semigroups are contained in **PRat**. We do not know whether these are all semigroups in **PRat**, and we know almost nothing about **CoPRat**.

**Open Question 10.2.4**

*Is* **CoPRat** *closed under direct product, finitely generated subsemigroups, or free product?*

**Open Question 10.2.5**

*Does* **CoPRat** *contain* **PRat***?*

Definition 3.5.2 allows for a complement operator. This means that a semigroup is in **ERat** if and only if it is in **CoERat**. This is the case with **Rec** too, and hence the class **ERat** is a natural step up from the class **Rec**.

Furthermore, to address a full hierarchy of rational phenomena, the full power of extended rational relations has to be considered and examined for expressive power, in particular with respect to word problems and coword problems of semigroups.

**Open Question 10.2.6**

*What are the properties of the semigroups contained in* **ERat***?*

A very interesting question in this context could be the following.

**Open Question 10.2.7**

*Is there a finitely generated group* G *that is a member of* **ERat**.

For all of the classes introduced above, the word problem and the coword problem are *efficiently* decidable, that is, it is decidable in time polynomial in the sum of the lengths of the two input strings. We have also shown that some interesting properties of semigroups in **Rat** are efficiently decidable.

## *10.3 Rational Monoids*

Sakarovitch introduced *rational monoids* as monoids where the normal forms for elements can be computed by a finite state transducer in [Sak87] and extended his theory together with Pelletier in [PS90].

An important open question is, whether the class of rational semigroups coincides with the class of semigroups with rational word problem. This problem is connected to the rational cross section problem, as stated in Open Question 3.7.2.

We define the notion of a rational semigroup as given by Sakarovitch.

**Definition 10.3.1**

*A semigroup $S$ is* rational *if there exists a finite generating set $A$ for $S$ and a rational map $A^+ \xrightarrow{\rho} A^+$ with $v\rho\pi_A = v\pi_A$ for all $v \in A^+$.*

We call $\rho$ the *normal form map*, because it computes for any input string $v \in A^+$ a unique normal form of the element $v\pi_A$ of $S$.

This enables us to define the *class of rational semigroups* as

$$\mathbf{RatSG} = [\, S \mid S \text{ is rational} \,].$$

We show that **RatSG** is contained in **Rat**.

**Theorem 10.3.2**

*Let $S$ be a finitely generated semigroup. If $S$ is rational, then $S$ has rational word problem.*

*Proof.* Let $A$ be a finite generating set for $S$, and let $A^+ \xrightarrow{\rho} A^+$ be the normal form map. The word problem $\iota_S(A)$ of $S$ with respect to the generating set $A$ is the composition

$$A^+ \xrightarrow{\rho} A^+ \xrightarrow{\rho^r} A^+,$$

which is rational by Theorem 3.7.4. □

By their very definition, rational monoids have a rational set of *unique* normal forms. Open Question 8.3.1 asks whether semigroups with rational word problem have a rational set of *unique* representatives. All of the properties shown to hold for semigroups with rational word problem in Section 8 also hold for rational semigroups, therefore we have not answered the following open question in previous chapters.

**Open Question 10.3.1**

*Let S be in* **Rat**, *is S in* **RatSG**? *In other words, is* **RatSG** = **Rat**?

In Sakarovitch and Pelletier in [PS90] construct a semigroup that fulfills Kleene's Theorem, but does not belong to **RatSG**. This semigroup is a potential example of a semigroup with rational word problem that is not rational. They also show that being rational is closed under a slightly more general notion of index than shown in Theorem 8.5.4 which would be worthwhile to examine in the case of rational word problem semigroups. There is not a lot of further research on this topic to be found to the knowledge of the author.

## *10.4 Linear Word Problem*

The definition of *linear word problem* requires a different *encoding* of the word problem, namely the one-tape encoding of the word problem as defined in Section 6.4. The encoding as a one-tape language is preferred by some researchers, and was proposed by Duncan and Gilman in [DG02], trying to extend hyperbolicity from groups to semigroups. We argue that it is not relevant for our purposes whether we take a one-tape or a two-tape encoding.

The definition of semigroups with linear word problem seems to be due to Richard Thomas. The author is only aware of unpublished results exchanged in private communication. In particular Thomas claims to have method to prove the equality of **RatSG** and **Rat** via showing the equality of **Lin** and **RatSG**. Note that proving that that semigroups with linear word problem are rational is one way of answering Open Question 10.3.1

We show that the classes of semigroups with linear one-tape word problem and semigroups with rational word problem coincide.

The following definition serves the purpose of terseness in this section. Linear languages are commonly defined as languages which are generated by a linear grammar, a concept we have not defined. It can be shown that the

definition given below is equivalent. A proof for this can be found in [Ber79, Chapter V].

**Definition 10.4.1**

*Let S be a semigroup. Then S has* linear word problem *if there is a rational relation* $A^+ \xrightarrow{\rho} A^+$ *such that*

$$_1\iota_S(A) = \left\{ v\#w^r \in (A \cup \#)^+ \mid w \in v\rho \right\}.$$

We define the *class of semigroups with linear word problem* by

$$\mathbf{Lin} = [\, S \mid S \text{ has linear word problem} \,].$$

We show that $\mathbf{Lin} = \mathbf{Rat}$.

