Local Divisors in Formal Languages

Von der Fakultät für Informatik, Elektrotechnik und Informationstechnik der Universität Stuttgart zur Erlangung der Würde eines Doktors der Naturwissenschaften (Dr. rer. nat.) genehmigte Abhandlung

Vorgelegt von
Tobias Walter
aus Bietigheim-Bissingen

Hauptberichter: Prof. Dr. Volker Diekert

Mitberichter: Prof. Dr. Klaus-Jörn Lange

Tag der mündlichen Prüfung: 30.11.2016

Institut für Formale Methoden der Informatik
2016

Contents

Abstract

Regular languages are exactly the class of recognizable subsets of the free monoid. In particular, the syntactic monoid of a regular language is finite. This is the starting point of algebraic language theory. In this thesis, the algebraic connection between regular languages and monoids is studied using a certain monoid construction – local divisors.

Using the local divisor construction, we give a Rees decomposition of a monoid into smaller parts – the monoid is a Rees extension of a submonoid and a local divisor. Iterating this concept gives an iterated Rees decomposition of a monoid into groups appearing in the monoid. This decomposition is similar to the synthesis theorem of Rhodes and Allen. In particular, the Rees decomposition shows that closure of a variety $\mathbf{V}$ of finite monoids under Rees extensions is the variety $\overline{\mathbf{H}}$ induced by the groups $\mathbf{H}$ contained in $\mathbf{V}$.

Due to the connection between $\overline{\mathbf{H}}$ and local divisors, we turn our attention to a language description of $\overline{\mathbf{H}}$. The language description is a continuation of classical work of Schützenberger. He studied prefix codes of bounded synchronization delay and used those codes to give a language description of $\overline{\mathbf{H}}$ in the case that the variety $\mathbf{H}$ of groups contains only abelian groups. We use the local divisor approach to generalize Schützenberger's language description of $\overline{\mathbf{H}}$ for all varieties $\mathbf{H}$ of finite groups. The main ingredient of this generalization is the concept of group-controlled stars. The group-controlled star is an operation on prefix codes of bounded synchronization delay which generalizes the usual Kleene star. The language class $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ is the smallest class which contains all finite languages and is closed under union, concatenation product and group-controlled stars for groups in $\mathbf{H}$. We show that $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ is the language class corresponding to $\overline{\mathbf{H}}$. As a by-product of the proof we give another language characterization of $\overline{\mathbf{H}}$: the localizable closure $\mathrm{Loc}_{\mathbf{H}}(A^\infty)$ of $\mathbf{H}$.

In the last part of this thesis, we deal with Church-Rosser congruential languages (CRCL). A language is Church-Rosser congruential if it is a finite union of congruence classes modulo a finite, confluent and length-reducing semi-Thue system. This yields a linear time algorithm for the membership problem of a fixed language in CRCL. A natural question, which was open for over 25 years, is whether all regular languages are in CRCL. We give an affirmative answer to this question by proving a stronger statement: for every regular language L and for every weight, there exists a finite, confluent and weight-reducing semi-Thue system S such that A^*/S is finite and recognizes L. Lifting the result from the special case of length-reducing to weight-reducing allows the use of local divisors.

Next, we focus on Parikh-reducing Church-Rosser systems for regular languages. Instead of constructing a semi-Thue system for a fixed weight, a Parikh-reducing Church-

Rosser system is weight-reducing for every weight. We construct such systems for all languages in $\overline{\mathbf{Ab}}$, that is, for all languages such that the groups in the syntactic monoid are abelian. Additionally, small changes in the proof of this result also yield that for all languages L over a two letter alphabet there exists a Parikh-reducing Church-Rosser system S of finite index such that L is recognized by A^*/S.

Lastly, we deal with the size of the monoid A^*/S for the constructed systems S. We show that in the group case this size has an exponential lower bound and a triple exponential upper bound. The key observation is that one can restrict the alphabet used in the inductive construction. Using the same observation, one can lower the upper bound in the general monoid case from a non-primitive function without this optimization to a quadruple exponential upper bound.

Previously published material. This thesis is based on two papers: [DKRW15] (conference version: [DKRW12]) and [DW16].

The work of [DW16] is incorporated into Chapter 3 and Chapter 4. Apart from the results of [DW16], Chapter 3 contains a new upper bound for the size of a Rees decomposition. In Chapter 4 there is an additional language characterization of $\overline{\mathbf{H}}$ with the introduction of localizable closures.

The main theorem of Chapter 5 – all regular languages are Church-Rosser congruential – is taken from [DKRW15]. This includes in particular the presentation of the material in Sections 5.2, 5.3, 5.4 and 5.6. The results of Chapter 5 which are not in [DKRW15] include the study of groups in the Church-Rosser representation, the treatise of Parikh-reducing systems and the results about the complexity of Church-Rosser representations.

Publications not included in this thesis.

- Volker Diekert and Tobias Walter. Asymptotic approximation for the quotient complexities of atoms. *Acta Cybernetica*, 22:349–357, 2015.
- Manfred Kufleitner and Tobias Walter. One quantifier alternation in first-order logic with modular predicates. *RAIRO-Theor. Inf. Appl.*, 49(1):1–22, 2015.
- Manfred Kufleitner and Tobias Walter. Level two of the quantifier alternation hierarchy over infinite words. In *CSR*, volume 9691 of *Lecture Notes in Computer Science*, pages 223–236. Springer, 2016. (invited to a special issue of Theory of Computing Systems)

Zusammenfassung

Die Klasse der regulären Sprachen entspricht genau den erkennbaren Sprachen über dem freien Monoid. Äquivalent dazu ist die Klasse der Sprachen, deren syntaktisches Monoid endlich ist. Dies ist der Ausgangspunkt der algebraischen Sprachtheorie. In dieser Arbeit wird dieser algebraische Zusammenhang zwischen regulären Sprachen und Monoiden mit Hilfe einer Monoid-Konstruktion untersucht: den lokalen Divisoren.

Zunächst werden lokale Divisoren benutzt um ein Monoid in kleinere Teile zu zerlegen. Die dabei verwendete Konstruktion ist ähnlich zur Rees-Matrix-Halbgruppe und liefert eine Zerlegung eines Monoids als sogenannte Rees-Erweiterung eines echten Untermonoids und eines lokalen Divisors. Wiederholtes Anwenden dieses Sachverhalts führt dann auf eine Rees-Zerlegung, bei der die grundlegenden Bausteine Gruppen sind, die im ursprünglichen Monoid vorkommen. Diese Zerlegung ist ähnlich zum Synthese-Theorem von Rhodes und Allen. Insbesondere liefert dies, dass der Abschluss einer Varietät $\mathbf{V}$ unter Rees-Erweiterungen die Varietät $\overline{\mathbf{H}}$ ist, wobei $\mathbf{H}$ die Varietät der endlichen Gruppen ist, die in $\mathbf{V}$ vorkommen.

Aufgrund des Zusammenhangs zwischen lokalen Divisoren und den Varietäten $\overline{\mathbf{H}}$, werden als nächstes Sprachbeschreibungen der Varietäten $\overline{\mathbf{H}}$ untersucht. Dabei wird die Arbeit von Schützenberger über Sprachcharakterisierungen mit Hilfe von Präfix-Codes mit beschränkter Synchronisierungsverzögerung (englisch: *bounded synchronization delay*) fortgesetzt. Schützenberger benutzte diese Codes um die Varietäten der Form $\overline{\mathbf{H}}$ zu beschreiben, wobei $\mathbf{H}$ eine Varietät von endlichen abelschen Gruppen ist. Wir verallgemeinern seine Beschreibung um $\overline{\mathbf{H}}$ für alle Varietäten $\mathbf{H}$ von endlichen Gruppen zu charakterisieren. Das Hauptkonzept dieser Verallgemeinerung sind gruppen-kontrollierte Sterne. Dabei sind gruppen-kontrollierte Sterne Sprachoperationen, die auf Präfix-Codes mit beschränkter Synchronisierungsverzögerung aufbauen und als Spezialfall für die triviale Gruppe den Kleene-Stern liefern.

Die Sprachklasse $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ ist die kleinste Klasse von Sprachen, die alle endlichen Sprachen enthält und abgeschlossen ist unter Vereinigung, Konkatenationsprodukt und gruppen-kontrollierten Sternen, wobei die Gruppen aus $\mathbf{H}$ sind. Wir zeigen, dass $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ die zu $\overline{\mathbf{H}}$ zugehörige Sprachklasse ist. Als Nebenprodukt des Beweises dieser Sprachcharakterisierung geben wir eine weitere Charakterisierung von $\overline{\mathbf{H}}$ an: der lokale Abschluss $\mathrm{Loc}_{\mathbf{H}}(A^\infty)$ von $\mathbf{H}$.

Der letzte Abschnitt dieser Arbeit handelt von der Sprachklasse CRCL (*Church-Rosser congruential languages*). Eine Sprache ist in CRCL, falls sie eine endliche Vereinigung von Kongruenzklassen eines endlichen, konfluenten und längenreduzierenden Ersetzungssystems ist. Dies liefert direkt einen Linearzeit-Algorithmus für das Wortproblem von Sprachen aus CRCL. Eine 25 Jahre lang offene Fragestellung war, ob alle regulären Sprachen in CRCL enthalten sind. Wir beantworten diese Frage pos-

itiv, indem wir eine stärkere Aussage beweisen: Für alle regulären Sprachen L und alle Gewichtsfunktionen gibt es ein endliches, konfluentes und gewichtsreduzierendes Ersetzungssystem S, für das A^*/S endlich ist und L erkennt. Durch das Erweitern der Aussage auf alle Gewichtsfunktionen erlaubt dies die Benutzung von lokalen Divisoren.

Als nächstes werden Parikh-reduzierende Church-Rosser-Ersetzungssysteme betrachtet. Diese repräsentieren eine Vertauschung der Quantorenreihenfolge: Ein Parikh-reduzierendes Ersetzungssystem ist gewichtsreduzierend für alle Gewichtsfunktionen. Wir konstruieren solche Systeme für alle Sprachen in der Varietät $\overline{\mathbf{Ab}}$, d.h. für alle Sprachen, in denen die im syntaktischem Monoid vorkommenden Gruppen abelsch sind. Zusätzlich liefert eine Abwandlung dieses Beweises dasselbe Resultat für alle regulären Sprachen über einem zwei-elementigem Alphabet.

Als letztes beschäftigt sich die Arbeit mit Abschätzungen für die Größe von A^*/S für die zuvor konstruierten Systeme S. Im Fall von Gruppensprachen ist die Größe von unten durch eine Exponentialfunktion und von oben durch eine dreifache Exponentialfunktion beschränkt. Für die obere Schranke wird dabei eine Beobachtung benutzt, wie man das Alphabet in der Induktion beschränken kann. Mit Hilfe dieser Beobachtung ist es ebenfalls möglich die obere Schranke im Monoid-Fall von einer nicht primitiven Funktion auf eine vierfach exponentielle Funktion zu reduzieren.

Chapter 1

Introduction

The local divisor is a monoid construction for finite monoids. In algebraic language theory the local divisor construction appeared first in [DG06] where local future temporal logic is studied. Originally, local divisors have been defined by Meyberg in the context of associative algebras [Mey72]. The construction of a local divisor is rather simple. For a monoid M and $c \in M$, the local divisor is given by $M_c = cM \cap Mc$. The multiplication on M_c is given by $xc \circ cy = xcy$. If c is not a unit, the local divisor M_c is strictly smaller than M. Therefore, the local divisor construction yields an induction mechanism. In the general setting, the induction is on homomorphisms $\varphi : A^* \to M$ which have two parameters: the size of the monoid and the size of the alphabet. The induction step has two parts: the baby-step, that is, the reduction of the size of the alphabet and the giant-step, that is, the reduction of the size of the monoid. In the latter case, the reduction of the size of monoids usually produces a much larger alphabet. The induction scheme terminates as soon as there is no choice for a non-unit element $c \in M$. This is the case if M is a group. Therefore, the group case has to be handled separately when using the local divisor technique. In particular, the local divisor technique is most useful for aperiodic monoids. Using this technique, Kufleitner gave a short "one-page" proof of Schützenberger's celebrated result SF = **A**: star-free languages are exactly the languages recognized by aperiodic monoids [Kuf14]. Another characterization for star-free languages by Schützenberger is replacing the closure under complementation with closure under star operation restricted to prefix codes of bounded synchronization delay [Sch75]. This characterization has been lifted to infinite words with the help of local divisors [DK15a]. Further, it has been proved that all star-free languages are Church-Rosser congruential [DKW12]. A result outside of aperiodic monoids is the simplified proof of the Krohn-Rhodes decomposition using local divisors, see [DKS12]. An overview over all these proofs is given in the survey paper [DK15b].

Outline. In Chapter 2 we introduce notation and basic results used in this thesis. First, we develop the algebra – we use monoids – used in algebraic language theory. Then we introduce formal languages and present their relation to monoids. This is further deepened by the introduction of varieties. Whenever possible, we present these basics for finite and infinite words. We also familiarize the reader with rewriting systems and combinatorics over words – a useful tool for the study of rewriting systems.

In Chapter 3 we study Rees extensions. A *Rees extension* is a monoid construction

which is similar to Rees matrix semigroups. Rees extensions have been introduced in [DKW12]. We give a novel and surprisingly simple decomposition for monoids which are no groups. Such monoids M allow a decomposition into a proper submonoid and a proper local divisor M_c. This yields a *Rees decomposition tree* whereas the leaves of the tree are groups contained in M. The Rees decomposition tree can be interpreted as a trace log of the baby-step-giant-step induction scheme. Let $\mathbf{H}$ be a variety of finite groups and $\overline{\mathbf{H}}$ be the variety of all finite monoids such that all subgroups are in $\mathbf{H}$. Rees extensions do not introduce new groups. Therefore, the class of monoids $\overline{\mathbf{H}}$ is exactly the class of monoids which have a Rees decomposition tree where all leaves are in $\mathbf{H}$. This indicates that the local divisor induction scheme is very fruitful for statements which hold exactly for a variety of the form $\overline{\mathbf{H}}$. In fact, the local divisor proofs discussed above either hold for aperiodic monoids or for all finite monoids; two examples of varieties of the form $\overline{\mathbf{H}}$. We will see an example of an intermediate statement in Chapter 5. There, $\mathbf{H}$ is the class of all finite abelian groups. Furthermore, Chapter 3 provides an upper bound for the size of a Rees decomposition tree and apply the decomposition in order to answer a question of Almeida and Klíma.

Having observed the connection between the local divisor induction scheme and the variety $\overline{\mathbf{H}}$, we study the language class corresponding to $\overline{\mathbf{H}}$ in Chapter 4. Our characterization of the languages recognized by some monoid in $\overline{\mathbf{H}}$ is based on codes with bounded synchronization delay. This kind of study has been initiated by Schützenberger for aperiodic monoids [Sch75]. We generalize the results of Schützenberger using so-called *group-controlled stars* and *group-controlled ω-powers*, in the case of infinite words. Additionally, we show that this class of languages is equivalent to the *localizable closure* of $\mathbf{H}$, a language class which is obtained by formalizing the operations needed in the usual local divisor approach.

In Chapter 5, we study a concrete example for the local divisor technique in detail. Namely, we deal with Church-Rosser congruential languages (CRCL). Languages in CRCL are defined in terms of a finite confluent length-reducing rewriting system. This directly yields a linear algorithm for the word problem. Naturally, one is interested in whether this language class is robust, that is, if all regular languages are Church-Rosser congruential. We solve this question – which has been open for over 25 years – affirmatively. It turns out that the construction of the Church-Rosser system yields a monoid which is a Rees extension of monoids arising from "smaller" Church-Rosser systems. Having solved this question positively, we examine a stronger variant of Church-Rosser congruential languages: languages which are saturated by a Parikh-reducing Church-Rosser system. We show that all regular languages in $\overline{\mathbf{Ab}}$ and all regular languages over a two-letter alphabet have such a Parikh-reducing system. Furthermore, we study the size of the monoids presented by such systems and give lower and upper bounds for this size.

We conclude the thesis in Chapter 6 by listing our contributions and stating open problems which arose from the previous chapters.

Chapter 2

Preliminaries

In this chapter we provide the notation and notions used in this thesis. The presented material is not original, in fact, most of it can be found in any introductory textbook on the topic, see e.g. [Eil76, Pin86, HU79, BO93]. Therefore, we mostly do not provide further citations of this basic material. We assume the reader to be familiar with basic concepts in computer science, e.g., Big O notation.

Note that the definition of recognizability in Subsection 2.2.2 differs from the classical definition. This definition, as well as the treatise of our variant of Schützenberger products in 2.3, is taken from [DW16].

Also noteworthy is Subsection 2.1.4, in which local divisors are defined.

2.1 Algebra

2.1.1 Monoids and Homomorphisms

The main algebraic concepts used in this thesis are monoids and, as a special kind of monoids, groups. Apart from the free monoid, we mostly work on finite monoids. The identity element of a monoid M is denoted by 1_M and the operation of M is denoted by $\cdot$, unless stated otherwise. If the monoid M is clear by the context, we write 1 for 1_M. We usually omit the operation $\cdot$, i.e., for elements $n, m \in M$ we write nm instead of $n \cdot m$. An element $e \in M$ is an *idempotent* if $e^2 = e$. A *subsemigroup* of M is a subset of M which is closed under the operation, whereas a *submonoid* of M is a subsemigroup which contains the identity element of M. We write $N \leq M$ if$N$ is a submonoid of M. A subsemigroup of M which is a group is called a *subgroup* of M. We will also say that it is a group in M. Note that a group G in M must not contain the identity element of M, but the identity element of G can be another idempotent $e \neq 1$ of M. Since groups have a unique idempotent, this notion coincides with the usual notion of a subgroup if M is also a group.

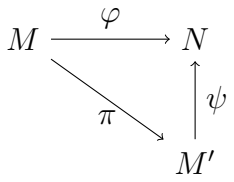
Let M and N be monoids. A *homomorphism* is a mapping $\varphi : M \to N$ such that $\varphi(1) = 1$ and $\varphi(nm) = \varphi(n)\varphi(m)$ for all $n, m \in M$. A bijective homomorphism is called *isomorphism*. We say that M and N are isomorphic, denoted by $M \simeq N$, if there exists an isomorphism $\varphi : M \to N$. The image $\varphi(M) = \{\varphi(m) \mid m \in M\}$ is a submonoid of N.

A *congruence* $\equiv$ on a monoid M is an equivalence relation on M such that $n \equiv n'$

and $m \equiv m'$ implies $nm \equiv n'm'$ for all $n, n', m, m' \in M$. One can check that the set of congruence classes $\{[m]_\equiv \mid m \in M\} = M/\equiv$ forms a new monoid equipped with the operation $[n]_\equiv \cdot [m]_\equiv = [nm]_\equiv$. The natural projection $\pi : M \to M/\equiv$ given by $\pi(m) = [m]_\equiv$ is a homomorphism. The *kernel* $\ker \varphi = \{(n, m) \in M \times M \mid \varphi(n) = \varphi(m)\}$ of a homomorphism φ is a congruence. In particular, every congruence is the kernel of some homomorphism.

The connection between kernels and homomorphisms is the *homomorphism theorem*.

Theorem 2.1. *Let $\varphi : M \to N$ and $\pi : M \to M'$ be homomorphisms such that $\ker \pi \subseteq \ker \varphi$ and π is surjective. Then there is a unique homomorphism $\psi : M' \to N$ such that $\varphi = \psi \circ \pi$, that is, the following diagram commutes:*



The homomorphism ψ is injective if and only if $\ker \pi = \ker \varphi$. In particular, for the projection $\pi : M \to M/\ker \varphi$, we obtain $\varphi(M) \simeq M/\ker \varphi$.

Let G, H be groups and $\varphi : G \to H$ be a homomorphism. Then $(g, g') \in \ker \varphi$ if and only if $\varphi(g^{-1}g') = 1$. For this reason in the case of groups, the subgroup $\varphi^{-1}(1)$ of G is called the kernel of φ.

Let $\varphi : M \to N$ be a surjective homomorphism, then N is called a *quotient* (due to the homomorphism theorem above) or *homomorphic image* of M. The monoid N is a *divisor* of a monoid M, if N is a homomorphic image of a submonoid[1] of M. We write $N \preceq M$ if N is a divisor of M. Note that every group in M is a divisor of M[2].

2.1.2 Group theory

Let G be a finite group and let $g \in G$. Since G is finite, there exist $i < j \in \mathbb{N}$ such that $g^i = g^j$. In particular, $g^{j-i} = 1$. The smallest number $0 < n \in \mathbb{N}$ such that $g^n = 1$ is called the *order* of g. The order is denoted by $\mathrm{ord}(g)$. The *exponent* of a group G is the smallest number $0 < n \in \mathbb{N}$ such that $g^n = 1$ for all $g \in G$. The exponent of G is denoted by $\exp(G)$. Since $g^{\exp(G)} = g^{\mathrm{ord}(g)} = 1$, the order of g must be a divisor of the exponent of G. In fact, the exponent of G is the least common divisor of the orders of all elements in G.

The set $\langle g \rangle = \{g^i \mid i \in \mathbb{N}\}$ forms a subgroup of G and is called the subgroup generated by g. A group G is called *cyclic* if it is generated by some element. The *order* $|G|$ of a group G is the number of elements in G. Obviously, the order of $\langle g \rangle$ is the order of g. Consider the homomorphism $\varphi : \mathbb{Z} \to \langle g \rangle$ given by $\varphi(i) = g^i$. The kernel of φ

[1] Since every subsemigroup can be made into a submonoid by adding the identity element, one can also consider subsemigroups here.

[2] However, not every group in M must be a submonoid of M.

is $\ker \varphi = \operatorname{ord}(g)\mathbb{Z}$. By Theorem 2.1 we obtain $\langle g \rangle \simeq \mathbb{Z}/\operatorname{ord}(g)\mathbb{Z}$. In particular, every finite cyclic group G is isomorphic to $\mathbb{Z}/|G|\mathbb{Z}$.

A group G is *commutative* or *abelian* if $gh = hg$ for all $g, h \in G$. Examples of commutative groups are cyclic groups. Moreover, cyclic groups are the basic building block of commutative groups. The classification of finite abelian groups states that every finite abelian group is isomorphic to some direct product of cyclic groups. A weaker statement is used in Theorem 5.24. Let $A \subseteq G$ be a set of generators of an abelian group G, then G is a homomorphic image of $\prod_{a \in A} \mathbb{Z}/\operatorname{ord}(a)\mathbb{Z}$.

2.1.3 Actions

This subsection is only needed in order to follow the proof of Proposition 4.17. An *action* of a monoid M on a set Q is a mapping $\cdot : Q \times M \to Q$ such that $q \cdot 1 = q$ and $(q \cdot m) \cdot n = q \cdot (mn)$ for all $q \in Q$ and $m, n \in M$. We also say that M acts on Q. An action is *faithful* if $q \cdot m = q \cdot n$ for all $q \in Q$ implies $m = n$. One can assign to every element $m \in M$ a mapping $\delta_m : Q \to Q$ given by $\delta_m(q) = q \cdot m$. Thus, the action is faithful if and only if the mapping $m \mapsto \delta_m$ is injective. Therefore, every faithful action provides an embedding into the transformation monoid of Q.

A monoid M acts *trivially* on Q if $q \cdot m = q$ for all $q \in Q$ and $m \in M$.

2.1.4 Local Divisors

Local divisors are used throughout the thesis as a powerful tool for inductive proofs on monoids, see for example Proposition 3.8, Proposition 4.14 or Theorem 5.31.