**Theorem 10.4.2**

*A semigroup S has rational word problem if and only if S has linear word problem.*

*Proof.* This follows from the definition and [Ber79, Theorem V.6.5]. □

A different way of defining linear word problem is using *linear context free grammars*. We refer the reader to [Ber79] for a definition of context-free and linear context-free grammars.

For groups it is known from results in [MS83; MS85] that, if the word problem of a group is context-free, then it is deterministically context-free, and therefore the coword problem is deterministically context-free. Furthermore, it is known that there exist groups with context-free coword problem, but non context-free word problem. Among those groups are not only fairly straightforward groups such as the free commutative groups of rank greater than one, but also the Higman-Thompson group as was shown in [LS07].

Note that linear grammars cannot define the word problem of a group by Theorem 10.4.2 and Corollary 8.7.8. Restricting to linear grammars, does it hold that if a semigroup has linear word problem, then it has deterministically linear word problem and therefore it holds that if a semigroup has linear word problem, it also has linear coword problem. This is again Open Question 10.2.1.

## 10.5 One-Counter Semigroups

Continuing with the word problems of semigroups encoded as a one tape language, we look at *one-counter word problems*.

Holt, Owens and Thomas consider semigroups with one-counter word problem in [HOT08]. The definition is as follows

**Definition 10.5.1**

*Let* $S$ *be a semigroup. Then* $S$ *has* one-counter word problem *if there is a one-counter machine that decides* ${}_1\iota_S(A)$.

We define the *class of semigroups with one-counter word problem* as

$$\textbf{OneCounter} = [\, S \mid S \text{has one counter word problem}].$$

In terms of context-free grammars mentioned in the previous section, a one-counter language is generated by a context-free grammar that only has one non-terminal symbol. We also remind ourselves that one-counter machines were defined as a finite state device with a memory that is a counter. A counter can store a natural number and the machine can only increment and decrement the counter and test for it being zero. It is also clear from our definition that one-counter word problems are efficiently decidable.

It is shown in [HOT08] that semigroups with one-counter word problem have at most a linear *growth rate*. The *growth function* $\mathbb{N} \xrightarrow{g} \mathbb{N}$ of a semigroup $S$ finitely generated by a set $A$ is defined as

$$g : \mathbb{N} \longrightarrow \mathbb{N},\ n \mapsto \left| \bigcup_{i \in \underline{n}} \left( A^i \right) \pi_A \right|,$$

that is $g$ maps a natural number $n$ to the number of elements of $S$ represented by strings of length up to $n$.

Having linear growth rate means that $\mathbb{N} \xrightarrow{g} \mathbb{N}$ is in the same Landau equivalence class as the linear function

$$l : \mathbb{N} \longrightarrow \mathbb{N},\ n \mapsto n.$$

The authors of [HOT08] prove the following main theorems, which show that semigroups with one-counter word problem have a very restricted structure. First they show that semigroups with one-counter word problem have linear growth.

**Theorem 10.5.2**

*Let $S$ be a semigroup with one-counter word problem. Then $S$ has linear growth.*

In a second theorem they show that elements in a semigroup with one-counter word problem factor in a very special way.

**Theorem 10.5.3**

*Let $S$ be a semigroup with linear growth. Then there exists for some $k \in \mathbb{N}$ a collection $a_i, b_i, c_i$ of elements from $S^e$ for $i \in \underline{k}$ such that every $s \in S$ can be written as $a_i b_i^n c_i$ for some $i \in \underline{k}$ and $n \in \mathbb{N}$.*

To shed some light on the relationship between semigroups contained in the class **OneCounter** and the previously defined classes, we give give an example of a semigroup with one-counter word problem that does not have rational word problem, or even polyrational word problem, and a family of semigroups with rational word problem that does not contain any semigroup with one-counter word problem.

It holds that **Rec** $\subset$ **OneCounter** and **Rec** $\subset$ **Rat**, therefore the intersection between **OneCounter** and **Rat** is not empty. In addition, the free semigroup on one generator has rational word problem and one-counter word problem, so the intersection **OneCounter** $\cap$ **Rat** is nonempty and larger than **Rec**.

The group of integers has one-counter word problem by results from [HOT08], but by Corollary 8.7.8 it does not have rational word problem. We even showed in Lemma 9.3.2 that the integers are not contained in **PRat**.

Any free semigroup with more than one generator has rational word problem as shown in Lemma 8.2.1, but exponential growth rate, therefore does have one-counter word problem by Theorem 10.5.2. It follows that neither of

the inclusions **OneCounter** $\subset$ **Rat**, **Rat** $\subset$ **OneCounter** or **PRat** $\subset$ **OneCounter** hold.

It is not clear what other interesting properties semigroups in the class **OneCounter** have.

It is shown in [HOT08] that groups with one-counter word problem are virtually cyclic. The authors also consider intersections of one-counter languages, but only in connection with groups, and they show the following. Let $G$ be a group finitely generated by $A$, then the following are equivalent.

- The word problem $W_G(A)$ is an intersection of $k$ one-counter languages.
- The word problem $W_G(A)$ is an intersection of $k$ deterministic one-counter languages.
- $G$ is virtually abelian of free abelian rank at most $k$.

It is worth noting that this is a consequence of results about groups with context-free word problem.