Let M be a monoid and $c \in M$. We set $M_c = cM \cap Mc$, that is, every element in $x \in M_c$ can be written as $x = cx_r = x_l c$ for some $x_l, x_r \in M$. We introduce an operation $\circ$ on M_c given by

$$uc \circ cv = ucv.$$

Since $uc \in cM$ and $cv \in Mc$, the result of $uc \circ cv$ is in M_c. Further, $\circ$ is well-defined: let $uc = u'c$ and $cv = cv'$, then $uc \circ cv = ucv = u'cv = u'cv' = u'c \circ cv'$. Note that for $cu, cv \in M_c$ we obtain $cu \circ cv = cuv$ which directly implies associativity of $\circ$. It is easy to see that c is the neutral element. Thus, $(M_c, \circ, c)$ forms a monoid, the *local divisor* of M at c. The motivation for the name is the following. Consider the submonoid $N = \{x \in M \mid cx \in Mc\}$ of M. Then the mapping $\varphi : N \to M_c$ given by $x \mapsto cx$ is surjective homomorphism:

$$\varphi(xy) = cxy = cx \circ cy = \varphi(x) \circ \varphi(y)$$

for $x, y \in N$ and every element of M_c is given by cx for some $x \in N$. Therefore, M_c is a divisor of M. If $c = e$ is an idempotent $e^2 = e$, the local divisor M_e is exactly the *local monoid* eMe of M.

The following lemma is fundamental for our usage of local divisors. It shows that certain local divisors are smaller than the original monoid.

Lemma 2.2. *Let M be a monoid and $c \in M$ be an element which is not a unit. Then $|M_c| < |M|$.*

Proof. Since c is not a unit, there either exists no $d \in M$ with $cd = 1$ or no $d \in M$ with $dc = 1$. Thus, $1 \notin cM \cap Mc = M_c$ which concludes the proof. □

In fact, $|M_c| < |M|$ holds if and only if c is not a unit. If c is a unit, we have $cM = M = Mc$ and thus $|M_c| = |M|$. Even stronger, if c is a unit, the mapping $m \mapsto cm$ is an isomorphism of M to M_c.

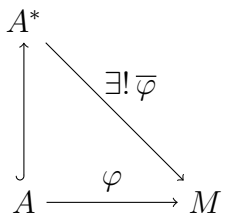
2.2 Words and Formal Languages

In this section we introduce some notions on formal languages. Our treatise of infinite words differs a bit from the classical approach, but is equivalent. The definition of recognizability is taken from [DK15a, DW16].

2.2.1 Words

An *alphabet* is a non-empty finite set A. An element of $a \in A$ is called a *letter*. A (finite) *word* $w = a_1 \cdots a_n$ is a finite concatenation of letters $a_1, \ldots, a_n \in A$. The set of finite words with letters in A is denoted by A^*. The *empty word* is denoted by 1. An infinite word $w = a_1 a_2 \cdots$ is an infinite concatenation of letters $a_i \in A$. Formally, an infinite word can be seen as a mapping $w : \mathbb{N} \to A$, mapping the positions of the word to the corresponding letter. The set of infinite words is denoted by A^ω. Since some of our results concern finite and infinite words, it is convenient to treat finite and infinite words simultaneously. Consequently, let $A^\infty = A^* \cup A^\omega$ be the set of finite or infinite words. For words $u \in A^*$ and $v \in A^\infty$, the concatenation of u with v is denoted by $u \cdot v$. Again, one omits the operation $\cdot$ and simply writes uv for $u \cdot v$. Note that one cannot concatenate an infinite word with another word, that is, uv is undefined for $u \in A^\omega$. The set of finite words A^* forms a monoid with the concatenation operation, the *free monoid*. The name stems from the following universal property:

For every function $\varphi : A \to M$ from an alphabet A to a monoid M there exists exactly one homomorphism $\overline{\varphi} : A^* \to M$ such that $\varphi(a) = \overline{\varphi}(a)$ for all $a \in A$, that is the following commutative diagram holds.



In order to define length and weight we apply this universal property for the monoid $M = \mathbb{N}$. Let $\|\cdot\| : A \to \mathbb{N}$ be a function with $\|a\| > 0$ for all $a \in A$. The unique homomorphism, which extends $\|\cdot\|$, is also denoted by $\|\cdot\|$. We call the homomorphism

$\|\cdot\|$ a *weight*. A special weight is the homomorphism *length* $|\cdot| : A^* \to \mathbb{N}$ which is induced by $|a| = 1$ for all $a \in A$. For a letter $c \in A$ we also define $|\cdot|_c : A^* \to \mathbb{N}$ to be the homomorphism which is induced by

$$|a|_c = \begin{cases} 1 & \text{if } a = c \\ 0 & \text{else.} \end{cases}$$

We set $A^{\leq n} = \{w \in A^* \mid |w| \leq n\}$ to be the set of words of length at most n.

2.2.2 Formal Languages

A *language* L is a subset of A^∞. Often, a language is defined to contain only either finite or infinite words. However, whenever feasible, we will work on both finite and infinite words simultaneously. For languages $L \subseteq A^*$ and $K \subseteq A^\infty$, we define the *concatenation product* $L \cdot K = \{uv \mid u \in L, v \in K\}$. Moreover, we define the *Kleene star*

$$L^* = \{u_1 u_2 \cdots u_n \mid u_i \in L\} \subseteq A^*$$

and the infinite iteration

$$L^\omega = \{u_1 u_2 \cdots \mid u_i \in L, u_i \text{ non-empty}, i \in \mathbb{N}\} \subseteq A^\omega.$$

In particular, the definition implies $L^\omega = (L \setminus \{1\})^\omega$.

We say that $L \subseteq A^\infty$ is *regular*, if first, $L \cap A^*$ is regular and second, $L \cap A^\omega$ is ω-regular in the standard meaning of formal language theory. Regular languages are exactly the class of languages recognized by finite automatons. The acceptance mode changes depending on whether one wants to recognize languages of finite words, infinite words or both. We will only use automatons for regular languages $L \subseteq A^*$. A *deterministic finite automaton* is a 5-tuple $\mathcal{A} = (Q, A, \cdot, q_0, F)$ where A is the alphabet, $q_0 \in Q$ is the initial state, $F \subseteq Q$ is the set of final states and $\cdot : Q \times A^* \to Q$ is an action of the free monoid A^* on Q. The automaton $\mathcal{A}$ recognizes the language $L(\mathcal{A}) = \{w \in A^* \mid q_0 \cdot w \in F\}$. Every word w induces a transformation $\sigma_w : Q \to Q$ given by $q \mapsto q \cdot w$. The set $\mathrm{TM}(\mathcal{A}) = \{\sigma_u \mid u \in A^*\}$ is a monoid equipped with the operation $\sigma_u \cdot \sigma_v = \sigma_{uv}$. The monoid $\mathrm{TM}(\mathcal{A})$ is called the *transformation monoid* of $\mathcal{A}$. Let $L \subseteq A^*$ and $\mathcal{A}$ be a minimal automaton for L, then $\mathrm{TM}(\mathcal{A})$ is the *syntactic monoid* of L, denoted by $\mathrm{Synt}(L)$.

A special kind of ω-regular languages are *arrow languages*. Let $L \subseteq A^*$ be a language. We define

$$\overrightarrow{L} = \{u \in A^\omega \mid \text{infinitely many prefixes of } u \text{ are in } L\}$$

to be the arrow language of L. The set of arrow languages is exactly the set of deterministic languages [Tho90].

Classical formal language theory states "regular" is the same as "recognizable". This means: $L \subseteq A^*$ is regular if and only if its syntactic monoid is finite; $L \subseteq A^\omega$ is regular if and only if its syntactic monoid, in the sense of Arnold [Arn85], is finite and, in

addition, L is saturated by the syntactic congruence, see [PP04, Tho90]. We use a notion of recognizability which applies to languages $L \subseteq A^\infty$. Let $\varphi : A^* \to M$ be a homomorphism to a finite monoid M. First, we define a relation $\sim_\varphi$ as follows. If $u \in A^*$ is a finite word, then we write $u \sim_\varphi v$ if v is finite and $\varphi(u) = \varphi(v)$. If $u \in A^\omega$ is an infinite word, then we write $u \sim_\varphi v$ if v is infinite and if there are factorizations $u = u_1 u_2 \cdots$ and $v = v_1 v_2 \cdots$ into finite nonempty words such that $\varphi(u_i) = \varphi(v_i)$ for all $i \geq 1$. It is easy to see that $\sim_\varphi$ is not transitive on infinite words, in general. Therefore, we consider its transitive closure $\approx_\varphi$. If $u, v \in A^*$, then we have

$$u \sim_\varphi v \iff u \approx_\varphi v \iff \varphi(u) = \varphi(v).$$

If $u, v \in A^\omega$, then we have $u \approx_\varphi v$ if and only if there is sequence of infinite words $u_0, \ldots u_k$ such that

$$u = u_0 \sim_\varphi \cdots \sim_\varphi u_k = v.$$

We say that $L \subseteq A^\infty$ is *recognizable* by M if there exists a homomorphism $\varphi : A^* \to M$ such that $u \in L$ and $u \sim_\varphi v$ implies $v \in L$. We also say that M or φ recognizes L in this case. A language $L \subseteq A^*$ is recognized by φ if $L = \varphi^{-1}(\varphi(L))$. More generally, since the syntactic monoid of a regular language is the smallest recognizing monoid, the connection to the classical notation is as follows. A regular language $L \subseteq A^\infty$ is recognizable (in our sense) by φ if and only if the syntactic monoids of $L \cap A^*$ and $L \cap A^\omega$ are divisors of M.

The following lemma is well-known for the classical approach. We repeat its proof for our notion of recognizability.

Lemma 2.3. *Let N and M be finite monoids such that $N \preceq M$ and $L \subseteq A^\infty$ be a language which is recognized by N. Then L is recognized by M.*

Proof. Let $\varphi : A^* \to N$ be a homomorphism which recognizes L. Furthermore, let M' be a submonoid of M such that there exists a surjective homomorphism $\pi : M' \to N$. For every $n \in N$, choose some preimage $m_n \in M'$, i.e., $\pi(m_n) = n$. Let $\psi : A^* \to M$ be the homomorphism given by $\psi(a) = m_{\varphi(a)}$. Inductively, one obtains $\psi(w) \in M'$ and $\pi(\psi(w)) = \varphi(w)$. Thus, $\psi(u) = \psi(v)$ implies $\varphi(u) = \varphi(v)$. In particular, $u \sim_\psi v$ implies $u \sim_\varphi v$ and every $\sim_\varphi$-class is a finite union of $\sim_\psi$-classes. This implies that L is recognized by ψ. □

2.3 Varieties

In this section we give a short introduction to varieties and define a few varieties which appear throughout the thesis. Then we define the varieties induced by groups, an important class of varieties which appears throughout the thesis, and study their basic properties.

Definition 2.4. A *variety*[3] $\mathbf{V}$ is a class of finite monoids such that

[3]This is no variety in the sense of [Bir35]. In fact, as we only treat finite monoids we do not allow arbitrary direct products. This is usually know as *pseudovariety*. However, as we work with finite monoids only, we call such classes a variety instead of a pseudovariety.

- If $M \in \mathbf{V}$, $N \preceq M$, then $N \in \mathbf{V}$,
- $\prod_{i \in I} M_i \in \mathbf{V}$ for a finite index set I with $M_i \in \mathbf{V}$ for all $i \in I$. ◇

Note that setting $I = \emptyset$, the second condition implies that every variety contains the trivial monoid. A variety which contains only groups is called a *variety of groups*. We assign every variety $\mathbf{V}$ a corresponding language class $\mathbf{V}(A^\infty)$ such that $L \in \mathbf{V}(A^\infty)$ if and only if there exists a monoid $M \in \mathbf{V}$ and a homomorphism $\varphi : A^* \to M$ such that L is recognized by φ. Furthermore, one can restrict this definition to only finite or only infinite words:

$$\mathbf{V}(A^*) = \{L \subseteq A^* \mid L \in \mathbf{V}(A^\infty)\}$$
$$\mathbf{V}(A^\omega) = \{L \subseteq A^\omega \mid L \in \mathbf{V}(A^\infty)\}.$$

A Boolean combination of languages is recognized by the direct product of their syntactic monoids. Therefore, the following holds.

Lemma 2.5. *$\mathbf{V}(A^\infty)$, $\mathbf{V}(A^*)$ and $\mathbf{V}(A^\omega)$ are closed under Boolean operations.*

Definition 2.6. We will define a few varieties.

- **I** is the trivial variety consisting only of the trivial monoid $\{1\}$.
- **A** is the variety consisting of all monoids, which contain no groups.
- **G** is the variety of all groups.
- **Ab** is the variety of all abelian groups.
- **Gsol** is the variety of all solvable groups.

Let P be a set of numbers such that every divisor of $n \in P$ is in P and for coprime numbers $n, m \in P$ it holds $n \cdot m \in P$.[4]

- $\mathbf{Ab_P}$ is the variety of all abelian groups with order in P.
- $\mathbf{Gsol_P}$ is the variety of all solvable groups with order in P. ◇

Example 2.7. It is $\mathbf{I}(A^\infty) = \{\emptyset, A^*, A^\omega, A^\infty\}$. ◇

The following characterization of the variety of finite commutative groups **Ab** is well-known, see e.g. [Pin86, Corollary 3.12].

Lemma 2.8. *Let $L \subseteq A^*$ be a language, then $L \in \mathbf{Ab}(A^*)$ if and only if L is a Boolean combination of languages of the form $\{w \in A^* \mid |w|_a \equiv i \bmod n\}$ for some n.*

[4] Note that such a set P is defined by its prime powers.

Proof. A commutative group G is the direct product of cyclic groups $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$. Since direct products recognize exactly Boolean combinations, it suffices to consider languages recognized by $\mathbb{Z}/n\mathbb{Z}$. Let $\varphi : A^* \to \mathbb{Z}/n\mathbb{Z}$ and $L = \varphi^{-1}(K)$ for some $K \subseteq \mathbb{Z}/n\mathbb{Z}$. Then

$$\begin{aligned} L &= \left\{ w \in A^* \;\middle|\; \sum_{a \in A} |w|_a \cdot \varphi(a) \in K \right\} \\ &= \bigcup_{i \in K} \left\{ w \in A^* \;\middle|\; \sum_{a \in A} |w|_a \cdot \varphi(a) = i \right\} \\ &= \bigcup_{i \in K} \bigcup_{\sum_{a \in A} n_a = i} \bigcap_{a \in A} \{ w \mid |w|_a \equiv n_a \bmod n \}. \end{aligned}$$

For the converse, let $\varphi : A^* \to \mathbb{Z}/n\mathbb{Z}$ be given by $\varphi(a) = 1$ and $\varphi(b) = 0$ for $a \neq b \in A$. Then $\varphi^{-1}(i) = \{ w \mid |w|_a \equiv i \bmod n \} \in \mathbf{Ab}$ and the claim follows since varieties are closed under Boolean combinations, see Lemma 2.5. □

Let $\mathbf{H}$ be a variety of finite groups. We define

$$\overline{\mathbf{H}} = \{ M \mid \text{every group in } M \text{ is in } \mathbf{H} \}$$

to be the maximal class of monoids whose subsemigroups, which are groups, are in $\mathbf{H}$.

Lemma 2.9 ([Eil76, Proposition V.10.4])**.** *Let $\mathbf{H}$ be a variety of finite groups. Then $\overline{\mathbf{H}}$ is the maximal variety such that $\overline{\mathbf{H}} \cap \mathbf{G} = \mathbf{H}$.*

The rest of this subsection is devoted to the proof that $\overline{\mathbf{H}}(A^\infty)$ is closed under concatenation products. We first introduce a variant of Schützenberger products. These products are the usual tool for the algebraic characterization of the concatenation product on A^*, see [Sch65]. Let M be a finite monoid and $\varphi : A^* \to M$ be a homomorphism. Let

$$[w] = \{ (\varphi(w_1), \varphi(w_2)) \in M \times M \mid w = w_1 w_2 \}.$$

be the set of all possible factors of w. We define the operations

$$\begin{aligned} u \cdot [w] &= \{ (\varphi(u)m, n) \mid (m, n) \in [w] \} \\ [w] \cdot u &= \{ (m, n\varphi(u)) \mid (m, n) \in [w] \}. \end{aligned}$$

Note that these operations do not depend on u, but only on $\varphi(u)$. Every factorization of $u \cdot v$ is either a factorization within u or a factorization within v, that is, the equation $u \cdot [v] \cup [u] \cdot v = [uv]$ holds. Our variant of the *Schützenberger product* is defined as the monoid

$$\diamondsuit_\varphi M = \left\{ [w] \in 2^{M \times M} \;\middle|\; w \in A^* \right\}$$

equipped with the operation $[u][v] = [uv]$. This is well-defined since $[u] = [v]$ implies $\varphi(u) = \varphi(v)$. In fact, $\tilde{\varphi} : \diamondsuit_\varphi M \to M$ given by $\tilde{\varphi}([w]) = \varphi(w)$ is a homomorphism.

Our variant of the Schützenberger product was similarly defined in [DR95, Section 11.7]. It recognizes the concatenation product over A^∞. The proof is an adaptation of [DR95, Proposition 11.7.10] to the present notation.

Proposition 2.10. *Let $L \subseteq A^*$ and $K \subseteq A^\infty$ be languages recognized by $\varphi : A^* \to M$. Then $L \cdot K$ is recognized by the homomorphism $\psi : A^* \to \diamondsuit_\varphi M$ given by $\psi(w) = [w]$.*

Proof. Let $u = u_1u_2 \in A^*$ such that $u_1 \in L$ and $u_2 \in K$ and consider some word $v \in A^*$ such that $\psi(u) = \psi(v)$, i.e., $u \sim_\psi v$. Since $(\varphi(u_1), \varphi(u_2)) \in [u] = [v]$, there exists a factorization $v = v_1v_2$ such that $(\varphi(u_1), \varphi(u_2)) = (\varphi(v_1), \varphi(v_2))$. Consequently, $v_1 \in L$ and $v_2 \in K$, that is, $v = v_1v_2 \in L \cdot K$.

In the case of infinite words let $u = u_1u_2 \cdots \in L \cdot K$ and $v = v_1v_2 \cdots$ such that $\psi(u_i) = \psi(v_i)$ for all $i \in \mathbb{N}$, i.e., $u \sim_\psi v$. We may assume that $u_1 = u'u''$ such that $u' \in L$ and $u''u_2 \cdots \in K$. Again, there must exist a factorization $v_1 = v'v''$ such that $\varphi(u') = \varphi(v')$ and $\varphi(u'') = \varphi(v'')$. In particular, $u' \sim_\varphi v'$ which implies $v' \in L$. Since $\psi(u_i) = \psi(v_i)$ implies $\varphi(u_i) = \varphi(v_i)$, this yields $(u''u_2)u_3 \cdots \sim_\varphi (v''v_2)v_3 \cdots$ and therefore $v''v_2v_3 \cdots \in K$. Thus, $v = v'v''v_2v_3 \cdots \in L \cdot K$, which completes the proof. □

We show that every group contained in $\diamondsuit_\varphi M$ is a group in M. The argument is a slight deviation of the original argument of Petrone and Schützenberger [PS65, Sch65], in order to adapt to our variant of the Schützenberger product.

Proposition 2.11. *Let $\varphi : A^* \to M$ be a homomorphism. Every group $G \subseteq \diamondsuit_\varphi M$ can be embedded into M.*

Proof. Let $[e]$ be the identity in G. Consider again the homomorphism $\tilde{\varphi} : \diamondsuit_\varphi M \to M$. Since G is finite, the set $N = \{[w] \in G \mid \tilde{\varphi}([w]) = \varphi(w) = \varphi(e) = \tilde{\varphi}([e])\}$ is a subgroup of G. In fact, by Theorem 2.1, N is normal and G/N is isomorphic to $\tilde{\varphi}(G)$, which is a group in M. Thus, it remains to show $N = \{[e]\}$, i.e., $\tilde{\varphi}$ is injective on G.

Let $[s] \in N$ be an arbitrary element and $[t] \in N$ be its inverse. Then the following equations hold:

- $[e]^2 = [e]$
- $[e] = [s][t]$
- $[s] = [e][s][e]$

By the first equation we have $[e] = e[e] \cup [e]e$, and thus in particular $e[e] \subseteq [e]$.

By the second equation and $\varphi(s) = \varphi(t) = \varphi(e)$, it holds $[e] = s[t] \cup [s]t = e[t] \cup [s]e$. Since $e[e] \subseteq [e]$, we conclude $e[s]e \subseteq [e]$. Finally, using the third equation, we obtain

$$[s] = e([s][e]) \cup [e]se = e(s[e] \cup [s]e) \cup [e]e = e[e] \cup e[s]e \cup [e]e = [e] \cup e[s]e = [e]. \quad \square$$

Combining Proposition 2.10 and Proposition 2.11 yields the following corollary.

Corollary 2.12. *Let $\mathbf{H}$ be a variety of groups. Then $\overline{\mathbf{H}}(A^*)$ and $\overline{\mathbf{H}}(A^\infty)$ are closed under concatenation products.*

2.4 Combinatorics on Words

Combinatorics on words is an important tool for studying semi-Thue systems. It is useful for checking properties, such as confluence, on semi-Thue systems. In this section we will provide some basic tools from combinatorics on words.

Let $x = uvw \in A^*$ be a word. Then we call u a *prefix*, v a *factor* and w a *suffix* of x. The factor v is *proper* if u and w are not empty. The set of prefixes is given by $\text{Prefixes}(w) = \{u \mid u \text{ is a prefix of } w\}$ and the set of factors is given by $\text{Factors}(w) = \{u \mid u \text{ is a factor of } w\}$. The word $a_1 \cdots a_n$, with $a_i \in A$, is a *subword* of a word u if $u \in A^*a_1A^* \cdots A^*a_nA^*$. The word u is a power of the word v if $u = v^i$ for some $i \in \mathbb{N}$.

A seminal theorem of Lyndon and Schützenberger characterizes the commutation of words.

Theorem 2.13 (Lyndon and Schützenberger, [LS62])**.** *Let $u, v \in A^*$. Then $uv = vu$ if and only if there exists a word w such that u, v are a power of w.*

Let $w = a_1 \cdots a_n \in A^*$ be a word with a_i letters. We say that $p \in \mathbb{N}$ is a *period* of w if $a_i = a_{i+p}$ for all $1 \leq i \leq n - p$. By definition, every number greater or equal than n is a period of w. The theorem of Fine and Wilf describes an important property of periods.

Theorem 2.14 (Fine and Wilf, [FW65])**.** *Let p, q be periods of some word w. If $|w| \geq p + q - \gcd(p, q)$, then $\gcd(p, q)$ is a period of w.*

A word u is called *primitive* if it is only a power of itself, that is, if $u = v^i$ with $i \geq 1$ implies $i = 1$. An easy application of Theorem 2.13 is the following characterization of primitive words.

Lemma 2.15. *A word $u \in A^*$ is primitive if and only if u is not a proper factor of u^2.*

Proof. Assume first that u is primitive. If $u^2 = u_1uu_2$, we conclude $u = u_1u_2$ by observing the prefix and suffix of u^2 and $|u| = |u_1| + |u_2|$. In particular $u_1u_2u_1u_2 = u_1u_1u_2u_2$ and thus $u_2u_1 = u_1u_2 = u$. By Theorem 2.13 u_1 and u_2 are powers of the same word. Thus, one of the words u_1 or u_2 is empty by the primitivity of u, and u is no proper factor in the factorization $u^2 = u_1uu_2$.