## *10.6 Small Overlap Monoids*

In [Kam09a; Kam09b], Mark Kambites shows that semigroups that have a presentation that fulfills certain small overlap conditions introduced by Remmers in [Rem80] have deterministic rational word problem. Since the definition of the small overlap conditions is slightly involved and of no further relevance to us, we will not go into detail here, and refer to Remmers' Kambites' work for details. We will be concerned with small overlap conditions $C(k)$ for $k \in \{1, 2, 3, 4\}$ and denote the classes of semigroups that have a presentation of this type by $\mathbf{C}(k)$.

The following theorem, which is Theorem 2 in [Kam09b], shows that monoids which have a *finite* presentation that fulfills the small overlap condition $C(4)$

are rational in the sense of the definition in Section 10.3. *Deterministic* automata that decide the word problem are explicitly constructed from the given presentation. Therefore Open Question 8.8.4 is answered in the positive for monoids given by a presentation that fulfills $C(4)$.

**Theorem 10.6.1**

*Let* $M$ *be a monoid specified by the finite presentation* $\mathrm{mon}\langle A \mid R\rangle$*, which satisfies the small overlap condition* $C(4)$*. Then* $M$ *has rational word problem and there is a deterministic automaton that decides* $\iota_M(A)$*.*

It is known that monoids specified by a presentation which satisfies the condition $C(3)$ have decidable word problem. We note that the small overlap conditions are conditions placed on a specific presentation of a monoid, and the results are proven for finite presentations.

Theorem 10.6.1 shows that $\mathbf{C}(4) \subset \mathbf{Rat}$. The inclusion is proper since $P$, as defined in Section 5.6 is a semigroup in **Rat** which is not in $\mathbf{C}(4)$ since it is not finitely presentable.

**Open Question 10.6.1**

*What are the relationships between* $\mathbf{C}(k)$, **Rat**, **CoRat**, $\mathbf{Rat}_k$, $\mathbf{CoRat}_k$, **PRat**, **CoPRat**, *and* **ERat***?*

It should be noted that the work of Remmers is motivated in the combinatorial and geometric analysis of semigroups, in an attempt to carry the this very fruitful approach from group theory to semigroup theory. Many results in semigroup theory suggest that the geometric analysis of semigroups has not come anywhere close to the results for groups yet.

## *10.7 Word Hyperbolic Monoids*

In group theory the notion of a hyperbolic group is well-established. The notion of hyperbolicity of groups was introduced by Gromov [Gro83], and

has subsequently been studied intensively. The fact that there are many characterisations of hyperbolic groups from different areas of group theory is a strong indicator that being hyperbolic is a very robust property of groups. A group is hyperbolic if its Cayley graph is a hyperbolic space.

Many have tried to extend the concept of hyperbolicity to semigroups and monoids with varying degrees of success. Most importantly the notions of hyperbolicity which are equivalent for groups are in general not equivalent for semigroups, and some of the nice properties of hyperbolicity are not closed under even the most basic constructions of semigroup theory, such as adding a zero element.

The following definition of hyperbolicity for semigroups and monoids has been proposed by Duncan and Gilman in [DG02], following a result by Gilman showing that a group is word hyperbolic if and only if its multiplication table can be represented as a context-free one-tape language.

We say that a semigroup $S$, finitely generated by a set $A$, is *word hyperbolic*, if the restriction of $\pi_A$ to $A$ is injective and there is a rational subset $L \subseteq A^+$ such that the set

$$M = \{u\#_1 v\#_2 w^r \mid (uv)\pi_A = w\pi_A\} \cap L\#_1 L\#_2 L,$$

where $\#_1$ and $\#_2$ are symbols not in $A$, is decided by a pushdown automaton. We define the *class of word hyperbolic semigroups* as

$$\mathbf{WordHyp} = [\, S \mid S \text{ is word hyperbolic} \,].$$

Note that the injectivity of the restriction of $\pi_A$ to $A$ was not part of the original definition by Duncan and Gilman, but omission of this condition leads to non-isomorphic semigroups with the same set $M$. This result has now also appeared as part of Alan Cain's work on word hyperbolic semigroups [Cai13]. Injectivity of the restriction can be achieved by removing superflous generators from the generating set.

It follows by an application of [Ber79, Theorem V.6.5] that any semigroup with rational word problem is word hyperbolic, or, in the hierarchy **Rat** $\subset$ **WordHyp**.

**Theorem 10.7.1**

*Let S be a finitely generated semigroup in* **Rat**. *Then S is also in* **WordHyp**.

*Proof.* Let $S$ be a semigroup finitely generated by a set $A$ with rational word problem. We remove elements $a \in A$ such that there is $b \in A$ with $a\pi_A = b\pi_A$ to form a generating set $B$ of $S$. Then the restriction of $\pi_A$ to $B$ is injective, $\iota_S(B)$ is rational, and we choose $L = A^+$. Applying [Ber79, Theorem V.6.5] now yields that there is a linear context-free grammar that generates $M$ as defined above. □

In [DG02, Example 3.8] it is shown that the bicyclic monoid is word hyperbolic in the sense defined above. It follows from this and Theorem 8.2.4 that the class of word hyperbolic semigroups is bigger than the class of semigroups with rational word problem. The relationship between **WordHyp** and the classes **PRat** and **ERat** needs further investigation. We note that crucially context-free languages, and linear context-free languages, are not closed under intersection.

We note that there is an efficient decision procedure for membership in a context-free language which runs in $\mathcal{O}\left(|v|^3\right)$, the so called Cocke-Younger-Kasami algorithm, and therefore the word problem of word hyperbolic semigroups is efficiently decidable. Note however that there exist word hyperbolic semigroups that have undecidable Green's $\mathcal{R}$ relation.

The notion of word hyperbolicity and hyperbolicity of semigroups has enjoyed close attention, by many researchers. Just to name a few examples: Duncan and Gilman [DG02], Cain [Cai13], Fountain and Kambites, [FK02]. Despite this close attention, word hyperblicity does not seem to be a robust notion for semigroups, since characterisations of hyperbolicity that hold in

group theory do not extend to semigroup theory easily. To an extent this is related to the fact that the geometric study of semigroups necessitates the development of a theory of directed geometry. The theory of directed geometry is by far not as developed as the theory of classical geometry.

## *10.8 Asynchronously Automatic Semigroups*

As the final family for this chapter, we want to mention asynchronously automatic semigroups. The motivation for defining automatic structures comes from two sources: One source is the geometric study of groups by Epstein, Paterson, Cannon, Holt, Levy, and Thurston in [Eps+92a] who noticed that certain groups allowed for defining group multiplication by means of finite state automata. The second source comes from logic and computer science. In their paper [KN95] Khoussainov and Nerode instigate the study of automaton presented structures. They cite earlier attempts to present structures by recursive functions, and shift the focus towards the field of algebraic structures that can be presented by finite state automata. Their main reasons being the success of autmatic groups, and the feasibility of decision procedures.

We follow the definition of asynchronously automatic groups pioneered in [Eps+92b], and subsequently generalised to semigroups by Campbell, Robertson, Ruskuc and Thomas [Cam+01].

**Definition 10.8.1**

*A semigroup $S$ finitely generated by a set $A$ is* asynchronously automatic *if*

- *there is a rational subset $W$ of $A^+$ such that the restriction of $\pi_A$ to $W$ is surjective onto $S$,*
- *the relations $\iota_S(A) \cap \mu_W$ and $\rho_a \iota_S(A) \cap \mu_W$ for all $a \in A$ are rational relations.*

Remember that $\mu_X$ refers to the universal relation, and $\rho_a$ refers to the right

multiplication by $a$. Also note that $\iota_S(A)$ is not implied or required to be rational.

We also define the *class of semigroups asynchronously automatic semigroups* as

$$\textbf{AsyncAut} = [\, S \mid S \text{ is asynchronously automatic} \,]$$

We show that semigroups with rational word problem are asynchronously automatic.

**Theorem 10.8.2**

*Let $S$ be a semigroup finitely generated by $A$ with rational word problem. Then $S$ is asynchronously automatic.*

*Proof.* Let $S$ be a semigroup with rational word problem with respect to the generating set $A$. We choose $W = A^+$. Then $\iota_S(A) \cap \mu_{A^+}$ is rational by Lemma 3.4.4, because $\mu_{A^+}$ is recognisable. the relation $\rho_a$ is recognisable and therefore by Theorem 3.7.4 rational. Again, because $\mu_{A^+}$ is recognisable, the relations $\rho_a \iota_S(A) \cap \mu_{A^+}$ are rational for all $a \in A$. Therefore $S$ is asynchronously automatic. □

For the hierarchy this means that **Rat** $\subset$ **AsyncAut**, and this inclusion is proper as well since for example the group of integers is an asynchronously automatic monoid, but does not have rational word problem.

The class of asynchronously automatic semigroups has been studied extensively as a promising class of semigroups with nice computational properties. Cain showed in [Cai06] that even if one insists on the relations to be recognisable, cancellativity is undecidable for automatic semigroups, therefore cancellativity is undecidable for asynchronously automatic semigroups. There is a host of results on automatic semigroups starting from [Cam+01].

As a final note we illustrate how to decide the word problem of asynchronously automatic semigroups. Let $S$ be an asynchronously automatic semigroup finitely generated by $A$ and let $W$ be a rational subset of $A^+$ such that $W\pi_A = S$ and such that $\rho_a \iota_S(A) \cap \mu_W$ for $a \in A$ is rational.

To decide the word problem of $S$, the following problem has to be solved first: Given a string $v$ in $A^+$, determine a string $v' \in W$ with $v\pi_A = v'\pi_A$. To achieve this, assume $v = [\mathbf{a_1 a_2 \dots a_k}]$. One now has to successively compute a sequence $v = v_1, v_2, \dots, v_{|v|} = v'$ with $v_{i+1} \in v_i\,(\rho_{a_i}\iota_S(A))$. While each of these steps can be achieved by an algorithm similar to the one introduced in Lemma 4.4.2, the computed representatives can become very long which means that potentially we get an exponential time complexity for this step, and also $v'$ can be exponentially longer than $v$. This means that the complexity of the word problem is exponential, although this is not a lower bound, in fact it is unknown whether there is an efficient algorithm to solve the word problem even for automatic groups.

# 11

# *Conclusions*

We have seen how the notion of word problem as introduced by Dehn can naturally be extended from a notion in the theory of groups to a notion in the theory of semigroups. We further generalised the notion to arbitrary relations on semigroups in Chapter 6.