If u is not primitive, that is, $u = v^i$ for $i > 1$, then $u^2 = vuv^{i-1}$ and henceforth u is a proper factor of u^2. □

2.5 Rewriting systems

In this section we introduce semi-Thue systems. Those systems go back to the seminal work of Thue [Thu10, Thu14]. A *semi-Thue system* S over the alphabet A is a finite subset of $A^* \times A^*$. An element $(\ell, r) \in S$ is called a *rule*, where ℓ is the left side and r is the right side of the rule. The idea of a semi-Thue system is, that left sides of rules can

be replaced by right sides of the rule. Thus, one often also calls a semi-Thue system a *rewriting system*. For a semi-Thue system S we define the relation $\underset{S}{\Longrightarrow}$ given by

$$u_1 \ell u_2 \underset{S}{\Longrightarrow} u_1 r u_2 \text{ for } u_1, u_2 \in A^* \text{ and } (\ell, r) \in S$$

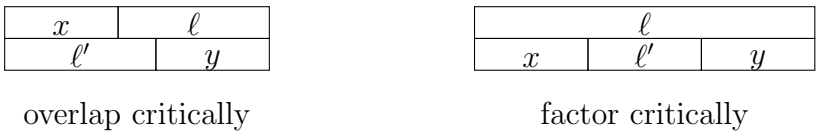
that is, $u \underset{S}{\Longrightarrow} v$ if v results from u by replacing the left side of a rule with the right side. The reflexive transitive closure of $\underset{S}{\Longrightarrow}$ is denoted by $\overset{*}{\underset{S}{\Longrightarrow}}$ and the reflexive, transitive and symmetric closure of $\underset{S}{\Longrightarrow}$ is denoted by $\overset{*}{\underset{S}{\Longleftrightarrow}}$. We write $v \underset{S}{\Longleftarrow} u$ for $u \underset{S}{\Longrightarrow} v$. A semi-Thue system S is

- *Church-Rosser*, if $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$ implies that there exists a $w \in A^*$ such that $u \overset{*}{\underset{S}{\Longrightarrow}} w$ and $w \overset{*}{\underset{S}{\Longleftarrow}} v$.
- *confluent*, if $u \overset{*}{\underset{S}{\Longrightarrow}} v_1$ and $u \overset{*}{\underset{S}{\Longrightarrow}} v_2$ imply that there exists a word $w \in A^*$ such that $v_1 \overset{*}{\underset{S}{\Longrightarrow}} w$ and $v_2 \overset{*}{\underset{S}{\Longrightarrow}} w$.
- *locally confluent*, if $u \underset{S}{\Longrightarrow} v_1$ and $u \underset{S}{\Longrightarrow} v_2$ imply that there exists a word $w \in A^*$ such that $v_1 \overset{*}{\underset{S}{\Longrightarrow}} w$ and $v_2 \overset{*}{\underset{S}{\Longrightarrow}} w$.
- *terminating*, if there is no infinite chain $(u_i)_{i \in \mathbb{N}}$ with $u_i \underset{S}{\Longrightarrow} u_{i+1}$ for all $i \in \mathbb{N}$.
- *length-reducing*, if $|\ell| > |r|$ for all rules $(\ell, r) \in S$.
- *weight-reducing* for a weighted alphabet $(A, \|\cdot\|)$, if $\|\ell\| > \|r\|$ for all rules $(\ell, r) \in S$.
- *Parikh-reducing*, if for all $a \in A$ and all rules $(\ell, r) \in S$ it holds $|\ell|_a \geq |r|_a$ and for all rules $(\ell, r) \in S$ there exists a letter $a \in A$ such that $|\ell|_a > |r|_a$.
- *subword-reducing*, if $r \neq \ell$ and r is a subword of ℓ for each rule $(\ell, r) \in S$.
- *convergent*, if S is locally confluent and terminating.

Lemma 2.16 ([BO93])**.** *Let $S \subseteq A^* \times A^*$ be a semi-Thue system. Then*

1. *S is confluent if and only if S is Church-Rosser.*
2. *S is convergent implies that S is confluent.*
3. *S is length-reducing (weight-reducing, Parikh-reducing, subword-reducing) implies that S is terminating.*

In the following we study different cases which may occur when checking for local confluence. Let $(\ell, r), (\ell', r') \in S$ be two rules and consider the word $u\ell v\ell' w$. Then



overlap critically factor critically

Figure 2.1: Sources of critical pairs [DKRW15]

$$\begin{array}{ccc} u\ell v\ell' w & \underset{S}{\Longrightarrow} & u\ell v r' w \\ \Big\Downarrow S & & \Big\Downarrow S \\ urv\ell' w & \underset{S}{\Longrightarrow} & urvr' w \end{array}$$

Thus, checking for local confluence in this case is trivial. The only non-trivial cases appear when two rules overlap. There are two different kinds of overlaps:

1. $w = x\ell = \ell' y$,
2. $w = \ell = x\ell' y$

for rules $(\ell, r), (\ell', r') \in S$. The resulting pairs $(xr, r'y)$ and $(r, xr'y)$ are called *critical pairs*. The first kind is called *overlap critical* and the second kind is called *factor critical*, see also Figure 2.1. We say that a critical pair (u, v) resolves if there exists a word $w \in A^*$ such that $u \underset{S}{\overset{*}{\Longrightarrow}} w \underset{S}{\overset{*}{\Longleftarrow}} v$ holds. Summarized, we obtain the following:

Lemma 2.17 ([KB70])**.** *A semi-Thue system is locally confluent if and only if all its critical pairs resolve.*

This directly yields a polynomial algorithm to check for confluence of weight-reducing semi-Thue systems. Lemma 2.17 will be used without explicitly referring to it.

The following lemma shows that one can consider minimal semi-Thue systems without losing properties.

Lemma 2.18. *Let $S \subseteq A^* \times A^*$ and $S' \subseteq A^* \times A^*$ be two semi-Thue systems with $u \underset{S}{\overset{*}{\Longrightarrow}} v$ if and only if $u \underset{S'}{\overset{*}{\Longrightarrow}} v$ for all $u, v \in A^*$. Then S is confluent if and only if S' is confluent.*

Proof. This is clear by definition. □

The notion Parikh-reducing comes from the connection to *Parikh images*. A Parikh image of a word $w \in A^*$ is the vector $(|w|_a)_{a \in A}$. A semi-Thue system S is Parikh-reducing if and only if the Parikh image $(|r|_a)_{a \in A}$ is smaller than $(|\ell|_a)_{a \in A}$ for every rule $(\ell, r) \in S$. By definition every subword-reducing system is Parikh-reducing. Further, for arbitrary weight $\|\cdot\|$, it is easy to see that every Parikh-reducing system is weight-reducing for $\|\cdot\|$. The following lemma shows that Parikh-reducing systems are exactly those systems that are weight-reducing for every weight.

Lemma 2.19. *A semi-Thue system $S \subseteq A^* \times A^*$ is Parikh-reducing if and only if it is weight-reducing for every weight $\|\cdot\| : A^* \to \mathbb{N}$.*

Proof. Let $\|\cdot\| : A^* \to \mathbb{N}$ be a weight. By definition it holds $\|w\| = \sum_{a \in A} |w|_a \cdot \|a\|$. Thus, Parikh-reducing implies weight-reducing for $\|\cdot\|$.

We assume that S is weight-reducing for every weight. Let $(\ell, r) \in S$ be a rule which contradicts the requirements for Parikh-reducing. Then either $|\ell|_a = |r|_a$ for all $a \in A$, that is, S is not weight-reducing for length, or there exists a letter $a \in A$ such that $|\ell|_a < |r|_a$. Consider the weight $\|\cdot\| : A^* \to \mathbb{N}$ given by $\|a\| = |\ell|$ and $\|b\| = 1$ for all $a \neq b \in A$. We obtain

$$\begin{aligned} \|\ell\| &= |\ell|_a \cdot \|a\| + \sum_{b \in A \setminus \{a\}} |\ell|_b \\ &\leq |\ell|_a \cdot \|a\| + |\ell| = (|\ell|_a + 1) \cdot \|a\| \\ &\leq |r|_a \cdot \|a\| \leq \|r\| \,. \end{aligned}$$

Thus, S is not weight-reducing for $\|\cdot\|$ which is a contradiction. □

A word w is *irreducible* in S if no left-side of a rule in S appears in w. We denote the set of irreducible elements of S by $\mathrm{IRR}_S(A^*)$. The relation $\overset{*}{\underset{S}{\Longleftrightarrow}}$ is a congruence on A^*. Thus, one can consider the monoid $A^*/S = A^*/\overset{*}{\underset{S}{\Longleftrightarrow}}$. The elements of A^*/S are equivalence classes $[u]_S = \left\{ v \in A^* \;\middle|\; u \overset{*}{\underset{S}{\Longleftrightarrow}} v \right\}$ of the congruence $\overset{*}{\underset{S}{\Longleftrightarrow}}$. The number of elements in A^*/S is called *index* of S. If S is confluent and terminating, there is a bijection between A^*/S and $\mathrm{IRR}_S(A^*)$. In this case, we denote elements of the monoid A^*/S with the corresponding irreducible words.

A semi-Thue system S is a *Church-Rosser system* if it is length-reducing and confluent. By Lemma 2.16 it suffices to require local confluence instead of confluence for a Church-Rosser system. Replacing the requirement of length-reducing rules with weight-reducing or Parikh-reducing rules yields *weighted Church-Rosser systems* or *Parikh-reducing Church-Rosser systems*.

Chapter 3

Rees extensions

In this chapter we use Rees extension to give a decomposition of monoids in $\overline{\mathbf{H}}$ as iterated Rees products of their groups. We use this decomposition to prove a conjecture of Almeida and Klíma. Additionally, we study the size of the resulting decomposition tree. Apart from this study of decomposition trees, this chapter has been published in [DW16].

3.1 Previous Work

There is a rich theory on Rees matrix semigroups. The starting point is Green-Rees local structure theory. We will present its results for finite semigroups, only. For a semigroup S, let S^1 be the monoid obtained by adjoining a neutral element to S. A (two-sided) *ideal* of a semigroup S is a subset $I \subseteq S$ such that $I = S^1 \cdot I \cdot S^1$. A semigroup S is *simple*, if S has no proper ideals, that is, S is the only ideal of S. In the terminology of Green [Gre51], this means that S has only one $\mathcal{J}$-class. The semigroup S is 0-*simple*, if S contains a zero element 0, it holds $S^2 \neq \{0\}$ and $\{0\}$ and S are the only ideals of S.

Let A, B be sets, G be a finite group and $f : B \times A \to G \cup \{0\}$ be a mapping. The underlying set of the *Rees matrix semigroup* $\mathcal{M}^0(A, G, B, f)$ is $A \times G \times B \cup \{0\}$. The multiplication is given by

$$(a, g, b)(a', g', b') = \begin{cases} (a, g \cdot f(b, a') \cdot g', b') & \text{if } f(b, a') \neq 0 \\ 0 & \text{else} \end{cases}$$

If $f(b, a) \neq 0$ for all $a \in A, b \in B$, we denote the semigroup $\mathcal{M}^0(A, G, B, f) \setminus \{0\}$ by $\mathcal{M}(A, G, B, f)$. The function $f : B \times A \to G \cup \{0\}$ can be interpreted as a $B \times A$ matrix having entries in $G \cup \{0\}$. The Rees matrix semigroup $\mathcal{M}^0(A, G, B, f)$ is regular[1] if and only if the matrix of f has no rows or columns which are zero, that is if for all $a \in A$ and $b \in B$ the functions $f(b, \cdot)$ and $f(\cdot, a)$ are not the constant 0-function. The Rees-Suschkewitsch Theorem classifies the class of finite (0-)simple semigroups in terms of regular Rees matrix semigroups. It has been proven by Suschkewitsch for finite semigroups and generalized by Rees for stable semigroups.

[1] in the sense of semigroup theory, that is, every element has a pseudoinverse.

Theorem 3.1 ([RS09], originally [Sus28, Ree40]). *Let S be a finite semigroup. Then S is 0-simple if and only if it is isomorphic to a regular Rees matrix semigroup $\mathcal{M}^0(A, G, B, f)$. Furthermore, S is simple if and only if it is isomorphic to $\mathcal{M}(A, G, B, f)$ for some sets A, B and a function $f : B \times A \to G$.*

Using this theorem, one can give a description of the local structure of a semigroup. The minimal $\mathcal{J}$-classes are characterized by the theorem above. Then one considers the semigroup obtained by the quotient of this $\mathcal{J}$-class to classify the rest of the semigroup, see [CP61, RT68] for a general treatise on Green-Rees local structure theory.

Let S be a finite semigroup. For their synthesis theorem, Allen and Rhodes considered a generalization of the Rees matrix semigroup $R(S) = \mathcal{M}(A, S, B, f)$ using a semigroup S instead of a group G. For a group G, let $S + G$ denote a monoid with ideal S and group of units G. Further, denote by $G^* = \{C_g \mid g \in G\} + G$ the semigroup obtained by the operation $C_g C_h = C_h$, $gC_h = C_h$ and $C_g h = C_{gh}$.

The synthesis theorem combines ("synthesizes") the local structure theory of Green and Rees together with the ideas obtained by the wreath product decomposition by Krohn and Rhodes [KR65, KRT68]. In particular, its proof borrows ideas obtained by Zeiger's proof [Zei67] of the wreath product decomposition. For an exposition and discussion of the result see [Rho70, RA73].

Theorem 3.2 ([RA73]). *Let S be a finite semigroup. Then there exists groups $G_1, \ldots, G_k$ which are divisors of S such that $S \preceq R = R(\cdots(R(G_1^*) + G_2)\cdots) + G_k$.*

Moreover, the embedding of S into the iterated Rees matrix semigroups and adjoining of groups is in a sense "nice", that is, there exists a subsemigroup T of R and a surjective homomorphism $\varphi : T \to S$ which has "nice" properties[2]. Further developments of the synthesis theorem can be found in [Rho86a, Rho86b] for infinite semigroups and in [Bir88] for a stronger statement in the case of regular finite semigroups.

3.2 Rees extensions

In this section, we use yet another definition of Rees matrix semigroups. First of all, we work over monoids. The main reason being that the proof technique of local divisors inherently uses monoids. Secondly, as in the synthesis theory of Allen and Rhodes, we use matrices of monoids instead of groups. Furthermore, our kind of Rees matrix monoid has a special Rees matrix semigroup of Allen and Rhodes as a proper ideal and finally the sets A, B are equal and monoids itself.

Let us now define our kind of *Rees extension monoids*. The definition is taken from [DKW12] and has recently also been used by Almeida and Klíma [AK16]. Let N, M be monoids and $\rho : N \to M$ be any mapping. As a set we define

$$\mathrm{Rees(N, M, \rho)} = N \cup N \times M \times N.$$

[2] "nice" in this context means it is a $\mathcal{J}'$ and $\gamma(\mathcal{H})$-homomorphism. We will not define these properties formally, as they are not important for the rest of the text.

The multiplication $\cdot$ on $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ is given by

$$\begin{aligned}
n \cdot n' &= nn' && \text{for } n, n' \in N,\\
n \cdot (n_1, m, n_2) &= (nn_1, m, n_2) && \text{for } n, n_1, n_2 \in N, m \in M,\\
(n_1, m, n_2) \cdot n &= (n_1, m, n_2 n) && \text{for } n, n_1, n_2 \in N, m \in M,\\
(n_1, m, n_2) \cdot (n_1', m', n_2') &= (n_1, m\rho(n_2 n_1')m', n_2') && \text{for } n_1, n_1', n_2, n_2' \in N, m, m' \in M.
\end{aligned}$$

The neutral element of $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ is $1 \in N$ and the inclusion $N \subseteq \mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ is an embedding of monoids. The Rees matrix semigroup $\mathcal{M}(N, M, N, f)$ with $f : N \times N \to M$ given by $f(n, n') = \rho(nn')$ is a subsemigroup of $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$. However, in general, M is not a divisor of $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ as observed by the following example.

Example 3.3. Let $M = \{1, a, 0\}$ be the monoid with identity 1, zero 0 and an idempotent a. Consider the Rees extension $\mathrm{Rees}(\{1\}, \mathrm{M}, \rho)$ with $\rho : \{1\} \to M$ given by $\rho(1) = 0$. The Rees extension $\mathrm{Rees}(\{1\}, \mathrm{M}, \rho)$ has no idempotents apart from 1 and $(1, 0, 1)$. In particular, M is not a divisor of $\mathrm{Rees}(\{1\}, \mathrm{M}, \rho)$. ◇

Example 3.4. Consider the mapping $\rho : N \to M$ given by $\rho(n) = 1$. Then $M \simeq \{1\} \times M \times \{1\} \leq \mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$, that is M is a submonoid of $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ for this choice of ρ. ◇

Lemma 3.5. *Let $N \preceq N'$ and $M \preceq M'$. Given $\rho : N \to M$, there exists a mapping $\rho' : N' \to M'$ such that* $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ *is a divisor of* $\mathrm{Rees}(\mathrm{N}', \mathrm{M}', \rho')$.

Proof. As a divisor is a homomorphic image of a submonoid, we will prove this in two steps. First, assume that N (resp. M) is a submonoid of N' (resp. M'). Let $\rho' : N' \to M'$ be any function such that $\rho'|_N = \rho$. The mapping $\pi : \mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho) \to \mathrm{Rees}(\mathrm{N}', \mathrm{M}', \rho')$ given by $\pi(n) = n$ and $\pi(n_1, m, n_2) = (n_1, m, n_2)$ is an injective homomorphism.

Second, let $\varphi : N' \to N$ and $\psi : M' \to M$ be surjective homomorphisms. Let $\rho' : N' \to M'$ be a function such that $\rho'(n) \in \psi^{-1}(\rho(\varphi(n)))$. Let

$$\pi : \mathrm{Rees}(\mathrm{N}', \mathrm{M}', \rho') \to \mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$$

be the mapping defined by $\pi(n) = \varphi(n)$ and $\pi(n_1, m, n_2) = (\varphi(n_1), \psi(m), \varphi(n_2))$. Given that φ and ψ are surjective, it is clear that π is surjective. It is a homomorphism since for all $n \in N'$, $x \in \mathrm{Rees}(\mathrm{N}', \mathrm{M}', \rho')$ it holds $\pi(nx) = \pi(n)\pi(x)$ and $\pi(xn) = \pi(x)\pi(n)$ and further for all $(n_1, m, n_2), (n_1', m', n_2') \in N \times M \times N$ it holds

$$\begin{aligned}
\pi((n_1, m, n_2) \cdot (n_1', m', n_2')) &= \pi(n_1, m\rho'(n_2 n_1')m', n_2')\\
&= (\varphi(n_1), \psi(m) \underbrace{\psi(\rho'(n_2 n_1'))}_{=\rho(\varphi(n_2 n_1'))} \psi(m'), \varphi(n_2'))\\
&= (\varphi(n_1), \psi(m), \varphi(n_2)) \cdot (\varphi(n_1'), \psi(m'), \varphi(n_2'))\\
&= \pi(n_1, m, n_2) \cdot \pi(n_1', m', n_2').
\end{aligned}$$

The result follows because $\preceq$ is transitive. □

An important property of the Rees extension monoid is that it does not introduce any new groups.

Proposition 3.6 ([AK16])**.** *Let G be a group in* $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$*, then there exists an embedding of G into N or into M.*

Proof. Let G be a subsemigroup of $\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho)$ which is a group. Since

$$(n, m, n')\mathrm{Rees}(\mathrm{N}, \mathrm{M}, \rho) \subseteq N \times M \times N,$$

one either has $G \subseteq N$ or $G \subseteq N \times M \times N$. In the case of $G \subseteq N$, we can directly embed G into N using the identity homomorphism. Consider the case $G \subseteq N \times M \times N$ and let $e = (n, \hat{e}, n') \in G$. For every $x \in G$, it holds $ex = x = xe$ and thus there must exist an element $\hat{x} \in M$ such that $x = (n, \hat{x}, n')$. Consider the mapping $\varphi : G \to M$ given by $\varphi(x) = \hat{x} \cdot \rho(n'n)$. Let $x = (n, \hat{x}, n'), y = (n, \hat{y}, n') \in G$, then

$$\varphi(x \cdot y) = \varphi((p, \hat{x}\rho(n'n)\hat{y}, n')) = \hat{x}\rho(n'n)\hat{y}\rho(n'n) = \varphi(x)\varphi(y).$$

Thus, φ is a homomorphism. Assume now that $\varphi(x) = \varphi(y)$, that is, $\hat{x}\rho(n'n) = \hat{y}\rho(n'n)$. Right multiplication by $\hat{e}$ and the fact the e is the neutral element of G yields $\hat{x} = \hat{x}\rho(n'n)\hat{e} = \hat{y}\rho(n'n)\hat{e} = \hat{y}$. Therefore, φ is injective which proves the claim. □

We are mainly interested in the case where N and M are proper divisors of a given finite monoid. This leads to the notion of local Rees monoids. More precisely, let M be a finite monoid, N be a proper submonoid of M and M_c be a local divisor of M at c where c is not a unit. The *local Rees product* $\mathrm{LocRees}(\mathrm{N}, \mathrm{M_c})$ is defined as the Rees extension $\mathrm{Rees}(\mathrm{N}, \mathrm{M_c}, \rho_c)$ where ρ_c denotes the mapping $\rho_c : N \to M_c; x \mapsto cxc$.

For a variety $\mathbf{V}$ we define $\mathrm{Rees}(\mathbf{V})$ to be the least variety which contains $\mathbf{V}$ and is closed under taking Rees products and $\mathrm{LocRees}(\mathbf{V})$ to be the least variety which contains $\mathbf{V}$ and is closed under local Rees products.

Thus, Proposition 3.6 implies $\mathrm{LocRees}(\mathbf{H}) \subseteq \mathrm{Rees}(\mathbf{H}) \subseteq \mathrm{Rees}(\overline{\mathbf{H}}) \subseteq \overline{\mathbf{H}}$ for any group variety $\mathbf{H}$. We want to prove equality, that is, every monoid which contains only groups in $\mathbf{H}$ is a divisor of an iterated Rees extension of groups in $\mathbf{H}$. However, we are able to prove a stronger statement using only local Rees extensions.

Lemma 3.7. *Let M be a monoid, N be a submonoid of M and $c \in M$. If N and c generate M, then M is a homomorphic image of the local Rees product* $\mathrm{LocRees}(\mathrm{N}, \mathrm{M_c})$*.*

Proof. Let $\varphi : \mathrm{LocRees}(\mathrm{N}, \mathrm{M_c}) \to M$ be the mapping given by $\varphi(n) = n$ for $n \in N$ and $\varphi(u, x, v) = uxv$ for $(u, x, v) \in N \times M_c \times N$. Since

$$\begin{aligned}\varphi((u, x, v)(s, y, t)) &= \varphi(u, x \circ cvsc \circ y, t) = \varphi(u, xvsy, t) \\ &= (uxv)(syt) = \varphi(u, x, v)\varphi(s, y, t),\end{aligned}$$

φ is a homomorphism. Obviously, $M = N \cup NM_cN$ and thus φ is surjective. □

Proposition 3.8. *Given M, we can construct a sequence of monoids $M_1, \ldots M_k = M$ with $k \leq 2^{|M|} - 1$ such that for each $1 \leq j \leq k$ we have for M_j one of the following:*

- *M_j is a group which is a divisor of M.*
- *M_j is a divisor of a local Rees product of a submonoid M_i of M_j and a local divisor M_ℓ of M_j with $i, \ell < j$.*

Proof. We prove the statement with induction on $|M|$. If M is a group, we set $M_1 = M$. This includes the base case $|M| = 1$. If M is not a group, we may choose a minimal generating set of M. Let c be a nonunit of this generating set, then there exists a proper submonoid N of M such that N and c generate M. Since c is not a unit, the local divisor M_c is smaller than M, that is, $|M_c| < |M|$ by Lemma 2.2. By induction, there exist sequences $M'_1, \ldots, M'_{k'} = N$ and $M''_1, \ldots, M''_{k''} = M_c$ with $k', k'' \leq 2^{|M|-1} - 1$. Note that every group, which is a divisor of N or M_c is also a divisor of M. Furthermore, M is a divisor of the local Rees product of $M_{k'} = N$ and $M_{k'+k''} = M_c$ by Lemma 3.7. Therefore, choosing

- $M_i = M'_i$ for $1 \leq i \leq k'$
- $M_{i+k'} = M''_i$ for $1 \leq i \leq k''$
- $M_{k'+k''+1} = M$

leads to such a sequence for M. Since

$$k' + k'' + 1 \leq 2 \cdot (2^{|M|-1} - 1) + 1 = 2^{|M|} - 1,$$

the bound on k holds. □

The inclusion $\overline{\mathbf{H}} \subseteq \mathrm{LocRees}(\mathbf{H})$ is immediate from Proposition 3.8. Therefore, a consequence of Proposition 3.6 and Proposition 3.8 is the following theorem.