The following discussion in Chapter 7 revealed that we can generalise a theorem in group theory, Anisimov's Theorem, to a semigroup equivalent. More precisely we characterised the class of finite semigroups by the class **Rec** of semigroups with recognisable word problem.

Results presented in Chapter 8 then extended the class **Rec** of semigroups with recognisable word problem to the class **Rat** which contains infinite semigroups with efficiently decidable word problem. The class **Rat** does not contain any infinite groups. We also presented algebraic properties of semigroups in **Rat**.

The purpose of Chapter 9 was to present a natural extension of the class **Rat**. This extension has, among others, the property that it is closed under finite direct products, a property that the class **Rat** lacks.

Chapter 10 then connected the results obtained in Chapters 7, 8 and 9 with each other and related research and resulted in the creation of a hierarchy of semigroups, where the partial order is based on the complexity of the word problem and the coword problem.

Many open questions have been brought up. A list of open questions can be found in Appendix A. One of the most important question to answer Open Question 10.3.1. Finding a structural characterisation of semigroups with rational word problem seems imminent and we conjecture that it will rely on choosing a finite combination of types of $\mathcal{L}$-classes and $\mathcal{R}$-classes and how they interact, probably in a way similar to Rees-Matrix semigroups and Clifford semigroups.

Once semigroups with rational word problem are characterised, it will be possible to cover a class of semigroups with polyrational word problem, namely the finitely generated subsemigroups of direct products of semigroups with rational word problem. Here it is important to answer Open Question 9.4.1.

Having covered semigroups with polyrational word problem, a characterisation of semigroups with extended rational word problem has to be found. It is conceivable that all semigroups in this class behave nicely with respect to decidability and efficiency of a variety of properties, like the ones listed in 8.8. This is because for all semigroups in this class there is a finite state device that efficiently decides the word problem.

Moving on from semigroups with extended rational word problem we already suggested extensions of this class by giving the computing devices involved more computing power by adding memories. In particular one appealing approach is defining a hierarchy of more and more sophisticated memories.

*"I may not have gone where I intended to go, but I think I have ended up where I needed to be."*

*Svlad Cjelli*

*"TTFN, ta ta for now!"*

*Tigger*

# A

# *Open Questions*

# B

# *Automata*

In this section we give pictures of automata from Chapter 8 in black and white.

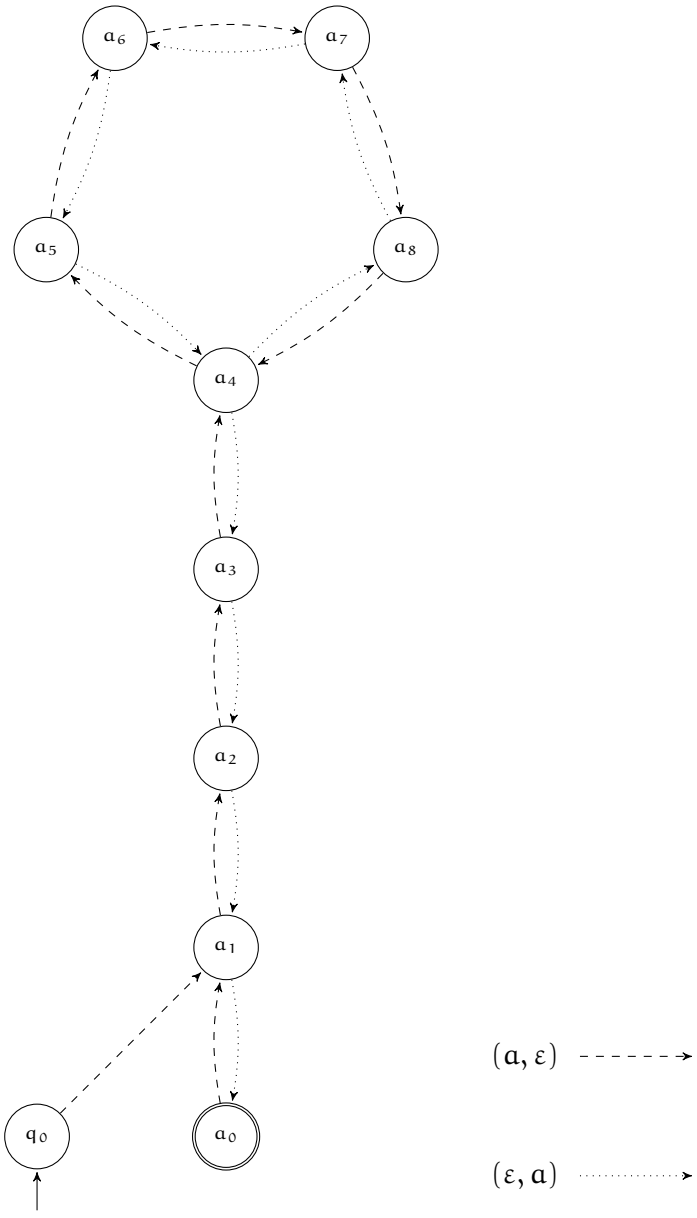



Figure B.1: Automaton for $\iota_S(A)$ where $S = \mathrm{sg}\langle a \mid a^4 = a^9 \rangle$ (no colours)

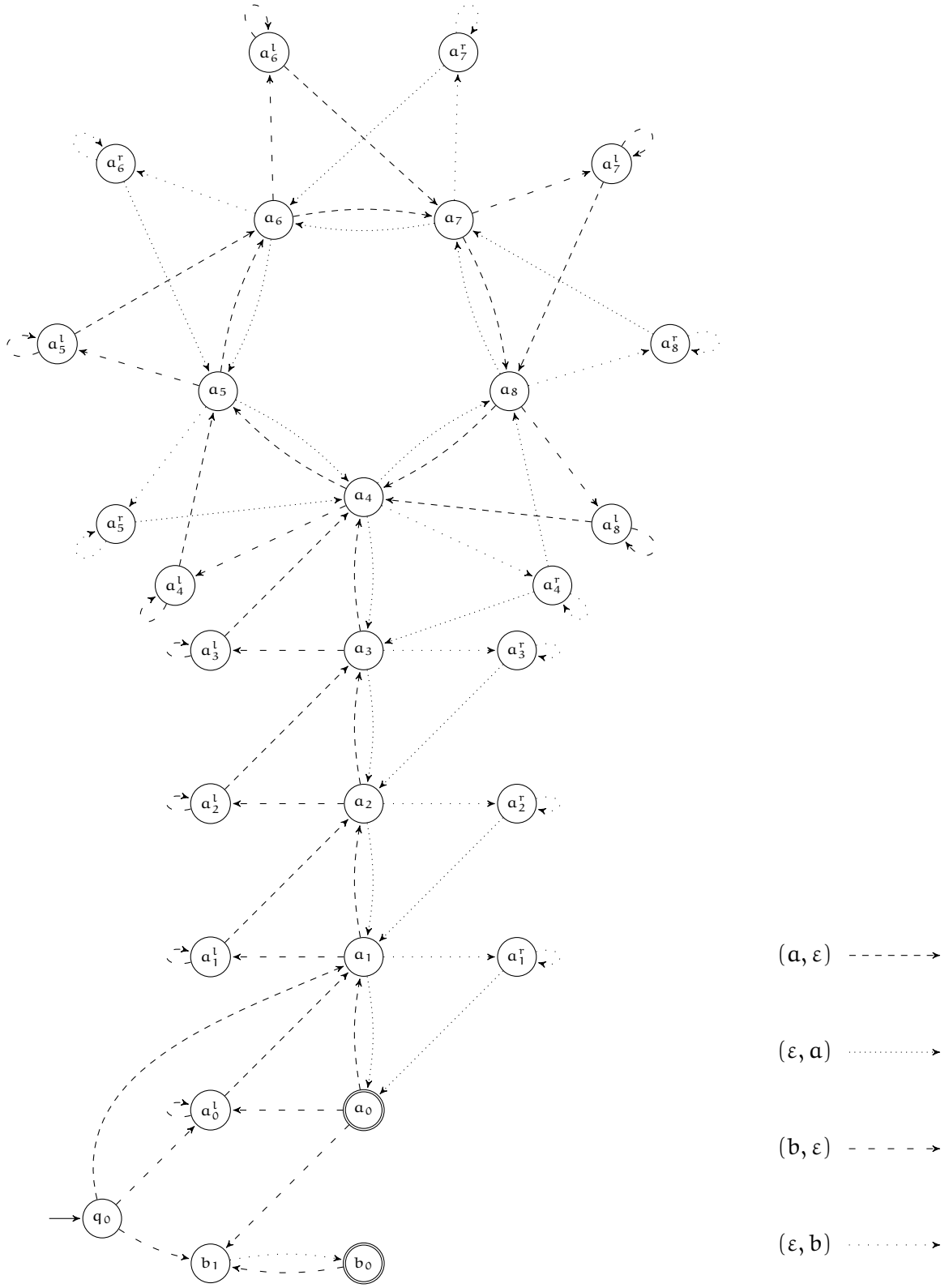



Figure B.2: Automaton for $\iota_{E(4,5)}(\{a, b\})$ (no colours)

# *Index*

# *Bibliography*


[Ani71] A. V. Anisimov. "On group languages". In: *Kibernetika* 4 (1971), pp. 18–24 (cit. on pp. x, 89).

[Bau93] Gilbert Baumslag. *Topics in combinatorial group theory*. Lectures in mathematics / ETH Zürich. Birkhäuser, 1993. ISBN: 978-3-7643-2921-1 (cit. on p. 77).

[Ber79] Jean Berstel. *Transductions and Context-Free Languages*. Teubner Studienbücher, Stuttgart, 1979 (cit. on pp. ix, 38, 51, 67, 163, 171, 177).

[BO93] Ronald V. Book and Friedrich Otto. *String-rewriting systems*. Texts and monographs in computer science. Springer, 1993, pp. I–VIII, 1–189. ISBN: 978-3-540-97965-4 (cit. on p. 142).

[Cai06] Alan J. Cain. "CANCELLATIVITY IS UNDECIDABLE FOR AUTOMATIC SEMIGROUPS". In: *Quarterly Journal of Mathematics* 57.3 (Sept. 15, 2006), pp. 285–295. ISSN: 0033-5606. DOI: 10.1093/qmath/hai023 (cit. on pp. 144, 179).

[Cai13] Alan J. Cain. "Decision problems for word-hyperbolic semigroups". In: (2013) (cit. on pp. 176, 177).