Theorem 3.9. *For every variety of groups* $\mathbf{H}$*, it holds* $\mathrm{LocRees}(\mathbf{H}) = \mathrm{Rees}(\mathbf{H}) = \overline{\mathbf{H}}$.

In particular, every monoid in $\overline{\mathbf{H}}$ is a divisor of an iterated Rees product of groups in $\mathbf{H}$ by Lemma 3.5. We can draw the decomposition as a tree based on the decomposition of M in submonoids and local divisors.

Definition 3.10. Let M be a monoid. A *Rees decomposition tree* of M is a full binary tree T such that

- the root node of T is M,
- every leaf of T is a group which is a divisor of M and
- for every node M' with children N_1, N_2 there exists a function $\rho : N_1 \to N_2$ such that M' is a divisor of $\mathrm{Rees}(\mathrm{N}_1, \mathrm{N}_2, \rho)$.

The size of a decomposition tree is its number of nodes. ◇

In particular, Proposition 3.8 implies the existence of a decomposition tree of a finite monoid M of size at most $2^{|M|} - 1$. We give an example of such a tree below.

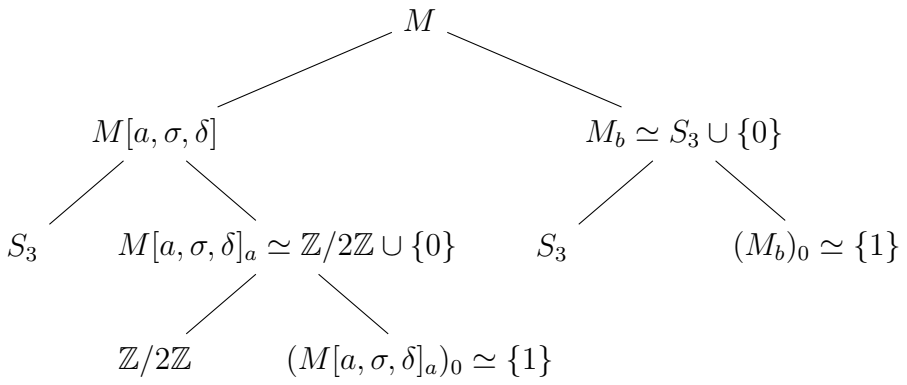


Figure 3.1: Decomposition tree of the monoid in Example 3.11.

Example 3.11. Let M be the monoid generated by $\{a, b, \delta, \sigma\}$ with the relations $a^2 = b^2 = ab = ba = 0$, $a\delta = a$, $\delta\sigma = \sigma\delta^2$, $\delta^3 = 1$, $\sigma^2 = 1$ and $d\delta = \delta d$, $d\sigma = \sigma d$ with $d \in \{a, b\}$. A possible set of representatives is

$$M = \left\{1, \delta, \delta^2, \sigma, \sigma\delta, \delta\sigma, b, b\delta, b\delta^2, b\sigma, b\sigma\delta, b\delta\sigma, a, a\sigma, 0\right\}.$$

In particular, M has 15 elements. The subgroup generated by δ and σ is the symmetric group S_3; it is solvable but not abelian. The monoid M is syntactic for the language L which is a union of L_a and L_b. The language L_a is the set of all words uav with $uv \in \{\delta, \sigma\}^*$ and the sign of the permutation uv evaluates to -1. The language L_b is the set of all words ubv with $uv \in \{\delta, \sigma\}^*$ and uv evaluates in S_3 to δ. We compute a possible decomposition in Rees products from Proposition 3.8. The decomposition is also depicted in Figure 3.1. We first decompose M using Lemma 3.7 by choosing $N = M[a, \sigma, \delta]$, the submonoid generated by $\{a, \sigma, \delta\}$, and $c = b$. It is

$$M[a, \sigma, \delta] = \left\{1, \delta, \delta^2, \sigma, \sigma\delta, \delta\sigma, a, a\sigma, 0\right\}$$

and

$$M_b = \left\{b, b\delta, b\delta^2, b\sigma, b\sigma\delta, b\delta\sigma, 0\right\} \simeq S_3 \cup \{0\}.$$

The decomposition of M_b is simple: S_3 is used as the proper submonoid and the local divisor is on $c = 0$, which yields the trivial group. For the decomposition of $M[a, \sigma, \delta]$ we choose again $\mathfrak{S}_3$ as the proper submonoid and $c = a$. Computing the local divisor yields $M[a, \sigma, \delta]_a = \{a, a\sigma, 0\}$, which again decomposes into the group $\{a, a\sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$ and the trivial group. In particular, this yields

$$M \preceq \mathrm{Rees}(\mathrm{Rees}(\mathrm{S}_3, \mathrm{Rees}(\mathbb{Z}/2\mathbb{Z}, \{1\}, \rho_1), \rho_2), \mathrm{Rees}(\mathfrak{S}_3, \{1\}, \rho_3), \rho_4)$$

for some $\rho_1, \rho_2, \rho_3, \rho_4$ by Lemma 3.5. ◇

Using local structure theory, one can improve the bound $2^n - 1$ of Proposition 3.8 to $\mathcal{O}(3^{n/3}) = \mathcal{O}((1.442\ldots)^n)$. First, we prove the following lemma which is a combination of classical local structure theory and the fact that the $\mathcal{H}$-class of c is the group of units

in M_c, see [CS14, DKRH16]. We give a self-contained proof without explicitly using known results of the local structure theory.[3]

Lemma 3.12. *Let M be a monoid and $x, c \in M$. Let further $MxM = McM$ and $x \in cM \cap Mc$, then x is a unit in M_c.*

Proof. We first prove $cM = xM$. Observe that $x \in cM$ implies $xM \subseteq cM$. Let $u \in M$ be such that $x = cu$ and let $y, z \in M$ such that $ycuz = c$. Iterating this equation yields $y^n c(uz)^n = c$. By choosing n large enough, we may assume that $(uz)^n$ is idempotent. Thus, this yields $c(uz)^n = c$ and therefore $cM = c(uz)^n M \subseteq xM$; showing $cM = xM$. The equation $Mc = Mx$ is clear by duality.

Since $Mc = Mx$, we obtain an element $v \in M$ such that $c = vx$. Consider the element $vc \in Mc$. We have $cM = xM$ and therefore $vcM = vxM = cM$. In particular, $vc \in cM$ and therefore $vc \in M_c$. Note that $vc \circ x = vx = c$, that is, vc is an inverse of x and x is a unit in M_c. □

Proposition 3.13. *Let M be a monoid having n elements which are not units. Then there exists a decomposition tree of M having $\mathcal{O}(3^{n/3})$ nodes.*

Proof. Let $g : \mathbb{N} \to \mathbb{N}$ be the function defined by $g(0) = 1$ and

$$g(n) = \max\{m(g(n-m)+1)+1 \mid m \leq n\}.$$

Note that $3^{1/3} = \max\left\{m^{1/m} \;\middle|\; m \in \mathbb{N}\right\}$ and therefore $g(n) \in \Omega(3^{n/3})$. The claim $g(n) \in \mathcal{O}(3^{n/3})$ can been seen by an induction. Furthermore, setting $m = 1$ yields that g is monotonically increasing. We show inductively on n that $g(n)$ is an upper bound to a minimal decomposition tree of M, that is, there exists a decomposition tree of M having at most $g(n)$ nodes. Choose an arbitrary, but minimal, set of generators for M and let m be the number of generators which are not a unit. We show by induction on n that M has a decomposition tree with at most $m(g(n-m)+1)+1$ nodes. The case that M is a group, i.e., $n = m = 0$, is easy. The tree has only one node: the root node M. Assume that $n, m > 0$. Denote by $\{a_1, \ldots, a_{m-1}, c\}$ the subset of generators which are not a unit. We may assume that $Ma_iM \subseteq McM$ implies $Ma_iM = McM$, that is, c generates a minimal, among those generators, two-sided ideal with respect to inclusion.[4] Using Lemma 3.7, we decompose M into the monoid N using the generators without c and $M_c = cM \cap Mc$. Note that $cM \cap Mc \subseteq McM$. Therefore, $a_i \in cM \cap Mc$ implies $Ma_iM = McM$ and by Lemma 3.12 we obtain that a_i is a unit in M_c. In particular, all elements in $\{a_1, \ldots, a_{m-1}, c\}$ are either not contained in M_c or are units in M_c, that is, M_c has at most $n - m$ elements which are not units. By induction, M_c has a decomposition tree of size at most $g(n-m)$. The monoid N has a minimal generating set with $m-1$ generators which are not a unit and at most $n-1$ elements which are not units. By induction and the fact that g is monotonically increasing, we

[3] The high-level version of the proof is as follows: $x \mathcal{J} c$ and $x \in cM \cap Mc$ implies $x \mathcal{H} c$ and therefore x is a unit of M_c.

[4] Using Green's relations, this means that c is $\leq_{\mathcal{J}}$-minimal.

obtain a decomposition tree of N of size at most $(m-1)(g((n-1)-(m-1))+1)+1$. In total this yields a decomposition tree for M of size at most

$$(m-1)(g((n-1)-(m-1))+1)+1+g(n-m)+1 = m(g(n-m)+1)+1 \leq g(n).$$

This proves that $g(n)$ is a upper bound for the size of a minimal decomposition tree. □

3.3 An application to bullet idempotent varieties

An application of Proposition 3.8 is the solution to an open question of Almeida and Klíma. Let $\mathbf{U}$ and $\mathbf{V}$ be varieties. Let $\mathrm{Rees}(\mathbf{U},\mathbf{V})$ be the variety generated by $\mathrm{Rees}(\mathrm{N},\mathrm{M},\rho)$ for $N \in \mathbf{U}$ and $M \in \mathbf{V}$. Since N is a submonoid of $\mathrm{Rees}(\mathrm{N},\mathrm{M},\rho)$, it holds $\mathbf{U} \subseteq \mathrm{Rees}(\mathbf{U},\mathbf{V})$. However, by Example 3.4, we also obtain $\mathbf{V} \subseteq \mathrm{Rees}(\mathbf{U},\mathbf{V})$.

Note that in general $\mathrm{Rees}(\mathbf{V}) \neq \mathrm{Rees}(\mathbf{V},\mathbf{V})$. However $\mathrm{Rees}(\mathbf{V})$ is the limit of this operation. Let $\mathbf{V}_i = \mathrm{Rees}(\mathbf{V}_{\mathrm{i}-1},\mathbf{V}_{\mathrm{i}-1})$ and $\mathbf{V}_0 = \mathbf{V}$, then

$$\mathrm{Rees}(\mathbf{V}) = \bigcup_{i\in\mathbb{N}} \mathbf{V}_i.$$

The variety $\mathrm{Rees}(\mathbf{U},\mathbf{V})$ has recently been introduced by Almeida and Klíma under the name of *bullet operation* [AK16]. They defined a variety $\mathbf{V}$ to be *bullet idempotent* if $\mathbf{V} = \mathrm{Rees}(\mathbf{V},\mathbf{V})$ and posed the open question whether there are varieties apart from $\overline{\mathbf{H}}$ which are bullet idempotent. Using Theorem 3.9, we prove that the answer to this question is no.

Theorem 3.14. *Let* $\mathbf{V}$ *be a bullet idempotent variety and let* $\mathbf{H} = \mathbf{V} \cap \mathbf{G}$*, then* $\mathbf{V} = \overline{\mathbf{H}}$*.*

Proof. Since $\overline{\mathbf{H}}$ is the maximal variety with $\overline{\mathbf{H}} \cap \mathbf{G} = \mathbf{H}$ by Lemma 2.9, we have $\mathbf{V} \subseteq \overline{\mathbf{H}}$. Note that $\mathbf{V} = \mathrm{Rees}(\mathbf{V},\mathbf{V})$ implies that $\mathbf{V} = \mathrm{Rees}(\mathbf{V})$ by the limit characterization of $\mathrm{Rees}(\mathbf{V})$. Thus, it holds

$$\overline{\mathbf{H}} \subseteq \mathrm{Rees}(\mathbf{H}) \subseteq \mathrm{Rees}(\mathbf{V}) = \mathbf{V} \subseteq \overline{\mathbf{H}}$$

by Theorem 3.9. □

Chapter 4

Language Characterizations of $\overline{\mathbf{H}}$

In this chapter we study varieties induced by certain varieties $\mathbf{H}$, that is, varieties of the form $\overline{\mathbf{H}}$. Most of this chapter has been published in [DW16]. The language class $\overline{\mathbf{H}}(A^*)$ is closed under concatenation products, see Corollary 2.12. However, the language class $\overline{\mathbf{H}}(A^*)$ is not the closure of $\mathbf{H}(A^*)$ under concatenation products. This can be seen as follows. By a result of Straubing, the closure of a variety of languages $\mathbf{V}$ under concatenation product is again a variety of languages [Str79a]. Algebraically, the closure is given by the Mal'cev product $(\mathbf{A} \mathbin{ⓜ} \mathbf{V})(A^*)$. In particular, [Str79a] shows that for a variety of groups $\mathbf{H}$ it is $\mathbf{A} \mathbin{ⓜ} \mathbf{H} = \mathbf{A} * \mathbf{H}$, that is, the Mal'cev product equals the semidirect product of the two varieties. However, Steinberg constructed for every non-trivial group variety $\mathbf{H}$ a monoid M such that $M \in \overline{\mathbf{H}}$ but $M \notin \mathbf{A} * \mathbf{H}$ [Ste05]. In particular, $\overline{\mathbf{H}}(A^*)$ cannot be the closure of $\mathbf{H}(A^*)$ under concatenation product.

The main goal of this chapter is to obtain a description of the language classes defined by $\overline{\mathbf{H}}$. There exist partial results for some special $\mathbf{H}$. The most prominent characterizations exist for group-free monoids, that is, for the variety of aperiodic monoids. As observed, this is the special case where $\mathbf{H}$ is the trivial group variety. Apart from the usual characterization of aperiodic monoids as star-free expressions, there exists a lesser known characterization of Schützenberger in terms of prefix codes with synchronization delay. The definition of codes with synchronization delay appeared first in an article of Golomb and Gordon in 1965 [GG65]. A *code* $K \subseteq A^*$ is a set such that every word in K^* has a unique factorization in words of K. A *prefix code* is a set $K \subseteq A^*$ such that $u, uv \in K$ implies $v = 1$. One can easily check that a prefix code is indeed a code.

Definition 4.1. A prefix code $K \subseteq A^*$ has *synchronization delay* d if

$$uvw \in K^* \implies uv \in K^* \quad \text{for } v \in K^d.$$

Note that since K is a code this implies $w \in K^*$. We say K has *bounded synchronization delay* if there exists a number d such that K has synchronization delay d. ◇

Example 4.2.

- Every subset $B \subseteq A$ is a prefix code of synchronization delay 0.
- For $c \in A$ and $c \notin B \subseteq A$ the language B^*c is a prefix code of synchronization delay 1. ◇

4.1 Previous Work

Surprisingly, applying the star operation on a star-free prefix code of bounded synchronization delay yields a star-free language, see e.g. [PP04, DK15a]. This was first observed by Schützenberger.

Theorem 4.3 ([Sch75]). *The variety of star-free languages is the least Boolean algebra $\mathcal{C}$ closed under marked product[1] and under the star operation restricted to languages $K \in \mathcal{C}$ where K is a prefix code of bounded synchronization delay.*

Theorem 4.3 has been generalized to infinite words in [DK15a]. Schützenberger further improved his result in [Sch74]. He described the languages classes corresponding to $\overline{\mathbf{H}}$ for $\mathbf{H} \subseteq \mathbf{Ab}$. Note that $\mathbf{H} \subseteq \mathbf{Ab}$, implies $\mathbf{H} = \mathbf{Ab_P}$ for some set P of numbers such that every divisor of $n \in P$ is in P and for coprime numbers $n, m \in P$ it holds $n \cdot m \in P$. This also includes the result on star-free languages for $P = \emptyset$.

Theorem 4.4 ([Sch74]). *The variety of languages associated with $\overline{\mathbf{Ab_P}}$ is the least Boolean algebra $\mathcal{C}$ closed under marked product and under the star operation restricted to languages of the form K^n, where $n > 0$ has only prime factors in P and $K \in \mathcal{C}$ is a prefix code of bounded synchronization delay.*

The characterization $\mathrm{SD}_{\mathbf{H}}$ of $\overline{\mathbf{H}}$ treated in this chapter is a generalization of this characterization. Using only slight derivations to our proof technique, we are able to reprove Theorem 4.4, see Remark 4.16.

Straubing has studied the case $\mathbf{H} = \mathbf{Gsol_P}$ of solvable groups whose prime divisors of the order of the group are contained in the set P. Straubing's proof is based on the decomposition of solvable groups as wreath products of cyclic groups of order $p \in P$. The operation

$$\langle L, r, n\rangle = \{w \in A^* \mid |\{u \mid uv = w, u \in L\}| \equiv r \bmod n\}$$

is the basic building block for the language description of $\overline{\mathbf{Gsol_P}}$.

Theorem 4.5 ([Str79b]). *The variety of languages over A^* associated with $\overline{\mathbf{Gsol_P}}$ is the least boolean algebra $\mathcal{C}$, which contains $\{a\}$ for $a \in A$, is closed under concatenation product and contains $\langle La, r, p\rangle$ for $L \in \mathcal{C}$, $a \in A$, $r \in \mathbb{N}$ and $p \in P$.*

4.2 Language classes for $\overline{\mathbf{H}}$

4.2.1 Localizable classes

Let G be a finite group. We define the *localizable closure* $\mathrm{Loc}_G(A^\infty)$ on G inductively. Let $\mathrm{Loc}_G^{(0)}(A^\infty)$ be the set of all languages $L \subseteq A^\infty$ which is recognized by G. Let $\mathrm{Loc}_G^{(i)}(A^\infty)$ be the smallest set of languages such that

[1] A *marked product* is a concatenation product of the form $L \cdot a \cdot K$ for a letter $a \in A$.

- $\mathrm{Loc}_G^{(i-1)}(A^\infty) \subseteq \mathrm{Loc}_G^{(i)}(A^\infty)$,
- $L, K \in \mathrm{Loc}_G^{(i-1)}(A^\infty)$ implies $L \cup K \in \mathrm{Loc}_G^{(i)}(A^\infty)$ and
- for every $c \in A$ and $B = A \setminus \{c\}$ we have:
  1. $\mathrm{Loc}_G^{(i-1)}(B^\infty) \subseteq \mathrm{Loc}_G^{(i)}(A^\infty)$.
  2. If $L \in \mathrm{Loc}_G^{(i-1)}(B^\infty)$ and $K \subseteq A^*c$ with $K \in \mathrm{Loc}_G^{(i-1)}(A^\infty)$, then $KL \in \mathrm{Loc}_G^{(i)}(A^\infty)$.
  3. If $L \in \mathrm{Loc}_G^{(i-1)}(A^\infty)$ and $K \subseteq B^*$ with $K \in \mathrm{Loc}_G^{(i-1)}(B^\infty)$, then $KcL \in \mathrm{Loc}_G^{(i)}(A^\infty)$.
  4. Let T be a finite alphabet and $g : B^* \to T$ be a function such that $g^{-1}(t) \in \mathrm{Loc}_G^{(i-1)}(B^*)$. Let further $\sigma : (B^*c)^\infty \to T^\infty$ be defined by $\sigma(u_1cu_2c\cdots) = g(u_1)g(u_2)\cdots$. If $K \in \mathrm{Loc}_G^{(i-1)}(T^\infty)$, then $\sigma^{-1}(K) \in \mathrm{Loc}_G^{(i)}(A^\infty)$.

Taking the union over all these levels, one obtains the definition of the localizable closure on G:

$$\mathrm{Loc}_G(A^\infty) = \bigcup_{i\in\mathbb{N}} \mathrm{Loc}_G^{(i)}(A^\infty).$$

The classes $\mathrm{Loc}_G(A^*)$ and $\mathrm{Loc}_G(A^\omega)$ are the restrictions of $\mathrm{Loc}_G(A^\infty)$ on languages $L \subseteq A^*$ or $L \subseteq A^\omega$. That is

$$\begin{aligned}\mathrm{Loc}_G(A^*) &= \{L \subseteq A^* \mid L \in \mathrm{Loc}_G(A^\infty)\} \quad \text{and}\\ \mathrm{Loc}_G(A^\omega) &= \{L \subseteq A^\omega \mid L \in \mathrm{Loc}_G(A^\infty)\}.\end{aligned}$$

Since every appliance of a closure property only increases the level by one, Loc_G is the smallest family of languages such that

- every language $L \subseteq A^\infty$ recognized by G is in $\mathrm{Loc}_G(A^\infty)$,
- $L, K \in \mathrm{Loc}_G(A^\infty)$ implies $L \cup K \in \mathrm{Loc}_G(A^\infty)$ and
- for every $c \in A$ and $B = A \setminus \{c\}$ we have:
  1. $\mathrm{Loc}_G(B^\infty) \subseteq \mathrm{Loc}_G(A^\infty)$.
  2. If $K \in \mathrm{Loc}_G(A^*)$, $K \subseteq A^*c$, and $L \in \mathrm{Loc}_G(B^\infty)$, then $KL \in \mathrm{Loc}_G(A^\infty)$.
  3. If $K \in \mathrm{Loc}_G(B^*)$ and $L \in \mathrm{Loc}_G(A^\infty)$, then $KcL \in \mathrm{Loc}_G(A^\infty)$.
  4. Let T be a finite alphabet and $g : B^* \to T$ be a function such that $g^{-1}(t) \in \mathrm{Loc}_G(B^*)$. Let further $\sigma : (B^*c)^\infty \to T^\infty$ be defined by $\sigma(u_1cu_2c\cdots) = g(u_1)g(u_2)\cdots$. If $K \in \mathrm{Loc}_G(T^\infty)$, then $\sigma^{-1}(K) \in \mathrm{Loc}_G(A^\infty)$.

The definition using different levels is cleaner as property 4 uses $\mathrm{Loc}_G(T^\infty)$ for an arbitrary alphabet T and at this moment $\mathrm{Loc}_G(T^\infty)$ is not yet defined.

Remark 4.6. For every group G the language $\{1\} \subseteq \emptyset^*$ is recognized by G. In particular, for every alphabet A we obtain $\{1\} \in \mathrm{Loc}_G(A^*)$. Closure property 3 yields $\{w\} \in \mathrm{Loc}_G(A^*)$ for all $w \in A^*$. Since $\mathrm{Loc}_G(A^*)$ is closed under union, every finite languages of finite words is in $\mathrm{Loc}_G(A^*)$. ◇

The next lemma is a direct consequence of Lemma 2.3.