[Cam+01] Colin M. Campbell et al. "Automatic semigroups". In: *Theoretical Computer Science* 250.1–2 (2001), pp. 365–391. ISSN: 0304-3975. DOI: 10.1016/S0304-3975(99)00151-6 (cit. on pp. 178, 179).

[Cam+95] C. M. Campbell et al. "Reidemeister-Schreier type rewriting for semigroups". In: *Semigroup Forum* 51.1 (1995), pp. 47–62 (cit. on pp. 17, 118, 121).

[CM09] Alan J. Cain and Victor Maltcev. "Decision Problems for Finitely Presented and One-Relation Semigroups and Monoids". In: *IJAC* 19.6 (2009), pp. 747–770 (cit. on p. 143).

[CP61] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups*. Vol. 1. American Mathematical Society, 1961 (cit. on pp. 71, 125).

[CP67] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups*. Vol. 2. American Mathematical Society, 1967 (cit. on p. 30).

[Deh11] M. Dehn. "Über unendliche diskontinuierliche Gruppen". In: *Math. Ann.* 71.1 (1911), pp. 116–144. ISSN: 0025-5831. DOI: 10.1007/BF01456932 (cit. on p. 82).

[DG02] A. Duncan and Robert H Gilman. "Word hyperbolic semigroups". In: *Math. Proc. Cambridge Philos. Soc.* 136 (2002), pp. 513–524 (cit. on pp. 170, 176, 177).

[Eil76a] Samuel Eilenberg. *Automata, Languages, and Machines*. Vol. A. Orlando, FL, USA: Academic Press, Inc., 1976. ISBN: 0122340027 (cit. on pp. ix, xii, 3, 4, 50–52, 57, 161).

[Eil76b] Samuel Eilenberg. *Automata, Languages, and Machines*. Vol. B. Orlando, FL, USA: Academic Press, Inc., 1976. ISBN: 0122340027 (cit. on p. 165).

[Eil98] Samuel Eilenberg. *Automata, Languages, and Machines*. Vol. C. 1998 (cit. on p. 162).

[EM65] C. C. Elgot and J. E. Mezei. "On relations defined by generalized finite automata". In: *IBM J. Res. Dev.* 9.1 (Jan. 1965), pp. 47–68. ISSN: 0018-8646. DOI: 10.1147/rd.91.0047 (cit. on p. 48).

[Eps+92a] David B. A. Epstein et al. *Word Processing in Groups*. Natick, MA, USA: A. K. Peters, Ltd., 1992. ISBN: 0867202440 (cit. on pp. 144, 178).

[Eps+92b] David B. A. Epstein et al. *Word Processing in Groups*. Natick, MA, USA: A. K. Peters, Ltd., 1992. ISBN: 0867202440 (cit. on p. 178).

[FK02] John Fountain and Mark Kambites. "Hyperbolic Groups and Completely Simple Semigroups". In: *Workshop on Semigroups and Languages* (2002) (cit. on p. 177).

[G S58] G. S. Tseitin. "An associative calculus with an insoluble problem of equivalence". In: *Trudy Mat. Inst. Steklov.* 52 (1958), pp. 172–189 (cit. on p. 79).

[Göd31] Kurt Gödel. "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme". In: *Monatshefte für Mathematik und Physik* 38.1 (1931), pp. 173–198 (cit. on p. 64).

[GR08] R. Gray and N. Ruškuc. "Green index and finiteness conditions for semigroups". In: *Journal of Algebra* 320.8 (2008), pp. 3145–3164. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2008.07.008 (cit. on pp. 28, 29, 123).

[Gre51] J. A. Green. "On the structure of semigroups". In: *Annals of Mathematics* (second series) 54(1) (1951), 163–172 (cit. on p. 28).

[Gro83] Mikhael Gromov. "Infinite Groups as Infinite Objects". In: *Proceedings of the International Congress of Mathematicians, Warzawa* (1983), pp. 385–392 (cit. on p. 175).

[Hol+05] Derek Holt et al. "Groups with context-free co-word problem". In: *Journal of the London Mathematical Society* 71.3 (2005), pp. 643–657 (cit. on p. 83).

[HOT08] D.F. Holt, M.D. Owens, and R.M. Thomas. "Groups And Semigroups With A One-Counter Word Problem". In: *Journal of the Australian Mathematical Society* 85 (2008), pp. 197–209 (cit. on pp. 172–174).

[How95] John M. Howie. *Fundamentals of Semigroup Theory*. Oxford Science Publications, 1995 (cit. on pp. viii, 137, 139).

[Joh83] John Howard Johnson. "Formal models for string similarity". AAI0553315. PhD thesis. University of Waterloo, School of Computer Science, 1983 (cit. on p. 52).

[Joh85] J. Howard Johnson. "Do Rational Equivalence Relations have Regular Cross-Sections?" In: *Proceedings of the 12th Colloquium on Automata, Languages and Programming*. London, UK: Springer-Verlag, 1985, pp. 300–309. ISBN: 3-540-15650-X (cit. on p. 52).

[Kam09a] Mark Kambites. "Small overlap monoids I: The word problem". In: *Journal of Algebra* 321.8 (2009). Computational Algebra, pp. 2187–2205. ISSN: 0021-8693. DOI: DOI:10.1016/j.jalgebra.2008.09.038 (cit. on pp. 145, 174).

[Kam09b] Mark Kambites. "Small overlap monoids II: Automatic structures and normal forms". In: *Journal of Algebra* 321.8 (2009). Computational Algebra, pp. 2302–2316. ISSN: 0021-8693. DOI: DOI:10.1016/j.jalgebra.2008.12.028 (cit. on pp. 145, 174).

[Kle56] S. C. Kleene. "Representation of Events in Nerve Nets and Finite Automata". In: *Automata Studies* (1956) (cit. on p. 43).

[KN95] Bakhadyr Khoussainov and Anil Nerode. "Automatic Presentations of Structures". In: *Lecture Notes in Computer Science* 960 (1995), pp. 367–392 (cit. on p. 178).

[KW57] R. J. Koch and A. D. Wallace. "Stability in semigroups". In: (1957) (cit. on p. 30).

[Lal79] G. Lallement. *Semigroups and combinatorial applications*. Pure and applied mathematics. Wiley, 1979. ISBN: 9780471043799 (cit. on p. 30).

[LS07] J. Lehnert and P. Schweitzer. "The Co-Word Problem for the Higman-Thompson Group is Context-Free". In: *Bull. London Math. Soc.* 39 (2007), pp. 235–241 (cit. on pp. 83, 171).

[Mat95] Yuri Matiyasevich. "Word Problem for Thue Systems with a Few Relations". In: *Term Rewriting, French Spring School of Theoretical Computer Science, Advanced Course*. London, UK, UK: Springer-Verlag, 1995, pp. 39–53. ISBN: 3-540-59340-3 (cit. on p. 79).

[McK64] J. D. McKnight. "Kleene quotient theorems." In: *Pacific J. Math.* 14 (1964), pp. 1343–1352 (cit. on p. 43).

[MS72] A. R. Meyer and L. J. Stockmeyer. "The equivalence problem for regular expressions with squaring requires exponential space". In: *Proceedings of the 13th Annual Symposium on Switching and Automata Theory (swat 1972)*. SWAT '72. Washington, DC, USA: IEEE Computer Society, 1972, pp. 125–129. DOI: 10.1109/SWAT.1972.29 (cit. on p. 161).

[MS83] David E. Muller and Paul E. Schupp. "Groups, the Theory of Ends, and Context-Free Languages". In: *J. Comput. Syst. Sci.* (1983), pp. 295–310 (cit. on pp. 84, 171).

[MS85] David E. Muller and Paul E. Schupp. "The Theory of Ends, Pushdown Automata, and Second-Order Logic". In: *Theor. Comput. Sci.* (1985), pp. 51–75 (cit. on pp. 84, 171).

[Niv68] M. Nivat. "Transductions des languages de Chomsky". In: *Ann. Inst. Fourier (Grenoble)* 18 (1968), pp. 339–455 (cit. on p. 50).

[NPR11] Max Neunhöffer, Markus Pfeiffer, and Nik Ruskuc. "Deciding Word Problems of Semigroups using Finite State Automata". In: *Theoretical Computer Science* submitted (2011) (cit. on pp. xi, 97).

[OCa69] L. O'Carroll. In: *Transactions of the American Mathematical Society* 146 (1969), pp. 377–386 (cit. on p. 30).

[Ogd68] William Ogden. "A helpful result for proving inherent ambiguity". In: 2 (3 1968), pp. 191–194 (cit. on p. 38).

[Pet62] Carl Adam Petri. "Kommunikation mit Automaten". PhD thesis. University of Bonn, School of Mathematics, 1962 (cit. on p. 162).

[Pet66] Carl Adam Petri. "Communication with Automata". In: *New York Griffiss AFB* (1966) (cit. on p. 162).

[PS90] Maryse Pelletier and Jacques Sakarovitch. "Easy Multiplications II. Extensions of Rational Semigroups". In: *Inf. Comput.* 88.1 (1990), pp. 18–59 (cit. on pp. 116, 168, 170).

[Rem80] J. H. Remmers. "On the geometry of semigroup presentations". In: *Adv. in Math* 36 (1980), pp. 283–296 (cit. on p. 174).

[RRW98] E.F. Robertson, N. Ruskuc, and J. Wiegold. "Generators And Relations Of Direct Products Of Semigroups". In: *Transactions of the American Mathematical Society* 350.7 (1998), pp. 2665–2685 (cit. on p. 126).

[Rus95] Nik Ruskuc. "Semigroup Presentations". PhD thesis. University of St Andrews, School of Mathematics, 1995 (cit. on p. 77).

[Sak87] Jacques Sakarovitch. "Easy Multiplications. I. The Realm of Kleene's Theorem". In: *Inf. Comput.* 74.3 (1987), pp. 173–197 (cit. on pp. 138, 168).

[Sch57] Marcel-Paul Schützenberger. "D-representation des demi-groupes". In: *Comptes-Rendus de l'Académie des Sciences* 244 (1957), pp. 1994–1996 (cit. on pp. 29, 30).

[Tur36] A. M. Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem". In: *Proceedings of the London Mathematical Society* 42 (1936). This is the paper that introduced what is now called the *Universal Turing Machine*., pp. 230–265. ISSN: 0024-6115 (cit. on p. 64).

[Wal63] A. D. Wallace. "Relative ideals in semigroups. II - the relations of green." In: *Acta Mathematica Academiae Scientiarum Hungaricae* 14(1-2) (1963), pp. 137–148 (cit. on p. 28).