Lemma 4.7. *Let $H \preceq G$, then $\mathrm{Loc}_H(A^\infty) \subseteq \mathrm{Loc}_G(A^\infty)$.*

Let us further define the *localizable closure of* $\mathbf{H}$ as the language class

$$\mathrm{Loc}_{\mathbf{H}}(A^\infty) = \bigcup \{\mathrm{Loc}_G(A^\infty) \mid G \in \mathbf{H}\}.$$

The definition of the localizable closure of $\mathbf{H}$ is a generalization of the localizable classes defined in [DK15b], in fact the smallest localizable class in the sense of [DK15b] is $\mathrm{Loc}_{\mathbf{I}}(A^\infty)$.

Actually, the name of the localizable closure and the choice of the closure properties come in hindsight of the proof of Proposition 4.14, which uses the local divisor technique. The proof of Proposition 4.14 is an adaptation of techniques used in [DK15a, DW16].

4.2.2 SD classes

We generalize the star-operation to prefix codes of bounded synchronization delay in order to capture the group information. Let G be a finite group and $K = \bigcup_{g\in G} K_g \subseteq A^*$ be a disjoint union of a prefix code of bounded synchronization delay whereas all K_g are regular. With such a union we associate the *G-controlled star*

$$\{u_{g_1} \cdots u_{g_k} \in K^* \mid u_{g_i} \in K_{g_i} \wedge g_1 \cdots g_k = 1 \in G\}.$$

The *group-controlled star* is a subset of the usual Kleene star K^*, as in addition the word has to evaluate to the identity in G. More formally, one can consider the homomorphism $\gamma : K^* \to G$ which is induced by $\gamma(u) = g$ for $u \in K_g$. This is well-defined since the union $K = \bigcup_{g\in G} K_g$ is disjoint. The group-controlled star is given by the equation

$$\gamma^{-1}(1) = \{u_{g_1} \cdots u_{g_k} \in K^* \mid u_{g_i} \in K_{g_i} \wedge g_1 \cdots g_k = 1 \in G\}.$$

This can be lifted to infinite words as follows: Instead of evaluating the word itself to 1, infinitely many prefixes must evaluate to 1. In other words, the *G-controlled ω-power* is the ω-language $\overrightarrow{\gamma^{-1}(1)} = \gamma^{-1}(1)^\omega$.

Let $\mathcal{C}$ be a class of regular languages. We say that $\mathcal{C}$ is closed under G-controlled star (G-controlled ω-power) if for every disjoint union $K = \bigcup_{g\in G} K_g$ of a prefix code of bounded synchronization delay with $K_g \in \mathcal{C}$, the G-controlled star (G-controlled ω-power) is in $\mathcal{C}$ too. Let $\mathbf{H}$ be a variety of groups. The class $\mathcal{C}$ is closed under $\mathbf{H}$-controlled star ($\mathbf{H}$-controlled ω-power) if $\mathcal{C}$ is closed under G-controlled star (G-controlled ω-power) for every group $G \in \mathbf{H}$.

By $\mathrm{SD}_G(A^\infty)$ we denote the smallest class of regular languages such that the empty set $\emptyset$ and all singletons $\{a\}$ for $a \in A$ are contained in $\mathrm{SD}_G(A^\infty)$, the class $\mathrm{SD}_G(A^\infty)$ is closed under finite union and concatenation product, that is, $L, K \in \mathrm{SD}_G(A^\infty)$ implies $L \cup K$ and $(L \cap A^*) \cdot K$ are both in $\mathrm{SD}_G(A^\infty)$, and $\mathrm{SD}_G(A^\infty)$ is closed under G-controlled star and G-controlled ω-power.
We also define

$$\mathrm{SD}_G(A^*) = \{L \subseteq A^* \mid L \in \mathrm{SD}_G(A^\infty)\} \quad \text{and}$$
$$\mathrm{SD}_G(A^\omega) = \{L \subseteq A^\omega \mid L \in \mathrm{SD}_G(A^\infty)\}.$$

Remark 4.8. Note that $\{1\} \in \mathrm{SD}_G(A^\infty)$ since $\{1\}$ is the G-controlled star of the prefix code $K = \emptyset$. In particular, by closure under union and concatenation product, this yields that every finite language of finite words is in $\mathrm{SD}_G(A^\infty)$. $\diamond$

Choosing the prefix code $K = A$ of synchronization delay 0 and an arbitrary homomorphism $\gamma : A^* \to G$, we have $\gamma^{-1}(1) \in \mathrm{SD}_G(A^*)$ and $\gamma^{-1}(1)^\omega \in \mathrm{SD}_G(A^\omega)$. In particular, all group languages over G are contained in $\mathrm{SD}_G(A^\infty)$.

Unlike the case of star-free sets, the definition of $\mathrm{SD}_G(A^\infty)$ does not use any complementation. By induction: for $L \subseteq A^\infty$ we have $L \in \mathrm{SD}_G(A^\infty)$ if and only if we can write $L = L_1 \cup L_2$ with $L_1 \in \mathrm{SD}_G(A^*)$ and $L_2 \in \mathrm{SD}_G(A^\omega)$. In the special case where $G = \{1\}$ is the trivial group, we simply write SD instead of $\mathrm{SD}_{\{1\}}$. In this case closure under group-controlled star and group-controlled ω-power can be rephrased in simpler terms as follows: if $K \in \mathrm{SD}(A^*)$ is a prefix code of bounded synchronization delay, then $K^* \in \mathrm{SD}(A^*)$ and $K^\omega \in \mathrm{SD}(A^\omega)$.

In [Sch74] Schützenberger showed (using a different notation) $\mathrm{SD}_{\mathbf{H}}(A^*) \subseteq \overline{\mathbf{H}}(A^*)$, but the converse only for $\mathbf{H} \subseteq \mathbf{Ab}$, see Proposition 4.17 for the first inclusion. Our aim is to show $\overline{\mathbf{H}}(A^\infty) \subseteq \mathrm{SD}_{\mathbf{H}}(A^\infty)$ for all $\mathbf{H}$, cf. Theorem 4.11. We begin with a technical lemma.

Lemma 4.9. *Let $K \subseteq A^+$ be a prefix code of bounded synchronization delay and let $\gamma : K^* \to G$ be a homomorphism such that $\gamma^{-1}(g) \cap K \in \mathrm{SD}_G(A^*)$ for all $g \in G$, then we have $\gamma^{-1}(g) \in \mathrm{SD}_G(A^*)$ for all $g \in G$.*

Proof. For a word $w = u_1 \cdots u_k \in K^*$ we define $P(w) = \{\gamma(u_1 \cdots u_i) \mid 1 \le i \le k\} \subseteq G$ to be the set of prefixes of w in G. By an induction on $|P(w)|$ we construct languages $L(w) \in \mathrm{SD}_G(A^*)$ such that $w \in L(w) \subseteq \gamma^{-1}(\gamma(w))$ and the number $|\{L(w) \mid w \in K^*\}|$ of such languages is finite. The base case $|P(w)| = 0$ implies $g = 1$. We may choose $L(w) = \gamma^{-1}(1)$ and obtain $\gamma^{-1}(1) \in \mathrm{SD}_G(A^*)$ by definition. Hence, we may assume $|P(w)| \ge 1$. Let $g_1 = \gamma(u_1)$ and choose i maximal such that $g_1 = \gamma(u_1 \cdots u_i)$. Then we have $u_1 \cdots u_i \in (K \cap \gamma^{-1}(g_1)) \cdot \gamma^{-1}(1)$. Note that $P(w') = g_1^{-1} \cdot \{\gamma(u_1 \cdots u_j) \mid i < j \le k\}$ for $w' = u_{i+1} \cdots u_k$. By choice of i we have $g_1 \notin \{\gamma(u_1 \cdots u_j) \mid i < j \le k\}$ and therefore $|P(w')| = |\{\gamma(u_1 \cdots u_j) \mid i < j \le k\}| < |P(w)|$. By induction there exists $L(w')$ and we let $L(w) = (K \cap \gamma^{-1}(g_1)) \cdot \gamma^{-1}(1) \cdot L(w')$. It is straightforward to see that the number of $|\{L(w) \mid w \in K^*\}|$ of such languages is finite and bounded by $\sum_{i=0}^{|G|} |G|^i$. The result follows because we can write $\gamma^{-1}(g) = \bigcup \{L(w) \mid w \in \gamma^{-1}(g)\}$ and this is a finite union. $\square$

Lemma 4.10. $\mathrm{SD}_H(A^\infty) \subseteq \mathrm{SD}_G(A^\infty)$ *holds for* $H \preceq G$.

Proof. Inductively, it suffices to prove that $\mathrm{SD}_G(A^\infty)$ is closed under H-controlled star and closed under H-controlled ω-power. Let $K = \bigcup_{h\in H} K_h$ be a disjoint union of a prefix code of bounded synchronization delay such that $K_h \in \mathrm{SD}_G(A^\infty)$ for all $h \in H$ and $\gamma : K^* \to H$ be the homomorphism of the free monoid K^* to the group H such that $K_h = K \cap \gamma^{-1}(h)$ for all $h \in H$. We have to show $\gamma^{-1}(1), \gamma^{-1}(1)^\omega \in \mathrm{SD}_G(A^\infty)$. Without loss of generality we may assume that there exists a surjective homomorphism $\pi : G \to H$. Let $g_h \in G$ be elements such that $\pi(g_h) = h$. Let $\psi : K^* \to G$ be the homomorphism such that $\psi(u) = g_{\gamma(u)}$ for $u \in K$. By definition it holds $\gamma = \pi \circ \psi$ which implies $K \cap \psi^{-1}(g_h) = K \cap \gamma^{-1}(h) \in \mathrm{SD}_G(A^\infty)$ and $K \cap \psi^{-1}(g) = \emptyset$ if $g \neq g_h$ for all $h \in H$. Thus, $\psi^{-1}(1), \psi^{-1}(1)^\omega \in \mathrm{SD}_G(A^\infty)$ and by Lemma 4.9 we have $\psi^{-1}(g) \in \mathrm{SD}_G(A^\infty)$ for all $g \in G$. Note that

$$\gamma^{-1}(1) = \bigcup_{\pi(g)=1} \psi^{-1}(g) \quad \text{and}$$
$$\gamma^{-1}(1)^\omega = \bigcup_{\pi(g)=1} \psi^{-1}(g)\psi^{-1}(1)^\omega$$

which proves that $\gamma^{-1}(1), \gamma^{-1}(1)^\omega \in \mathrm{SD}_G(A^\infty)$. □

We formulate our results on the language classes $\mathrm{SD}_G(A^\infty)$ to obtain finer statements, however our main result then is formulated with the language class

$$\mathrm{SD}_{\mathbf{H}}(A^\infty) = \bigcup \{\mathrm{SD}_G(A^\infty) \mid G \in \mathbf{H}\}.$$

Note that Lemma 4.10 implies that $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ is the smallest class of regular languages such that $\emptyset \in \mathrm{SD}_{\mathbf{H}}(A^\infty)$, $\{a\} \in \mathrm{SD}_{\mathbf{H}}(A^\infty)$ for all letters $a \in A$, $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ is closed under finite union and concatenation, that is, $L, K \in \mathrm{SD}_{\mathbf{H}}(A^\infty)$ implies $L \cup K$ and $(L \cap A^*) \cdot K$ are both in $\mathrm{SD}_{\mathbf{H}}(A^\infty)$, and $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ is closed under $\mathbf{H}$-controlled star and $\mathbf{H}$-controlled ω-power.

The main result in this chapter is the following equality between $\mathrm{SD}_{\mathbf{H}}$, $\mathrm{Loc}_{\mathbf{H}}$ and $\overline{\mathbf{H}}$.

Theorem 4.11. *Let $L \subseteq A^\infty$ be a language and $\mathbf{H}$ a variety of finite groups. Then the following properties are equivalent:*

1. $L \in \mathrm{Loc}_{\mathbf{H}}(A^\infty)$.
2. $L \in \mathrm{SD}_{\mathbf{H}}(A^\infty)$.
3. $L \in \overline{\mathbf{H}}(A^\infty)$.

Since $\overline{\mathbf{H}}(A^\infty)$ is closed under complementation and intersection, this yields the following corollary.

Corollary 4.12. $\mathrm{Loc}_{\mathbf{H}}(A^\infty)$ *and* $\mathrm{SD}_{\mathbf{H}}(A^\infty)$ *are closed under complementation and intersection for every variety* $\mathbf{H}$ *of finite groups.*

Let $(\mathrm{FO} + \mathrm{MOD}_q)[<]$ be the fragment of first-order sentences which only use first-order quantifiers, modular quantifiers of modulus q and the order predicate $<$. Then the following corollary holds.

Corollary 4.13. $(\mathrm{FO} + \mathrm{MOD}_q)[<](A^\infty) = \mathrm{SD}_{\mathbf{Sol_q}}(A^\infty)$

Proof. By [STT95] (for infinite words) and [Str94] (for infinite words), it holds $(\mathrm{FO} + \mathrm{MOD}_q)[<](A^\infty) = \overline{\mathbf{Gsol_P}}(A^\infty)$ for $P = \left\{ d \in \mathbb{N} \;\middle|\; d \mid q^d \right\}$ the set of numbers dividing a power of q. Theorem 4.11 implies the stated equality. □

4.3 The inclusion $\overline{\mathbf{H}}(A^\infty) \subseteq \mathrm{Loc}_{\mathbf{H}}(A^\infty)$

We prove that if every subgroup of M is a divisor of G, then every language recognized by M is contained in $\mathrm{Loc}_G(A^\infty)$. This result is finer than just the inequality $\overline{\mathbf{H}}(A^\infty) \subseteq \mathrm{Loc}_{\mathbf{H}}(A^\infty)$. The proof works by induction on $|M|$ and on the alphabet and decomposes every $\approx_\varphi$-class into several sets in $\mathrm{Loc}_G(A^\infty)$.

Proposition 4.14. *Let $L \subseteq A^\infty$ be recognized by $\varphi : A^* \to M$ and let G be a group such that every subgroup of M is a divisor of G, then $L \in \mathrm{Loc}_G(A^\infty)$.*

Proof. Let $[\![w]\!]_\varphi = \{v \in A^\infty \mid w \approx_\varphi v\}$ be the equivalence class of w. Since L is recognized by φ, it holds $L = \cup_{w \in L} [\![w]\!]_\varphi$. Our goal is to construct languages $L(w) \in \mathrm{Loc}_G(A^\infty)$ such that

- $w \in L(w) \subseteq [\![w]\!]_\varphi$ and
- the number of such languages is bounded.

In particular, we want to saturate $[\![w]\!]_\varphi$ by sets in $\mathrm{Loc}_G(A^\infty)$. The construction of the set $L(w)$ is by induction on $(|M|, |A|)$ with lexicographic order.

If $w = 1$, then we set $L(w) = \{1\}$. This concludes the induction base $|A| = 0$. Let us consider the case that $\varphi(A^*)$ is a group, that is, a divisor of G. Then $L(w) = [\![w]\!]_\varphi \in \mathrm{Loc}_{\varphi(A^*)}(A^\infty) \subseteq \mathrm{Loc}_G(A^\infty)$ by Lemma 4.7. In particular, this case includes the induction base $|M| = 1$.

In the following we assume that $\varphi(A^*)$ is not a group and therefore there exists a letter $c \in A$ such that $\varphi(c)$ is not a unit. Fix this letter $c \in A$ and set $B = A \setminus \{c\}$. If $w \in B^\infty$, the set $L(w)$ exists by induction. Let $w = uv$ with $u \in B^*$ and $v \in cA^\infty$. By induction we obtain $L(u) \in \mathrm{Loc}_G(B^\infty) \subseteq \mathrm{Loc}_G(A^\infty)$. Our goal is to construct a language $L(v) \in \mathrm{Loc}_G(A^\infty)$. The construction of $L(v)$ below yields that we can choose $L(v) = cK$ for some language $K \in \mathrm{Loc}_G(A^\infty)$. Thus, setting $L(w) = L(u) \cdot L(v)$, we obtain $L(w) = L(u) \cdot L(v) \subseteq [\![u]\!]_\varphi [\![v]\!]_\varphi \subseteq [\![uv]\!]_\varphi$ and $L(w) \in \mathrm{Loc}_G(A^\infty)$. From now on it remains to construct $L(w)$ in the case $w \in cA^\infty$. By the same argument as above, we can further assume that either w is finite and ends with the letter c or there are infinitely many occurrences of c in w, i.e., we may assume $w \in c(B^*c)^\infty$.

Consider the alphabet $T = \varphi(B^*) = \{\varphi(u) \mid u \in B^*\}$. Let M_c be the local divisor of M at $\varphi(c)$. Since M_c is a divisor of M, every subgroup of M_c is a divisor of G. Consider

the homomorphism $\psi : T^* \to M_c$ given by $\psi(\varphi(u)) = \varphi(cuc)$ and the substitution $\sigma : (B^*c)^\infty \to T^\infty$ defined by $\sigma(u_1cu_2c\ldots) = \varphi(u_1)\varphi(u_2)\cdots$.

By induction on the monoid size, there exists a language $L(\sigma(v)) \in \mathrm{Loc}_G(T^\infty)$ for all $v \in (B^*c)^\infty$. We define $L(w) = c\sigma^{-1}(L(\sigma(v)))$ for $w = cv$. It is clear that $w \in L(w) \in \mathrm{Loc}_G(A^\infty)$ and therefore it remains to prove $L(w) \subseteq [\![w]\!]_\varphi$. Note that $cu \in L(w)$ implies $\sigma(u) \in L(\sigma(v))$ and thus $\sigma(u) \approx_\psi \sigma(v)$. Since $\approx_\psi$ is the transitive closure of $\sim_\psi$, we show that $\sigma(u) \sim_\psi \sigma(v)$ implies $cu \approx_\varphi cv$ for all $u, v \in (B^*c)^\infty$. Note that

$$\begin{aligned}\psi(\sigma(u_1cu_2c\ldots u_nc)) &= \psi(\varphi(u_1)\varphi(u_2)\cdots\varphi(u_n))\\ &= \varphi(cu_1c)\circ\varphi(cu_2c)\circ\cdots\circ\varphi(cu_nc)\\ &= \varphi(cu_1cu_2c\ldots cu_nc).\end{aligned}$$

Therefore, if $u, v \in (B^*c)^*$, we have $\varphi(cu) = \varphi(cv)$ and $cu \approx_\varphi cv$. Thus, we may assume $u, v \in (B^*c)^\infty$. Let $\sigma(u) = \sigma(u_1c)\sigma(u_2c)\cdots$ and $\sigma(v) = \sigma(v_1c)\sigma(v_2c)\cdots$ such that $\psi(\sigma(u_ic)) = \psi(\sigma(v_ic))$. As observed above, this implies $\varphi(cu_ic) = \varphi(cv_ic)$. Thus,

$$\begin{aligned}cu &= (cu_1c)u_2(cu_3c)u_4(c\cdots\\ &\sim_\varphi (cv_1c)u_2(cv_3c)u_4(c\cdots\\ &= cv_1(cu_2c)v_3(cu_4c)\cdots\\ &\sim_\varphi cv_1(cv_2c)v_3(cv_4c)\cdots\\ &= cv,\end{aligned}$$

which concludes the proof. □

4.4 The inclusion $\mathrm{Loc}_G(A^\infty) \subseteq \mathrm{SD}_G(A^\infty)$

Proposition 4.15. *Let G be a finite group and $L \in \mathrm{Loc}_G(A^\infty)$, then $L \in \mathrm{SD}_G(A^\infty)$. Moreover, L can be written as finite union*

$$L = L_0 \cup \bigcup_{i=1}^{m} L_i \cdot \gamma_i^{-1}(1)^\omega$$

for $L_i \in \mathrm{SD}_G(A^*)$ and $\gamma_i : K_i^* \to G$ for prefix codes $K_i \in \mathrm{SD}_G(A^*)$ of bounded synchronization delay with $\gamma_i^{-1}(g) \cap K_i \in \mathrm{SD}_G(A^*)$ for all $g \in G$. All products in the expressions L_i are unambiguous.

Proof. We prove this inductively on the levels i in the definition of

$$\mathrm{Loc}_G(A^\infty) = \bigcup_{i\in\mathbb{N}} \mathrm{Loc}_G^{(i)}(A^\infty).$$

For the induction base $i = 0$ consider a homomorphism $\varphi : A^* \to G$. Since every language recognized by φ is a finite union of $\approx_\varphi$-classes, it suffices to show that $[\![w]\!]_\varphi \in \mathrm{SD}_G(A^\infty)$ for all $w \in L$.

The alphabet A is a prefix code of synchronization delay 0. The homomorphism φ induces a disjoint union $A = \cup_{g\in G}(A \cap \varphi^{-1}(g))$ and $A \cap \varphi^{-1}(g) \in \mathrm{SD}_G(A^\infty)$ by Remark 4.8. This shows $\varphi^{-1}(g) \in \mathrm{SD}_G(A^*)$ for all $g \in G$ by Lemma 4.9 and Lemma 4.10. Therefore, if $w \in A^*$, then $[\![w]\!]_\varphi = \varphi^{-1}(\varphi(w)) \in \mathrm{SD}_G(A^\infty)$. For $w \in A^\omega$ we have $w \in \varphi^{-1}(g)\varphi^{-1}(1)^\omega \in \mathrm{SD}_G(A^\infty)$ for some $g \in G$.[2] Since $\varphi^{-1}(g)\varphi^{-1}(1)^\omega \subseteq [\![w]\!]_\varphi$ and there are only $|G|$ sets of this type, $[\![w]\!]_\varphi$ is a finite union of sets in $\mathrm{SD}_G(A^\infty)$ and thus $[\![w]\!]_\varphi \in \mathrm{SD}_G(A^\infty)$.

Consider the case $i > 0$. By induction we obtain $\mathrm{Loc}_G^{(i-1)}(A^\infty) \subseteq \mathrm{SD}_G(A^\infty)$ for all alphabets A. Note that $\mathrm{SD}_G(B^\infty) \subseteq \mathrm{SD}_G(A^\infty)$ for $B = A \setminus \{c\}$ and $\mathrm{SD}_G(A^\infty)$ is closed under union and concatenation product. Let $g : B^* \to T$ be a function with $g^{-1}(t) \in \mathrm{Loc}_G^{(i-1)}(B^\infty) \subseteq \mathrm{SD}_G(B^\infty)$. Consider the mapping $\sigma : (B^*c)^\infty \to T^\infty$ given by $\sigma(u_1cu_2c\cdots) = g(u_1)g(u_2)\cdots$. It remains to show $\sigma^{-1}(K) \in \mathrm{SD}_G(A^\infty)$ for all $K \in \mathrm{Loc}_G^{(i-1)}(T^\infty) \subseteq \mathrm{SD}_G(T^\infty)$. We show this inductively on the definition of SD_G.

For $K = \emptyset$, we obtain $\sigma^{-1}(K) = \emptyset \in \mathrm{SD}_G(A^\infty)$. Furthermore, $\sigma^{-1}(t) = g^{-1}(t) \in \mathrm{SD}_G(A^\infty)$. Let $L, K \in \mathrm{SD}_G(T^\infty)$. The equation $\sigma^{-1}(L \cup K) = \sigma^{-1}(L) \cup \sigma^{-1}(K)$ holds. Let $\sigma(v) = w_1w_2$ for some $v \in (B^*c)^*$. Since B^*c is a prefix code, there exists a unique factorization $v = v_1v_2$ with $v_1, v_2 \in (B^*c)^*$ such that $\sigma(v_1) = w_1$ and $\sigma(v_2) = w_2$. Thus, we conclude $\sigma^{-1}(L \cdot K) = \sigma^{-1}(L) \cdot \sigma^{-1}(K)$. Note that $\sigma^{-1}(L) \cdot \sigma^{-1}(K)$ is unambiguous if $L \cdot K$ is unambiguous.

Let $K \in \mathrm{SD}_G(T^\infty)$ be a prefix code of synchronization delay d. We first show that $\sigma^{-1}(K)$ is a prefix code of bounded synchronization delay. Let $u, uv \in \sigma^{-1}(K)$, then $\sigma(u), \sigma(uv) = \sigma(u)\sigma(v) \in K$ and therefore $\sigma(v) = 1$. This implies $v = 1$ and $\sigma^{-1}(K)$ is a prefix code. We prove that $\sigma^{-1}(K)$ has synchronization delay $d+1$. The incrementation of the synchronization delay by one comes from the fact that B^*c is not a suffix code, and we need another word in B^*c to act as a left marker. Consider $uvw \in \sigma^{-1}(K)^*$ with $v \in \sigma^{-1}(K)^{d+1}$ and factorize $v = v_1cv_2$ with $v_2 \in \sigma^{-1}(K)^d = \sigma^{-1}(K^d)$. Then $\sigma(uvw) = \sigma(uv_1c)\sigma(v_2)\sigma(w)$, and by $\sigma(v_2) \in K^d$ this implies $\sigma(uv) = \sigma(uv_1c)\sigma(v_2) \in K^*$. Thus, $uv \in \sigma^{-1}(K)^*$.

Let $\gamma : K^* \to G$ be some homomorphism and $K_g = K \cap \gamma^{-1}(g) \in \mathrm{SD}_G(T^\infty)$ for all $g \in G$. Inductively, $\sigma^{-1}(K_g) \in \mathrm{SD}_G(A^\infty)$ and $\sigma^{-1}(K) = \bigcup \sigma^{-1}(K_g)$. Let $\gamma' : \sigma^{-1}(K)^* \to G$ be induced by $\gamma'(u) = \gamma(\sigma(u))$. By definition of $\mathrm{SD}_G(A^\infty)$ we obtain $\gamma'^{-1}(1) \in \mathrm{SD}_G(A^\infty)$. However, $u_1 \cdots u_n \in \sigma^{-1}(\gamma^{-1}(1))$ if and only if $\gamma(\sigma(u_1 \cdots u_n)) = 1$. Furthermore, note that

$$\begin{aligned}\gamma(\sigma(u_1 \cdots u_n)) &= \gamma(\sigma(u_1)) \cdots \gamma(\sigma(u_n)) \\ &= \gamma'(u_1) \cdots \gamma'(u_n) \\ &= \gamma'(u_1 \cdots u_n).\end{aligned}$$

Thus, we obtain

$$\begin{aligned}\sigma^{-1}(\gamma^{-1}(1)) &= \gamma'^{-1}(1) \in \mathrm{SD}_G(A^\infty) \text{ and} \\ \sigma^{-1}(\gamma^{-1}(1)^\omega) &= \gamma'^{-1}(1)^\omega \in \mathrm{SD}_G(A^\infty).\end{aligned}$$

[2] Note that the product $\varphi^{-1}(g)\varphi^{-1}(1)^\omega$ is not unambiguous. This is the reason that the unambiguity is only stated for the languages L_i.

This concludes the proof of $\mathrm{Loc}_G^{(i)}(A^\infty) \subseteq \mathrm{SD}_G(A^\infty)$. □

Remark 4.16. Let $\mathcal{C}(A^*)$ be the least Boolean algebra closed under marked product and under star operation restricted to languages of the form K^n, where $n > 0$ has only prime factors in P and $K \in \mathcal{C}(A^*)$ is a prefix code of bounded synchronization delay. Using the proof scheme of Proposition 4.15 we prove that $\mathrm{Loc}_G(A^*) \subseteq \mathcal{C}(A^*)$ for a group $G \in \mathbf{Ab_P}$; the difficult part of Theorem 4.4.

For the induction base we consider group languages recognized by a group $G \in \mathbf{Ab_P}$. By Lemma 2.8 the languages recognized by G are Boolean combinations of languages of the form $\{w \in A^* \mid |w|_a \equiv i \bmod n\}$ for $n \in P$. Note that $K = B^*a$ for $B = A \setminus \{a\}$ is a prefix code of synchronization delay 1. Thus, $(K^n)^* \in \mathcal{C}(A^*)$ which implies

$$\{w \in A^* \mid |w|_a \equiv i \bmod n\} = (K^n)^* \cdot K^i \in \mathcal{C}(A^*).$$

For the inductive step, we show $\sigma^{-1}(L) \in \mathcal{C}(A^*)$ for $L \in \mathrm{Loc}_G^{(i-1)}(T^*) \subseteq \mathcal{C}(T^*)$. The only case not yet covered in the proof of Proposition 4.15 is $(K^n)^* \in \mathcal{C}(T^*)$ for a prefix code $K \in \mathcal{C}(T^*)$ of bounded synchronization delay. Again, $\sigma^{-1}(K) \in \mathcal{C}(A^*)$ is a prefix code of bounded synchronization delay and

$$\sigma^{-1}((K^n)^*) = (\sigma^{-1}(K)^n)^* \in \mathcal{C}(A^*). \qquad \diamond$$

4.5 Closure properties of $\mathrm{SD}_{\mathbf{H}}$

Proposition 4.17 ([Sch74])**.** *Let G be a finite group and the disjoint union $K = \bigcup_{g\in G} K_g \subseteq A^+$ be a prefix code of bounded synchronization delay for regular languages K_g. Then the subgroups in the syntactic monoid of the G-controlled star are either divisors of G or of the direct product $\prod_{g\in G} \mathrm{Synt}(K_g)$.*

The statement has been proved by Schützenberger, however the presentation of his proof was very short. Therefore, we give a detailed proof following the proof of [Sch74] loosely.

Proof. Let $\gamma : K^* \to G$ be the homomorphism from the free submonoid K^* to the group G such that $\gamma^{-1}(g) \cap K = K_g$ for all $g \in G$.

Without restriction we may assume $K \neq \emptyset$ and we let d be the synchronization delay of K. For $g \in G$ let Q_g be the state set of the minimal automaton for K_g and q_g the corresponding initial state. Let $Q = \prod_{g\in G} Q_g$ be the direct product of sets Q_g with initial state $q_0 = \prod\{q_g \mid g \in G\}$. The product automaton allows to assign to each language K_g a subset $F_g \subseteq Q$ such that the deterministic finite automaton $(Q, A, \cdot, q_0, F_g)$ accepts K_g. Since $K_g \cap K_h = \emptyset$ for $g \neq h$ we have $F_g \cap F_h = \emptyset$ for $g \neq h$. Since $\mathrm{Synt}(K_g)$ acts on Q_g, it is clear that $\prod_{g\in G} \mathrm{Synt}(K_g)$ acts on Q.

By F we denote the union $\bigcup\{F_g \mid g \in G\}$. The set of states $\{p \in Q \mid p \cdot A^* \cap F = \emptyset\}$, which cannot reach a final state, can be merged into a single sink state $\perp$. Since K is a prefix code, there is no word $u \in A^+$ such that $p \cdot u \in F$ for any $p \in F$. Thus, $p \cdot u = \perp$ for every $p \in F$ and $u \in A^+$. Moreover, without restriction we may assume

that every state is reachable from the initial state q_0 and by slight abuse of language, the new state space is still called Q.

Let $S = \mathrm{TM}(Q) = \{\sigma_u \mid u \in A^*\}$ with $\sigma_u : Q \to Q, p \mapsto p \cdot u$ be the transition monoid of Q. The monoid S becomes a divisor of $\prod_{g \in G} \mathrm{Synt}(K_g)$. It is therefore enough to show that every subgroup in the syntactic monoid $\mathrm{Synt}(\gamma^{-1}(1))$ is either a divisor of G or a divisor of S. For later use we denote by $\sigma : A^* \to S$ the homomorphism which maps u to σ_u.

Next, consider the product set $\widetilde{Q} = G \times (Q \setminus F)$. We view $\widetilde{Q}$ as a state space of an automaton accepting $\gamma^{-1}(1)$ as follows:

$$(g, q) \cdot a = \begin{cases} (g, q \cdot a) & \text{if } q \cdot a \in Q \setminus F \\ (gh, q_1) & \text{if } q \cdot a \in F_h \end{cases}$$

Note that the transition function is well-defined since, as mentioned above, $F_g \cap F_h = \emptyset$ for $g \neq h$. Again, this yields a homomorphism $\mu : A^* \to M$ into the transition monoid $M = \mathrm{TM}(\widetilde{Q})$ of $\widetilde{Q}$. Moreover, letting $(1, q_1) \in \widetilde{Q}$ be the only initial and final state, the resulting deterministic finite automaton $(\widetilde{Q}, A, \cdot, (1, q_1), \{(1, q_1)\})$ accepts $\gamma^{-1}(1)$ as a subset of A^*. To see this observe that every word $u \in \gamma^{-1}(1)$ belongs to $K^* \subseteq A^*$. Moreover, u admits a unique factorization $u = u_1 \cdots u_k$ such that for all i we have $q_0 \cdot u_i \in F_{g_i}$ for $g_i = \gamma(u_i)$ and $1 = g_1 \cdots g_k$. Since the automaton accepts $\gamma^{-1}(1)$, it is enough to show that every subgroup of M is either a subgroup of G or a divisor of S.

Let H be a subgroup of M. Then H contains a unique idempotent $e \in M$ which is the neutral element in H. In particular, $H = eHe$. Let $\mathcal{H} = \mu^{-1}(H)$. It is a nonempty subsemigroup of A^*. The group H does not act as a group on $\widetilde{Q}$, because there might be states (g, p) such that $(g, p) \neq (g, p) \cdot e$. However, it acts faithfully on $\widetilde{Q}_e = \widetilde{Q} \cdot e$. Indeed, if $h \neq h'$ in H, then there are states $(g, p) \cdot h \neq (g, p) \cdot h'$. Since $h = ehe$ and $h' = eh'e$, we have $(g, p) \cdot e \in \widetilde{Q}_e$, $(g, p) \cdot eh \neq (g, p) \cdot eh'$, and $(g, p) \cdot eh, (g, p) \cdot eh' \in \widetilde{Q}_e$. We distinguish two cases.

Case 1. *There is a state $(g, p) \in \widetilde{Q}_e$ such that there is a word $uv \in \mathcal{H}$ where $p \cdot u \in F$.*

For $w = (uv)^{|H|}$ we have $\mu(w) = e$ and w factorizes as $w = uw'x$ such that $w' \in K^*$ and $q_0 \cdot x = p$. It follows $xu \in K$. Letting $y = wuw'$ we have $yx = w^2 \in \mathcal{H}$ with $\mu(yx) = e$ and hence, $(g, q_0) \cdot x = (g, p)$ implies $(g, p) \cdot y = (g, q_0)$.

The element $\mu(xy)$ is idempotent in M. Indeed, calculating in M we have:

$$(xy)^2 = xwuw' \cdot xwuw' = xw^3uw' = xwuw' = xy.$$

The subsemigroup $H' = xHy$ contains the idempotent xy and $f \mapsto xfy$ defines a homomorphism of H onto the group H' and its inverse is given by $xfy \mapsto yxfyx = f$. As H and H' are isomorphic, we start all over with the idempotent $e' = \mu(xy)$, the group H', and its inverse image $\mathcal{H}'$ instead of $e, H, \mathcal{H}$.

In order to simplify the notation we rename $e', H', \mathcal{H}'$ as $e, H, \mathcal{H}$. The difference is that, now, we have $(g, q_0) \cdot e = (g, q_0)$ and $\mu(xy) = e$ with $xy \in K^+$. Consider $(g, q) \in \widetilde{Q}_e$ such that $q \neq \perp$ and hence, q is not the sink state of Q. Then there exist words $u, v \in A^*$ such that $q_0 \cdot u = q$ and $q \cdot v \in F$. Since $(g, q) = (g, q_0) \cdot u \in \widetilde{Q}_e$, we obtain

$(g, q_0) \cdot u(xy)^d v = (g, q) \cdot v = (g', q_0)$ for some $g' \in G$. Consequently, $u(xy)^d v \in K^*$ and, by synchronization delay, we obtain $u(xy)^d \in K^*$. In particular, $(g, q_0) \cdot u(xy)^d = (g, q_0)$. Thus, $(g, q) = (g, q) \cdot (xy)^d = (g, q_0)u(xy)^d = (g, q_0)$ and therefore, $q = q_0$. Thus,

$$\widetilde{Q}_e \subseteq \{(g, q_0) \mid g \in G\} \cup \{(g, \perp) \mid g \in G\}.$$

This implies $\mathcal{H} \subseteq K^*$ by the definition of the automaton. (The group H acts trivially on $\{(g, \perp) \mid g \in G\}$ and this part is irrelevant in the following.)

Consider the mapping $\pi : H \to G$ given by $\pi(\mu(u)) = \gamma(u)$ for $u \in \mathcal{H}$. This mapping is well-defined, since $(g, q_0) \cdot \mu(u) = (g \cdot \gamma(u), q_0)$ for some $(g, q_0) \in \widetilde{Q}_e$. Thus, the homomorphism $\gamma : \mathcal{H} \to G$ factorizes as follows:

$$\gamma : \mathcal{H} \xrightarrow{\mu} H \xrightarrow{\pi} G.$$

Let us show that the homomorphism π is injective. We know that H acts faithfully on $\widetilde{Q}_e$. Hence, for $h \neq 1$ there is some $(g, q) \in \widetilde{Q}_e$ such that $(g, q) \cdot h \neq (g, q)$. Since H acts trivially on $(g, \perp)$, we must have $q = q_0$ and

$$(g\pi(h), q_0) = (g, q_0) \cdot h \neq (g, q_0).$$

This shows, as desired, $\pi(h) \neq 1$ and H is a subgroup of G.

Case 2. *For every state* $(g, p) \in \widetilde{Q}_e$ *and every* $uv \in \mathcal{H}$ *we have* $p \cdot u \notin F$.

Thus, for all $(g, p) \in \widetilde{Q}_e$ and all $u \in \mathcal{H}$ we have

$$(g, p) \cdot \mu(u) = (g, p \cdot u) = (g, p \cdot \sigma(u)).$$

This means that H acts faithfully on the set

$$Q' = \left\{ p \in Q \;\middle|\; (g, p) \in \widetilde{Q}_e \right\}.$$

Let S' denote the submonoid $S' = \{s \in S \mid Q' \cdot s \subseteq Q'\}$, then $\sigma(\mathcal{H}) \subseteq S'$ and H becomes a quotient of S' and therefore, a divisor of S. This concludes the proof. □

We will prove the same result for $\gamma^{-1}(1)^\omega$, relying on Proposition 4.17 as a black box result. The concept used for transferring the properties to infinite words are Birget-Rhodes expansions [BR84, BR89]. The *Birget-Rhodes expansion* of a monoid M is the monoid

$$\mathrm{Exp(M)} = \{(X, m) \mid 1, m \in X \subseteq M\}.$$

The multiplication on Exp(M) is given as a semi-direct product:

$$(X, m) \cdot (Y, n) = (X \cup m \cdot Y, m \cdot n).$$

Note that M is isomorphic to the submonoid $\{(M, m) \mid m \in M\}$ of Exp(M), that is, M is a divisor of Exp(M). Moreover, the following lemma shows that the Birget-Rhodes expansion has the same groups as M.

Lemma 4.18. *Every group contained in* Exp(M) *is isomorphic to some group in* M*.*

Proof. Let $G \subseteq \mathrm{Exp(M)}$ be a group contained in Exp(M) and let $(X, e) \in G$ be the identity in G. For every element $(Y, m) \in G$ we have $(X, e)(Y, m) = (X \cup eY, em) = (Y, m)$ and thus $X \subseteq Y$. Furthermore, by Lagrange's theorem $(Y, m)^{|G|} = (Y \cup \ldots, m^{|G|}) = (X, e)$ and we conclude $X = Y$. Thus, $G \subseteq \{(X, m) \mid m \in M\}$ and $(X, m) \mapsto m$ is an injective embedding of G in M. □

The idea behind the Birget-Rhodes expansion is that it stores the seen prefixes in a set.

Lemma 4.19. *Let* $\varphi : A^* \to M$ *be a homomorphism and* $\psi : A^* \to \mathrm{Exp(M)}$ *be the homomorphism given by* $\psi(a) = (\{1, \varphi(a)\}, \varphi(a))$*. Let* $u \in A^*$ *and* $\psi(u) = (X, \varphi(u))$*. For every* $m \in X$ *there exists a prefix* v *of* u *such that* $\varphi(v) = m$*.*

Proof. The statement is true if u is the empty word. Thus, consider $u = va$ for some letter $a \in A$. Let $\psi(v) = (Y, \varphi(v))$, then

$$\psi(u) = \psi(v) \cdot (\{1, \varphi(a)\}, \varphi(a)) = (Y \cup \{\varphi(v), \varphi(v)\varphi(a)\}, \varphi(u)).$$

Inductively, we obtain prefixes of v, and therefore prefixes of u, for all elements of Y. The only (potentially) new element in X is $\varphi(u)$. This proves the claim. □

Proposition 4.20. *Let* $L \subseteq A^*$ *be some regular language and* $\varphi : A^* \to M$ *be a homomorphism which recognizes* L*, then* $\overrightarrow{L}$ *is recognized by* Exp(M)*.*

Proof. Let $\psi : A^* \to \mathrm{Exp(M)}$ be the homomorphism given by $\psi(a) = (\{1, \varphi(a)\}, \varphi(a))$. Let $u \in \overrightarrow{L}$ and $u \sim_\psi v$. We show that $v \in \overrightarrow{L}$. Let $u = u_1 u_2 \cdots$ and $v = v_1 v_2 \cdots$ be factorizations such that $\psi(u_i) = \psi(v_i)$. Since $u \in \overrightarrow{L}$, infinitely many prefixes of u are in L. Thus, by merging some u_i's, we may assume that for every i there exists a decomposition $u_i = u_i' u_i''$ such that $u_1 \cdots u_{i-1} u_i' \in L$. By $\psi(u_i) = \psi(v_i)$ and Lemma 4.19, there exists a decomposition $v_i = v_i' v_i''$ such that $\varphi(u_i') = \varphi(v_i')$. Thus, $u_1 \cdots u_{i-1} u_i' \sim_\varphi v_1 \cdots v_{i-1} v_i'$ and therefore $v_1 \cdots v_{i-1} v_i' \in L$. This implies $v \in \overrightarrow{L}$. □

Proposition 4.21. *If* $L \in \mathrm{SD}_G(A^\infty)$*, then all subgroups in* Synt(L) *are a divisor of a direct product of copies of* G*.*

Proof. We will prove this inductively on the definition of $\mathrm{SD}_G(A^\infty)$. The cases $\emptyset \in \mathrm{SD}_G(A^\infty)$ and $\{a\} \in \mathrm{SD}_G(A^\infty)$ for all letters $a \in A$ are straightforward, as they are recognized by aperiodic monoids. Let L, K be languages, such that their syntactic monoids contain only groups which are divisors of a direct product of G. The language $L \cup K$ is recognized by the direct product of their syntactic monoids which implies the statement. Let M be a monoid which recognizes both L and K. As the direct product of the syntactic monoids of L and K satisfies this, we may assume that M contains only groups which are divisors of a direct product of G. By Proposition 2.10, the Schützenberger product of M recognizes $(L \cap A^*) \cdot K$ and by Proposition 2.11 the Schützenberger product of M contains only groups which are also contained in M. Let

$K \subseteq A^+$ be a prefix code of bounded synchronization delay and $\gamma : K^* \to G$ be a homomorphism such that for all $g \in G$ the code $K_g = K \cap \gamma^{-1}(g)$ is in $\mathrm{SD}_G(A^*)$. By induction we may assume that every subgroup of $\mathrm{Synt}(K \cap \gamma^{-1}(g))$ is a divisor of a direct product of copies of G. Proposition 4.17 implies that every subgroup of $\mathrm{Synt}(\gamma^{-1}(1))$ is a divisor of a direct product of copies of G. This concludes the case of closure under G-controlled star. For G-controlled ω-powers note that $\gamma^{-1}(1)^\omega = \overrightarrow{\gamma^{-1}(1)}$ and therefore Proposition 4.20 and Lemma 4.18 imply that every subgroup of $\mathrm{Synt}(\gamma^{-1}(1)^\omega)$ is a divisor of a direct product of copies of G. □

Chapter 5

Church-Rosser congruential languages

In this chapter we study the class of *Church-Rosser congruential languages*. A language L is Church-Rosser congruential if there exists a Church-Rosser system S such that L is a finite union of equivalence classes $[u]_S$. We write CRCL for the class of Church-Rosser congruential languages. Let $\varphi : A^* \to M$ be a homomorphism and $S \subseteq A^* \times A^*$ be a semi-Thue system. We say that φ *factorizes through* S if for all $u \underset{S}{\Longrightarrow} v$ it holds $\varphi(u) = \varphi(v)$, that is, equivalence classes of S map to the same element in M. We also say that S is φ-*invariant* if φ factorizes through S. This notion is algebraically motivated. Let S be a semi-Thue system such that φ factorizes through S, then $\psi : A^*/S \to \varphi(A^*)$ given by $\psi([u]_S) = \varphi(u)$ is a well-defined homomorphism. Let $\pi_S : A^* \to A^*/S$ be the natural projection and L be some language which is recognized by φ and π_L be the syntactic homomorphism of L. Then we obtain the situation in Figure 5.1. Since φ factorizes through S if and only if $\varphi : A^* \to \varphi(A^*)$ factorizes through S, we may assume that φ is surjective. If further S is a Church-Rosser system, we call A^*/S a *Church-Rosser representation* of φ (or M). We are especially interested in the case that S has finite index. We call a language *strongly Church-Rosser congruential* if there exists a Church-Rosser system S of finite index such that L is a (finite) union of equivalence classes $[u]_S$. In other words, a language is strongly Church-Rosser congruential if it is recognized by the natural homomorphism $\pi_S : A^* \to A^*/S$ for a Church-Rosser representation A^*/S of finite index. In particular, every language recognized by the syntactic monoid of a strongly Church-Rosser congruential language is strongly Church-Rosser congruential. The class of strongly Church-Rosser congruential languages is denoted by sCRCL, see [NW02, Nie02] for the original definition. Since the index of S is finite and π_S

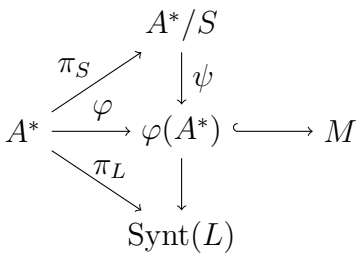


Figure 5.1: Algebraic situation of φ factorizes through S [DKRW15]

recognizes L, we obtain sCRCL $\subseteq$ REG. In this chapter we will prove the converse, that is, sCRCL = REG. This result, especially Sections 5.2, 5.3, 5.4 and 5.6, is taken from [DKRW15]. The rest of this chapter is not published yet. In Subsection 5.5.1 it is shown that every language in **Ab** is a union of equivalence classes of a Parikh-reducing Church-Rosser system S of finite index. Using the machinery of Theorem 5.31, this yields the same result for $\overline{\mathbf{Ab}}$. Furthermore, the construction yields a system S such that the groups in the Church-Rosser representation A^*/S of M already appear in M or are cyclic. In Subsection 5.5.2 we construct a Parikh-reducing Church-Rosser system S of finite index for every homomorphism $\varphi : \{a, b\}^* \to G$ for G a group. In Section 5.7 we study the size of a Church-Rosser representation A^*/S for a monoid M in relation to the size of M.

5.1 Previous Work

The study of Church-Rosser congruential languages was initiated by Narendran in his PhD thesis [Nar84]. This lead to the Journal of the ACM publication [MNO88] together with McNaughton and Otto. In this paper they also introduced the class of Church-Rosser languages CRL. The class of Church-Rosser languages is more general than CRCL, in particular every deterministic context-free language is in CRL [MNO88]. More precisely, CRL is the class of deterministic growing context-sensitive languages [NO05]. The class of Church-Rosser languages is well-understood, see e.g. [BO98, Nar84, Woi01, Woi03]. The progress on Church-Rosser congruential languages was much slower. The main question raised by [MNO88] is whether all regular languages are Church-Rosser congruential. The first partial result on this is on regular languages of polynomial density. Let $L \subseteq A^*$ be a language, then $\rho_L(n) = \left|A^{\leq n} \cap L\right|$ is the density function of L. We say that L has polynomial density if $\rho_L(n) \in \mathcal{O}(n^k)$ for some $k \in \mathbb{N}$.

Theorem 5.1 ([Nie00])**.** *Every regular language of polynomial density is Church-Rosser congruential.*

A language $L \subseteq A^*$ is *piecewise testable*[1] if it is a Boolean combination of languages of the form $A^*a_1A^* \cdots a_nA^*$ for $a_1, \ldots, a_n \in A$.

Theorem 5.2 ([NW02])**.** *The following results hold:*

- *Every piecewise testable language is in* sCRCL*.*
- *For every finite alphabet A the language $(A^2)^*$ is in* sCRCL*.*

An overview of these two results can be found in the doctoral thesis of Niemann [Nie02]. The languages $(A^2)^*$ are group languages for $\mathbb{Z}/2\mathbb{Z}$, that is, they are a preimage of the homomorphism $\varphi : A^* \to \mathbb{Z}/2\mathbb{Z}$ given by $\varphi(a) = 1$ for all $a \in A$. In 2003 a more advanced result was announced by Reinhardt and Thérien.

[1] This is exactly level 1 of the Straubing-Thérien hierarchy, which exhausts the aperiodic languages [CB71].

Theorem 5.3 ([RT03])**.** *All group languages are strongly Church-Rosser congruential.*

Unfortunately, this result was never published as a refereed paper and the presentation had some flaws. Having this result at the back of their mind, Diekert, Kufleitner and Weil studied group-free languages.

Theorem 5.4 ([DKW12])**.** *All aperiodic languages are strongly Church-Rosser congruential.*

The main two ingredients in the proof that all aperiodic languages are in sCRCL are the use of local divisors and the fact that they showed a stronger statement: all aperiodic languages can be saturated by a subword-reducing Church-Rosser system of finite index.

5.2 Examples and easy cases

In this section we consider some special cases for which the construction of a Church-Rosser representation is easy. In particular, we will see that the case of simple groups is surprisingly easy to solve.

Example 5.5. Consider the following two languages $L_1 = \{a^n b^n \mid n \geq 1\}$ and $L_2 = a(ba)^*$ over the two-letter alphabet $A = \{a, b\}$. The language L_1 is non-regular but deterministic context-free whereas L_2 is regular. The first language L_1 is Church-Rosser congruential. The corresponding system is $S_1 = \{a^2b^2 \to ab\}$; and we have $L_1 = [ab]_{S_1}$.

The complement of L_1 is not Church-Rosser congruential. Indeed assume that S' is a Church-Rosser system such that we can write $A^* \setminus L_1$ as a finite union of congruence classes. Then some congruence class must contain words $a^k b$ and $a^m b$ with $k > m \geq 1$. But then $a^k b^m$ and $a^m b^m$ share the same class, too. This is impossible since $a^k b^m \notin L_1$ and $a^m b^m \in L_1$.

Consider $L_2 = a(ba)^*$. It is Church-Rosser congruential due to the system $S_2 = \{aba \to a\}$. With respect to S_2 all words a^n are irreducible. In particular, the monoid A^*/S_2 is infinite. Hence, S_2 has infinite index. An explicit Church-Rosser system T for L_2 of finite index has been constructed in [DKW12]. It is given by

$$\begin{aligned} T = \{\ & bbb \to bb,\ bba \to bb,\ abb \to bb,\ bab \to b, \\ & aaa \to bb,\ aab \to bb,\ baa \to bb,\ aba \to a\}. \end{aligned}$$

The monoid $\{a, b\}^*/T$ has seven elements: $[1]_T$, $L_2 = [a]_T$, $[b]_T$, $[ab]_T$, $[ba]_T$, $[aa]_T$, and $[bb]_T$. It is not the smallest monoid recognizing L_2, because aa and bb behave as a "zero" and could be identified. The smallest monoid recognizing L_2 is its syntactic monoid and has 6 elements. ◇

Let us next consider the situation for a unary alphabet $A = \{a\}$. Let $\varphi : A^* \to M$ be a surjective homomorphism onto a finite monoid M. Since φ is surjective and

$|A| = 1$, the monoid M is generated by $\varphi(a)$. By finiteness of M, we obtain $M = \{1, \varphi(a), \ldots, \varphi(a)^{i-1}\}$ for some $i \in \mathbb{N}$ and there exists some $0 \leq j < i$ such that $\varphi(a)^i = \varphi(a)^j$. The system $S = \{a^i \to a^j\}$ is confluent and subword-reducing. Obviously, S factorizes through φ, and even stronger, $A^*/S \simeq M$ and the natural projection $\pi : A^* \to A^*/S$ is essentially the homomorphism φ. Thus, the case for a unary alphabet is easy to solve. We will reuse this case as the base case for induction later.

For the rest of the section we study Church-Rosser representation of groups. We consider the case that for a weighted alphabet $(A, \|\cdot\|)$ and a homomorphism $\varphi : A^* \to M$ there exist words $v_m \in A^*$ for $m \in M$ such that $\varphi(v_m) = m$ and $\|v_m\| = \|v_{m'}\|$ for all $m, m' \in M$. Then one can consider the rules $w \to v_{\varphi(w)}$ for all words w which have greater weight than v_m. However, this are infinitely many rules and therefore one has to cut down the number of rules to a finite number. Since φ is a homomorphism, one can restrict the words w to those of length at most $\|v_m\| + \max\{\|a\| \mid a \in A\}$. This is a generalization of the proof technique used by [NW02] in order to prove Theorem 5.2.[2] One possible way to obtain such normal forms v_m is the padding technique which is used in the next proposition. This proposition has been observed in [DKRW15] for finite groups, but also holds for finite monoids.

Proposition 5.6. *Let $(A, \|\cdot\|)$ be a weighted alphabet and $\varphi : A^* \to M$ be a surjective homomorphism onto a finite monoid M. If*

$$\gcd\{\|w\| \mid \varphi(w) = 1\} = \gcd\{\|a\| \mid a \in A\},$$

then there exists a weighted Church-Rosser system S of finite index which factorizes through φ. Moreover, every group contained in A^*/S is contained in M too.

Proof. Let $\gcd\{\|w\| \mid \varphi(w) = 1\} = \gcd\{\|a\| \mid a \in A\} = q$ for some $q \in \mathbb{N}$. By Bézout's lemma, there exist words $u, v \in A^*$ such that $\varphi(u) = \varphi(v) = 1$ and $\|u\| - \|v\| = q$. Let $v_m \in A^*$ for $m \in M$ be words such that $\varphi(v_m) = m$. By padding the words v_m of smallest weight by u and every other word $v_{m'}$ of larger weight by v, we obtain after finitely many steps a set of words v_m such that $\varphi(v_m) = m$ and their weights $\|v_m\|$ are the same for all $m \in M$. Let $d = \|v_m\|$ be the common weight of all v_m. Consider the semi-Thue system

$$S = \left\{ w \to v_{\varphi(w)} \;\middle|\; d < \|w\| \leq d + \max\{\|a\| \mid a \in A\} \right\}.$$

By definition of the rules, the system S is weight-reducing. We show inductively that $w \overset{*}{\underset{S}{\Longrightarrow}} v_{\varphi(w)}$ for all words with $\|w\| > d$. This is true by definition if $\|w\| \leq d + \max\{\|a\| \mid a \in A\}$. If $\|w\| > d + \max\{\|a\| \mid a \in A\}$, then there exists a factorization $w = w'w''$ such that $d < \|w'\| \leq d + \max\{\|a\| \mid a \in A\}$. Then $w \underset{S}{\Longrightarrow} v_{\varphi(w')}w''$ and inductively $v_{\varphi(w')}w'' \overset{*}{\underset{S}{\Longrightarrow}} v_{\varphi(w')\varphi(w'')} = v_{\varphi(w)}$. Note that $u \underset{S}{\Longrightarrow} v$ implies $\varphi(u) = \varphi(v)$. Consider $v_1 \underset{S}{\Longleftarrow} u \underset{S}{\Longrightarrow} v_2$ for some $u, v_1, v_2 \in A^*$. For $i \in \{1, 2\}$ either $\|v_i\| = d$ and

[2] In fact, according to the acknowledgments of [NW02], this technique was suggested by Klaus Reinhardt.

$v_i = v_{\varphi(u)}$, or $v_i \xrightarrow[S]{*} v_{\varphi(u)}$ by the proof above. Thus, the system S is locally confluent which implies confluence by Lemma 2.16. Since every irreducible word has weight at most d, the index of S is finite.

Let $G \subseteq A^*/S$ be a non-trivial group. Since every word w of weight at least d reduces to $v_{\varphi(w)}$, the elements of G must be contained in $\{v_m \mid m \in M\}$. However, this set is isomorphic to M and thus G is a group in M. □

We apply Proposition 5.6 in the case of simple non-abelian groups. A *simple group* is a group G such that for every surjective homomorphism $\varphi : G \to H$ onto another group H either $H \simeq \{1\}$ or $H \simeq G$, that is, G has no nontrivial quotients. However the result is actually more general. It holds not only for all simple non-abelian groups, but for all groups which have no abelian group as a quotient.

Corollary 5.7. *Let $(A, \|\cdot\|)$ be a weighted alphabet and $\varphi : A^* \to G$ be a surjective homomorphism into a group G which has no nontrivial abelian quotient groups. Then there exists a weighted Church-Rosser system S which factorizes through φ.*

Proof. Without loss of generality we may assume that $\gcd\{\|a\| \mid a \in A\} = 1$ (else divide the weight by $\gcd\{\|a\| \mid a \in A\}$). If $\gcd\{\|w\| \mid \varphi(w) = 1\} > 1$, there exists a prime number p which divides $\gcd\{\|w\| \mid \varphi(w) = 1\}$. Consider the homomorphism $\psi : A^* \to \mathbb{Z}/p\mathbb{Z}$ given by $\psi(w) = \|w\| \bmod p$. If $\varphi(u) = \varphi(v)$, then there exists a word $w \in A^*$ such that $\varphi(uw) = \varphi(vw) = 1$. Thus, $\|uw\| \equiv \|vw\| \equiv 0 \bmod p$ and we conclude $\psi(u) = \psi(v)$. Therefore, it holds $\ker\varphi \subseteq \ker\psi$ and by Theorem 2.1 there exists a homomorphism $\pi : G \to \mathbb{Z}/p\mathbb{Z}$ such that $\psi = \pi \circ \varphi$. Since G has no nontrivial abelian quotients and $\mathbb{Z}/p\mathbb{Z}$ has no nontrivial subgroups, we conclude $\ker\pi = G$ and thus $\|w\| \equiv 0 \bmod p$ for all $w \in A^*$. This is a contradiction to $\gcd\{\|a\| \mid a \in A\} = 1$. Thus, we obtain $\gcd\{\|a\| \mid a \in A\} = \gcd\{\|w\| \mid \varphi(w) = 1\}$ and can apply Proposition 5.6. □

Note that there are cases in which Proposition 5.6 can be applied for groups which have nontrivial abelian quotients. For example consider the representation $\varphi : A^* \to S_n$ given by $a \mapsto (1,2), b \mapsto (1,2,\ldots,n)$ of the symmetric group S_n where the weight is length. If n is not even, we have $\gcd(|a^2|, |b^n|) = 1$ and there exists a length-reducing Church-Rosser system S of finite index which factorizes through φ by Proposition 5.6. However, not every presentation of S_n satisfies the properties of Proposition 5.6. Consider for example the representation φ of S_n given by all transpositions, then $\gcd\{|w| \mid \varphi(w) = 1\} = 2$. In particular, since the signum is a homomorphism onto a cyclic group of order two, one cannot apply Corollary 5.7 on S_n.

Let us consider briefly consider the case of cyclic groups. Cyclic groups are a class of main groups which cannot satisfy Proposition 5.6. The case of the cyclic group of order 2 was solved by Niemann and Waldmann by using extensive computer search, see [NW02]. However, it is already much harder to find a Church-Rosser system for the homomorphism $\varphi : \{a,b,c\}^* \to \mathbb{Z}/3\mathbb{Z}$ where $\varphi(a) = \varphi(b) = \varphi(c) = 1 \bmod 3$. Restricting φ to the submonoid $\{a,b\}^*$ makes the situation simpler.[3] Still it is surprisingly

[3] A solution for this example was announced in [MNO88], but apparently their system was never published.

complicated. A possible Church-Rosser system $S \subseteq \{a,b\}^* \times \{a,b\}^*$ of finite index such that the restriction of φ factorizes through S is given by:

$$S = \left\{ aaa \to 1,\ baab \to b,\ (ba)^3 b \to b,\ bb\,u\,bb \to b^{|u|+1} \;\middle|\; 1 \leq |u| \leq 3 \right\}.$$

There are 273 irreducible elements and the longest irreducible word has length 16. Note that the last set of rules has bb as a prefix and as a suffix on both sides of every rule. The idea of preserving end markers such as $\omega = bb$ in the above example is essential for the solution of the general group case, too.

5.3 Preparations

In this section we prepare some tools which will be necessary in the proof of Theorem 5.14 and Theorem 5.24. In particular, we study an important inductive construction on the alphabet which is also used in Theorem 5.31. Whenever necessary, we stated the lemmas more general than in [DKRW15] in order to prove the statement about the groups in the Church-Rosser representation constructed in Theorem 5.14 or to reuse them for the proof of Theorem 5.24.

5.3.1 An Inductive Construction

The following lemma is used for an inductive construction of Church-Rosser systems. The main idea is to distinguish a letter $c \in A$ and use an inductive system for all words which do not contain the letter c. This system gets then glued back by using some system on a new alphabet consisting of the irreducible words in $(A \setminus \{c\})^*$ followed by an end marker c. This idea has been used in [DKW12, DKRW12, DKRW15]. Further, this construction yields a Rees extension monoid, as observed in [DKW12].

Lemma 5.8. *Let A be an alphabet of size at least two, $\varphi : A^* \to M$ be a homomorphism and $B = A \setminus \{c\}$ for some $c \in A$. Assume that $R \subseteq B^* \times B^*$ is a Parikh-reducing (subword-reducing, weight-reducing) Church-Rosser system of finite index which is φ-invariant. Let $K = \mathrm{IRR}_R(B^*)c$ be a new alphabet and $T \subseteq K^* \times K^*$ be a Parikh-reducing (subword-reducing, weight-reducing for the induced weights) Church-Rosser system of finite index such that*

$$T' := \{c\ell \to cr \mid \ell \to r \in T\} \subseteq A^* \times A^*$$

is φ-invariant. Then

a) $S = R \cup T' \subseteq A^* \times A^*$ is a φ-invariant Parikh-reducing (subword-reducing, weight-reducing) Church-Rosser system of finite index,

b) A^*/S is isomorphic to the Rees extension monoid $\mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$ with $\rho : B^*/R \to K^*/T$ given by $\rho([u]_R) = [\hat{u}c]_T$ where $u \xRightarrow[R]{*} \hat{u}$ and $\hat{u} \in \mathrm{IRR}_R(B^*)$.

Proof. a) The system T' is Parikh-reducing (resp. subword-reducing, weight-reducing), as the additional c on the left side does not change those properties. Since both R and T' are Parikh-reducing (resp. subword-reducing, weight-reducing) and φ-invariant, we have that S is Parikh-reducing (resp. subword-reducing, weight-reducing) and φ-invariant.

We show that S is confluent. Since S is terminating, it suffices to show that S is locally confluent by Lemma 2.16. Note that R is locally confluent. Since $K = \mathrm{IRR}_R(B^*)c$, every left side of a rule in T' starts and ends with a c and thus there is no overlap critical pair between two rules in R and T'. Obviously, there can be no factor critical pairs. Thus, it remains to show that T' is locally confluent. We already know that T is confluent. Let $u, v \in K^*$ be words. We first show that $cu \underset{S}{\Longrightarrow} cv$ if and only if $u \underset{T}{\Longrightarrow} v$. By the definition of K and the system T', one can see that $cu \underset{S}{\Longrightarrow} cv$ if and only if $cu \underset{T'}{\Longrightarrow} cv$. We have $cu \underset{T'}{\Longrightarrow} cv$ if and only if $cu = cu_1\ell u_2$ and $cv = cu_1 r u_2$ such that $cu_1 \in K^*$ and $(c\ell, cr) \in T'$. This holds if and only if $u = u_1\ell u_2$ and $v = u_1 r u_2$ for some $u_1, u_2 \in K^*$ and $(\ell, r) \in T$ which holds if and only if $u \underset{T}{\Longrightarrow} v$. Since T is confluent and terminating, for every $u \in K^*$ there exists a unique word $\hat{u} \in \mathrm{IRR}_T(K^*)$ such that $u \overset{*}{\underset{T}{\Longrightarrow}} \hat{u}$. By the above, $cu \overset{*}{\underset{S}{\Longrightarrow}} c\hat{u}$ and $c\hat{u} \in \mathrm{IRR}_S(A^*)$ is unique with this property. We conclude that every critical pair in T' must resolve. Therefore, S is a Church-Rosser system. Note that

$$\mathrm{IRR}_S(A^*) = \{u_0 c u_1 \cdots c u_k \mid u_1 c \cdots u_{k-1} c \in \mathrm{IRR}_T(K^*), u_i \in \mathrm{IRR}_R(B^*)\}\,.$$

In particular, since $\mathrm{IRR}_T(K^*)$ and $\mathrm{IRR}_R(B^*)$ are finite, we conclude that $\mathrm{IRR}_S(A^*)$ is finite, that is, S has finite index.

b) Consider the homomorphism $\psi : A^* \to \mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$ given by $\psi(a) = [a]_R$ and $\psi(c) = ([1]_R, [1]_T, [1]_R)$. We obtain $\psi(u) = [u]_R$ for $u \in B^*$. Let $u = u_1 c u_2 \cdots c u_n$ be the factorization of some word in $u \in A^*$ with $u_i \in B^*$ and $n > 1$. Then

$$\begin{aligned}
\psi(u) &= \psi(u_1 c u_2 \cdots c u_n) \\
&= [u_1]_R \circ ([1]_R, [1]_T, [1]_R) \circ [u_2]_R \circ \cdots \circ ([1]_R, [1]_T, [1]_R) \circ [u_n]_R \\
&= ([u_1]_R, \rho(u_2) \cdots \rho(u_{n-1}), [u_n]_R) \\
&= ([u_1]_R, [\widehat{u_2} c \cdots \widehat{u_{n-1}} c]_T, [u_n]_R),
\end{aligned}$$

where $\widehat{u_i}$ denotes the irreducible element such that $u_i \overset{*}{\underset{R}{\Longrightarrow}} \widehat{u_i}$.

Let $x = ([u]_R, [v]_T, [w]_R) \in \mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$, then $\psi(ucvw) = x$ and if $[u]_R \in \mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$, then $\psi(u) = [u]_R$ by definition. In particular, ψ is surjective. We show that for $u, v \in A^*$ the equivalence $\psi(u) = \psi(v)$ holds if and only if $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$. Obviously, both $\psi(u) = \psi(v)$ and $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$ imply that $u \in B^*$ if and only if $v \in B^*$. For $u, v \in B^*$ it is $[u]_R = \psi(u) = \psi(v) = [v]_R$ and therefore $\psi(u) = \psi(v)$ if and only if $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$. Thus, we may assume that $u, v \notin B^*$. Let $u = u_1 c u_2 \cdots c u_n$ be a word with $u_i \in B^*$ and $n > 1$ and let $u \underset{S}{\Longrightarrow} u'$. We show that $\psi(u) = \psi(u')$. If $u \underset{R}{\Longrightarrow} u'$, then there exist words

u_i such that $u_i \underset{R}{\Longrightarrow} u_i'$ and $u' = u_1 c \cdots u_{i-1} c u_i' c u_{i+1} c \cdots c u_n$. Since $\widehat{u_i} = \widehat{u_i'}$, we obtain $\psi(u) = \psi(u')$ in this case. If $u \underset{T'}{\Longrightarrow} u'$, then there exists some factor $u_i c \cdots u_j c$ of u with $u_i c \cdots u_j c \underset{T}{\Longrightarrow} v_1 c \cdots v_\ell c$ and $i > 1$ such that $u' = u_1 c \cdots u_{i-1} c v_1 c \cdots v_\ell c u_{j+1} c \cdots c u_n$. In particular, $[\widehat{u_2} c \cdots \widehat{u_{n-1}} c]_T = [\widehat{u_2} c \cdots \widehat{u_{i-1}} c v_1 c \cdots v_\ell c \widehat{u_{j+1}} c \cdots \widehat{u_{n-1}} c]_T$ and therefore $\psi(u) = \psi(u')$. Since S is confluent and $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$, there exists a word w such that $u \overset{*}{\underset{S}{\Longrightarrow}} w$ and $v \overset{*}{\underset{S}{\Longrightarrow}} w$. Using the above inductively, we conclude $\psi(u) = \psi(w) = \psi(v)$.

For the converse, assume that $\psi(u) = \psi(v)$. If $u, v \in B^*$, we obtain $[u]_R = [v]_R$ and from $R \subset S$ we deduce $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$. Thus, let $u = u_1 c u_2 \cdots c u_n$ and $v = v_1 c v_2 \cdots c v_m$ be factorizations with $u_i, v_j \in B^*$ and $n, m > 1$. Then

$$\begin{aligned} u &\overset{*}{\underset{R}{\Longrightarrow}} \widehat{u_1} c \widehat{u_2} \cdots c \widehat{u_{n-1}} c \widehat{u_n} \\ &= \widehat{v_1} c \widehat{u_2} \cdots c \widehat{u_{n-1}} c \widehat{v_m} \\ &\overset{*}{\underset{T}{\Longleftrightarrow}} \widehat{v_1} c \widehat{v_2} \cdots c \widehat{v_{m-1}} c \widehat{v_m} \\ &\overset{*}{\underset{R}{\Longleftarrow}} v \end{aligned}$$

and therefore $u \overset{*}{\underset{S}{\Longleftrightarrow}} v$. Thus, by Theorem 2.1, ψ induces an isomorphism $\hat{\psi} : A^*/S \to \mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$. □

It is worth to note that Lemma 5.8 does not work for length-reducing systems. A length-reducing system $T \subseteq K^* \times K^*$ does not necessarily yield a length-reducing system $T' \subseteq A^* \times A^*$. This is the reason one has to consider the stronger variants, that is, Parikh-, subword- or weight-reducing systems.

5.3.2 Outline

In this subsection we give an outline on the proof strategy which will be used in Theorem 5.14 and Theorem 5.24. The proofs of these two theorems are the same on a macro level, but differ in the combinatorial details.

The macro structure of the proof is as follows: Given a homomorphism $\varphi : A^* \to G$, we construct a system S which is φ-invariant by induction on A. For a fixed letter $c \in A$ we remove c and obtain the alphabet $B = A \setminus \{c\}$. Inductively, one obtains a system $R \subseteq B^* \times B^*$ which factorizes through φ. Now, consider a new alphabet $K = \mathrm{IRR}_R(B^*)c$. Having Lemma 5.8 in mind, it remains to construct a system $T \subseteq K^* \times K^*$. The system T contains two kinds of rules: Δ-rules and Ω-rules. The set T_Δ of Δ-rules deals with long repetitions of short words. Whenever there is no long repetition of short words, this yields a marker word ω. The set T_Ω of Ω-rules contains rules of the form $\omega u \omega \to \omega v_g \omega$ for some normal forms v_g. Lemma 5.10, Lemma 5.12 and Lemma 5.13 in the next subsection lay the foundation for these kind of rules.

5.3.3 Some lemmas

The following lemma is formulated for weighted Church-Rosser system, but holds for Parikh-reducing or subword-reducing Church-Rosser systems too.

Lemma 5.9. *Let $(A, \|\cdot\|)$ be a weighted alphabet, $e \in \mathbb{N}$ be some natural number and $S \subseteq A^* \times A^*$ be a weighted Church-Rosser system such that $\mathrm{IRR}_S(A^*)$ is finite. Then*

$$S_e = \{u\ell v \to urv \mid u, v \in A^e \text{ and } \ell \to r \in S\}$$

is a weighted Church-Rosser system satisfying:

(i) The mapping $[u]_{S_e} \mapsto [u]_S$ for $u \in A^*$ is well-defined and yields a surjective homomorphism from A^*/S_e onto A^*/S.

(ii) All words of length at most $2e$ are irreducible with respect to S_e.

(iii) The set $\mathrm{IRR}_{S_e}(A^*)$ is finite.

(iv) For every group G in A^*/S_e exists an embedding into A^*/S.

Proof. Since S is weight-reducing, the system S_e is weight-reducing, too. For all $w, w' \in A^*$ and $u, v \in A^e$, we have $w \overset{*}{\underset{S}{\Longrightarrow}} w'$ if and only if $uwv \overset{*}{\underset{S_e}{\Longrightarrow}} uw'v$. Moreover, rules of S_e apply only to words of length more than $2e$ and an application of a rule leaves the prefix and suffix of length e invariant. Hence, confluence of S transfers to confluence of S_e. Thus, S_e is indeed a weighted Church-Rosser system. Since $w \overset{*}{\underset{S_e}{\Longleftrightarrow}} w'$ implies $w \overset{*}{\underset{S}{\Longleftrightarrow}} w'$ for all $w, w' \in A^*$, we obtain $[u]_{S_e} \subseteq [u]_S$ and assertion (i) holds.

All words of length at most $2e$ belong to $\mathrm{IRR}_{S_e}(A^*)$. This yields assertion (ii). More precisely, we can write $\mathrm{IRR}_{S_e}(A^*)$ as a disjoint union

$$\mathrm{IRR}_{S_e}(A^*) = A^{<2e} \cup A^e \cdot \mathrm{IRR}_S(A^*) \cdot A^e.$$

Since $\mathrm{IRR}_S(A^*)$ is finite by hypothesis, the set $\mathrm{IRR}_{S_e}(A^*)$ is finite, too. This shows assertion (iii).

Let $G \subseteq A^*/S_e$ be a non-trivial group. Since every element of G has an inverse, the irreducible elements of G are a subset of $A^e \cdot \mathrm{IRR}_S(A^*) \cdot A^e$. Reusing the argument used in the proof of Proposition 3.6, we can construct an embedding of G into A^*/S. This yields assertion (iv). □

The next lemma says that whenever a word is not a factor of a repetition of a word of length at most n, it contains a witness of length at most $2n$. This is the key lemma in the definition of the markers Ω.

Lemma 5.10. *Let $\Delta \subseteq A^{\leq n}$ for some $n \in \mathbb{N}$ be a set which is closed under conjugation and let $F = \bigcup_{\delta \in \Delta, i \in \mathbb{N}} \mathrm{Factors}(\delta^i)$. Then $A^* \setminus F$ is an ideal which is generated by a set $J \subseteq A^{\leq 2n}$ of words of length at most $2n$, that is, $A^* \setminus F = A^* J A^*$.*

Proof. By definition, F is closed under taking factors. Hence, $w_1w_2w_3 \in F$ implies $w_2 \in F$, or equivalently, $w_2 \notin F$ implies $w_1w_2w_3 \notin F$. Thus, $A^* \setminus F$ is an ideal.

In order to show that $A^* \setminus F$ is generated by some $J \subseteq A^{\leq 2n}$, we show that for all $u \notin F$ with $|u| > 2n$ there is a proper factor of u which is not in F. Note that since Δ is closed under conjugation, we have $F = \bigcup_{\delta\in\Delta,i\in\mathbb{N}} \mathrm{Factors}(\delta^i) = \bigcup_{\delta\in\Delta,i\in\mathbb{N}} \mathrm{Prefixes}(\delta^i) = \bigcup_{\delta\in\Delta,i\in\mathbb{N}} \mathrm{Suffixes}(\delta^i)$. Write $u = awb$ for $a, b \in A$ and assume $aw, wb \in F$. Then aw is a suffix of δ^+ and wb is a prefix of η^+ for some $\delta, \eta \in \Delta$. Let $p = |\delta|$ and $q = |\eta|$. Note that p is a period of aw and q is a period of wb. Thus, p and q are both periods of w. Since $|w| \geq 2n - 1 \geq p + q - \gcd(p, q)$, we see that $\gcd(p, q)$ is also a period of w by the Periodicity Theorem of Fine and Wilf, see Theorem 2.14. By symmetry we may assume $p \leq q$; and we can write $q + 1 = p + 1 + k\gcd(p, q)$ for some $k \in \mathbb{N}$. Since the $(p + 1)$-th letter in aw is a and w has period $\gcd(p, q)$, the $(q + 1)$-th letter in aw is a, too. The $(q + 1)$-th letter in aw is the last letter of η, because $q = |\eta|$. It follows that awb is a factor of η^+, that is, $u \in F$. This is a contradiction and therefore either $aw \notin F$ or $wb \notin F$. □

Remark 5.11. If Δ' is the closure of Δ under conjugation, then $\bigcup_{\delta\in\Delta'} \mathrm{Factors}(\delta^i) \subseteq \bigcup_{\delta\in\Delta} \mathrm{Factors}(\delta^{i+1})$. Therefore, the requirement that Δ is closed under conjugation is not needed in Lemma 5.10. However, the proof is easier to understand by being able to refer to the last letter. In our applications Δ will always be closed under conjugation. ⋄

Lemma 5.12. *Let $\Delta \subseteq A^{\leq d}$ be a set of nonempty words of length at most d which is closed under nontrivial factors, $t > 2d$ and $n \geq 1$. Then*

$$T_\Delta = \left\{ \delta^{t+n} \to \delta^t \;\middle|\; \delta \in \Delta \right\}$$

is a subword-reducing Church-Rosser system. In particular, T_Δ is Parikh-reducing and weight-reducing for every weight.

Proof. Since δ^t is a factor of δ^{t+n}, the word δ is nonempty and $n \geq 1$, it follows that the system T_Δ is subword-reducing. Thus, it suffices to show that T_Δ is locally confluent. Let $\delta^i \in \Delta$ for some $i \geq 2$. Then $\delta \in \Delta$ and

$$(\delta^i)^{t+n} = \delta^{it+in} \underset{T_\Delta}{\overset{*}{\Longrightarrow}} \delta^{it+(i-1)n} \underset{T_\Delta}{\overset{*}{\Longrightarrow}} \cdots \underset{T_\Delta}{\overset{*}{\Longrightarrow}} \delta^{it} = (\delta^i)^t.$$

This allows us to assume that Δ contains only primitive words by Lemma 2.18. Let $\delta, \eta \in \Delta$ with $|\delta| \geq |\eta|$ and suppose $\delta^{t+n} \to \delta^t$ and $\eta^{t+n} \to \eta^t$ are rules which are part of a critical pair. We have to study the two cases of factor critical and overlap critical pairs.

We cover factor critical pairs first and consider the case that η^{t+n} is a factor of δ^{t+n}. Note that $|\eta^t| \geq t > 2d \geq |\delta^2|$. Thus, there is a conjugate $\zeta = \eta^r\eta_1$ of δ such that η_1 is a proper prefix of η and ζ^2 is a prefix of η^t. By canceling the prefix η^r we see that $\eta_1\eta$ is a prefix of η^2. By primitivity of η this implies that η_1 is empty and by primitivity of δ we obtain $\zeta = \eta$. This implies $|\delta| = |\eta|$ and since η^{t+n} is a factor of δ^{t+n} we obtain that $\eta = \delta$.

The second case are overlap critical pairs. Let $\delta^{t+n} = xy$ and $\eta^{t+n} = yz$ for non-empty words x, y, z. If $|y| > |\eta^t|$, then by $|\eta^t| > |\delta^2|$ we get that δ^2 is a factor of η^t. Using the same argument as above, we conclude that δ is a conjugate of η and the critical pair resolves. Thus, it remains to prove the case for $|y| \leq |\eta^t| \leq |\delta^t|$. As y is small enough we proceed by writing $x = \delta^n x_1$ and $z = z_1\eta^n$. The critical pair can be resolved as follows:

$$xyz = \delta^{t+n}z \underset{T_\Delta}{\Longrightarrow} \delta^t z = x_1\eta^{t+n} \underset{T_\Delta}{\Longrightarrow} x_1\eta^t = x_1yz_1,$$
$$xyz = x\eta^{t+n} \underset{T_\Delta}{\Longrightarrow} x\eta^t = \delta^{t+n}z_1 \underset{T_\Delta}{\Longrightarrow} \delta^t z_1 = x_1yz_1. \qquad \square$$

The following lemma is crucial in showing that the index of the constructed system is finite. It is used for the proof that there exists a number t_Ω such that every word of length at least t_Ω is reducible.

Lemma 5.13. *Let $(A, \|\cdot\|)$ be a weighted alphabet, $d \in \mathbb{N}$ and $\Delta \subseteq A^{\leq d}$, $\Omega \subseteq A^*$ be sets. Furthermore, let $\preceq$ be a total preorder on Ω. Let $t, t_0 \in \mathbb{N}$ be numbers such that*

1. *$t > 2\max_{\omega\in\Omega} \|\omega\|$ and $t > \max_{a\in A} \|a\|$.*
2. *every word v of length at least t_0 either contains a factor δ^{t+n} for $\delta \in \Delta$ or a factor $\omega \in \Omega$.*

Then there exists a number t_Ω such that every word v of weight at least t_Ω contains either

- *a factor δ^{t+n} for $\delta \in \Delta$ or*
- *a factor $\omega u\omega$ with $\omega \in \Omega$, $t < \|\omega u\omega\| < t_\Omega$ and for every $\eta \in \Omega$ with $\omega u\omega \in A^*\eta A^*$ we have $\eta \preceq \omega$.*

Proof. Let $\Omega_v = \{\omega \in \Omega \mid v \in A^*\omega A^*\}$ be the set of Ω-factors of v and let t_k be defined by the recursion $t_k = 2t_{k-1} + t$. A quick calculation verifies the explicit formula $t_k = 2^k(t_0 + t) - t$. We prove the following statement by induction on k: For every word v with $\|v\| \geq t_k$, at least k different Ω-factors, i.e., $k \geq |\Omega_v|$ and which does not contain a factor δ^{t+n} for $\delta \in \Delta$, there exists a factor $\omega u\omega$ of v such that

- $\omega \in \Omega$,
- $t < \|\omega u\omega\| < t_k + t$ and
- ω is a maximal Ω-factor of $\omega u\omega$.

The case $k = 0$ is trivial since by hypothesis every word v with weight at least t_0 and $|\Omega_v| = 0$ must contain a factor δ^{t+n} for $\delta \in \Delta$. Consider the case $k > 0$. Since we require that the weight of the factor $\omega u\omega$ is smaller than $t_k + t$, we consider a factor of minimal weight among those factors of v of weight at least t_k. As every factor of such

a factor is also a factor of v, we can assume that every proper factor of v has weight smaller than t_k. In particular, we may assume $\|v\| < t_k + t$ since every letter has weight at most t.

Consider the factorization $v = pfq$ with $f \in (\omega A^* \cap A^*\omega)$ such that ω is a maximal Ω-factor of v and f is maximal with regard to the weight. If $\|f\| \leq t$, we obtain

$$t_k = 2t_{k-1} + t \leq \|pfq\| = \|pq\| + \|f\| \leq \|pq\| + t$$

which implies $\|pq\| \geq 2t_{k-1}$. Since p and q contain no factor ω, we can either apply induction to p or q. If $\|f\| > t$, then f has the form $f = \omega u \omega$ for a word u because of $t > 2\max_{\omega\in\Omega} \|\omega\|$ and $f \in (\omega A^* \cap A^*\omega)$. The factor f has the required properties since $\|f\| \leq \|v\| < t_k + t$. This concludes the induction. We infer the statement of the lemma from the induction by setting $t_\Omega = t_{|\Omega|} + t$. □

5.4 Groups are Church-Rosser congruential

In this section we show that for every weighted alphabet $(A, \|\cdot\|)$ and every homomorphism $\varphi : A^* \to G$ to a finite group G, there exists a weight-reducing Church-Rosser system S of finite index which is φ-invariant.

Theorem 5.14. *Let $(A, \|\cdot\|)$ be a weighted alphabet and let $\varphi : A^* \to G$ be a homomorphism to a finite group G. Then there exists a weighted Church-Rosser system S of finite index such that φ factorizes through S. All groups in A^*/S are subgroups of G or of $\mathbb{Z}/n\mathbb{Z}$ where n is the exponent of G.*

We may assume that φ is surjective. In the following n denotes the exponent of G. We will prove the theorem by induction on the size of the alphabet A. Fix a letter $c \in A$. If $A = \{c\}$, then we may choose $S = \{c^n \to 1\}$. Let $B = A \setminus \{c\}$ and $B = \{a_0, \ldots, a_{s-1}\}$ with $s \geq 1$ such that a_0 has minimal weight in B. For $i \in \mathbb{N}$ define words γ_i by

$$\gamma_i = a_{i \bmod s}^{n+\lfloor i/s \rfloor} c. \tag{5.1}$$

In particular, $\gamma_0 = a_0^n c$, $\gamma_1 = a_0^{n+1} c$ for $s = 1$, $\gamma_1 = a_1^n c$ for $s \geq 2$, $\gamma_s = a_0^{n+1} c$, and for $k \geq 0$ we have $\gamma_{ks} = a_0^{n+k} c$. The words γ_i act as generators of G: it is $\varphi(\gamma_0) = \varphi(c)$ and, since n is the exponent of G, it holds $\varphi(\gamma_{s+i}) = \varphi(a_i c)$ for $0 \leq i < s$. Note that in every word γ_i one letter of B appears at least n times and thus the weight of every γ_i is larger than $n\,\|a_0\|$. This will be used numerous times. Since the words γ_i generate G and $\|\gamma_0\| + \|a_0\| = \|\gamma_s\|$, there exists a number m with $1 \leq m \leq |G| \cdot n \cdot |A|$ such that for every $g \in G$ there exists a word

$$v_g = \gamma_0 \gamma_0^{n_0} \gamma_1^{n_1} \cdots \gamma_m^{n_m} \gamma_m \gamma_0 \tag{5.2}$$

with $n_i \geq 0$ satisfying $\varphi(v_g) = g$ and $\|v_g\| - \|v_h\| < n\,\|a_0\|$ for all $g, h \in G$. Indeed, assume $\|v_g\| - \|v_h\| \geq n\,\|a_0\|$ for some $g, h \in G$. For those v_g with maximal weight replace the exponent n_0 of γ_0 by $n_0 + n$; for all other words v_h replace the exponent n_s

of γ_s by $n_s + n$. This decreases the maximal difference $\|v_g\| - \|v_h\|$ at least by 1. The image $\varphi(v_h)$ did not change by definition of the exponent n. Iterating this procedure until the weights of all v_g differ by less than $n\,\|a_0\|$ yields the normal forms v_g with the properties mentioned above. Fix the number m from the normal forms and let

$$\Gamma = \{\gamma_0, \ldots, \gamma_m\}\,.$$

By induction on the size of the alphabet there exists a weighted Church-Rosser system $R \subseteq B^* \times B^*$ of finite index such that the restriction $\varphi : B^* \to G$ factorizes through R. Note that induction applies to $\varphi : B^* \to G$ even if the restriction of φ to B^* is not surjective. By Lemma 5.9, we may choose R such that $\Gamma \subseteq \mathrm{IRR}_R(B^*)\,c$. Let

$$K = \mathrm{IRR}_R(B^*)\,c.$$

The set K is a finite prefix code in A^* with $\Gamma \subseteq K$. We consider K as an extended alphabet and its elements as extended letters. The free monoid K^* is viewed as the subset $K^* \subseteq A^*$. The weight $\|u\|$ of $u \in K$ is the weight of u seen as a word over A. Each word $\gamma_i \in \Gamma$ is a letter in K. The restriction of the homomorphism $\varphi : A^* \to G$ to K^* induces a homomorphism $\psi : K^* \to G$; it is given by $\psi(u) = \varphi(u)$ for $u \in K$. We define a lexical order on A by $a_0 < \cdots < a_{s-1} < c$ which leads to the length-lexicographic order on B^*c. (Words are compared first by length, and if they have equal length, they are compared in lexicographic order.) The length-lexicographic order induces a linear order $\leq$ on $\mathrm{IRR}_R(B^*)c$ and hence also a linear order on the extended alphabet K. Equation (5.1) and Equation (5.2) show that the words v_g satisfy as words over the weighted alphabet $(K, \|\cdot\|)$ the following five properties:

(i) Each word v_g starts with the extended letter γ_0.

(ii) The last two extended letters of v_g are $\gamma_m\gamma_0$, i.e., $v_g \in K^*\gamma_m\gamma_0$.

(iii) From left to right all extended letters in v_g are in non-decreasing order with respect to $\leq$ with the sole exception of the last letter γ_0, which is smaller than its predecessor γ_m.

(iv) All extended letters in v_g have a weight greater than $n\,\|a_0\|$.

(v) All differences $\|v_g\| - \|v_h\|$ are smaller than $n\,\|a_0\|$.

Proposition 5.15. *There exists a weighted Church-Rosser system $T \subseteq K^* \times K^*$ of finite index such that $\psi : K^* \to G$ factorizes through T. Moreover, every group in K^*/T is a subgroup of G.*

Let us postpone the proof of Proposition 5.15 and finish the proof of Theorem 5.14 first. Using Proposition 5.15, the requisites of Lemma 5.8 are satisfied. Thus, $S = R \cup T'$ is a φ-invariant weighted Church-Rosser system, where $T' := \{c\ell \to cr \mid \ell \to r \in T\} \subseteq A^* \times A^*$ is defined as in Lemma 5.8. Lemma 5.8 yields $A^*/S \simeq \mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$. By Proposition 3.6, all groups in A^*/S are in B^*/R or in K^*/T. By Proposition 5.15

d, m, n, κ	positive natural numbers
$(K, \|\cdot\|)$	finite weighted alphabet with linear order $<$
$\psi : K^* \to G$	homomorphism, w.l.o.g. surjective
$v_g \in K^+$	normal form for $g \in G$
$\Gamma = \{\gamma_0, \ldots, \gamma_m\} \subseteq K$	with $\gamma_0 < \cdots < \gamma_m$ and $\|\gamma_i\| > \kappa$
$\Delta = K \cup \{\delta \in K^+ \mid \|\delta\| \leq \kappa\}$	in particular, $\Gamma \subseteq K \subseteq \Delta \subseteq K^{\leq d}$
F	set of factors of all δ^+ with $\delta \in \Delta$
$J \subseteq K^{\leq 2d}$	minimal such that $K^*JK^* = K^* \setminus F$ (i.e., J is a basis of the ideal $K^* \setminus F$)
$\Omega \subseteq J$	maximal such that $\Omega \cap \Gamma K^* = \{\gamma\gamma' \mid \gamma, \gamma' \in \Gamma, \gamma > \gamma'\}$ and linear ordered such that $\gamma_m\gamma_0 \prec b\gamma_0 \prec \omega$ for $b \neq \gamma_m$ and $\omega \in \Omega \setminus K^+\gamma_0$
$t < t_0 < t_\Omega$	"threshold" values
T_Δ, $T_\Omega \subseteq T'_\Omega$,	semi-Thue systems
$T = T_\Delta \cup T_\Omega$	T_Δ, T_Ω and T are weighted Church-Rosser systems

Figure 5.2: Overview of some notation in this section

all groups in K^*/T are subgroups in G and by Lemma 5.9 and induction all groups in B^*/R are subgroups of G. This reduces the proof of Theorem 5.14 to the proof of Proposition 5.15.

The difference between Proposition 5.15 and Theorem 5.14 is that the (much larger[4]) alphabet K satisfies more hypotheses than A. We show Proposition 5.15 from an abstract viewpoint. An overview of some notation which will be used in the proof of Proposition 5.15 is summarized in Table 5.2.

In a first step we fix $\kappa = n\,\|a_0\|$, and view κ as a constant which is attached to the finite weighted alphabet $(K, \|\cdot\|)$. The set K contains a linearly ordered subset $\Gamma = \{\gamma_0, \ldots, \gamma_m\}$ with $\gamma_0 < \cdots < \gamma_m$ such that $\|\gamma\| > \kappa$ for all $\gamma \in \Gamma$. In addition we require that there exists a homomorphism $\psi : K^* \to G$ and a subset $\widehat{G} \subseteq \Gamma^*$ with the following properties.

(i) We have $\widehat{G} \subseteq \gamma_0\gamma_0^*\gamma_1^* \cdots \gamma_m^*\gamma_m\gamma_0$.

(ii) For each $g \in G$ there is exactly one word $v_g \in \widehat{G}$ with $\psi(v_g) = g$.

(iii) For all $g, h \in G$ we have $\|v_g\| - \|v_h\| < \kappa$.

Note that (ii) implies that ψ is surjective which we assume without restriction. Let us define a subset $\Delta \subseteq K^+$ and a parameter d as follows.

$$\Delta = K \cup \left\{\delta \in K^+ \;\middle|\; \|\delta\| \leq \kappa\right\} \text{ and } d = \max\{|\delta| \mid \delta \in \Delta\}.$$

The set Δ is closed under conjugation, that is, if $uv \in \Delta$ for $u, v \in K^*$, then $vu \in \Delta$. We let $F \subseteq K^*$ be the set of all factors of δ^+ where $\delta \in \Delta$, that is, we set

$$F = \left\{u \in K^* \;\middle|\; u \text{ is factor of } \delta^+ \text{ for some } \delta \in \Delta\right\}.$$

[4]See Section 5.7 on how to make K fairly small.

Let $u\gamma v \in F \cap K^*\gamma K^*$, that is, $u\gamma v$ is a factor of δ^+ for some $\delta \in \Delta$. Since $\|\gamma\| > \kappa$, we conclude $\delta = \gamma$ and $u\gamma v \in \gamma^+$. Thus, we obtain

$$K^*\gamma K^* \cap F = \gamma^+ \text{ for all } \gamma \in \Gamma. \tag{5.3}$$

By Lemma 5.10, there exists a uniquely defined minimal set $J \subseteq K^{\leq 2d}$ such that $K^* \setminus F = K^*JK^*$. Since J and Δ are disjoint, all words in J have a weight greater than κ. Let Ω contain all $\omega \in J$ such that $\omega \in \Gamma K^*$ implies $\omega = \gamma\gamma'$ for some $\gamma, \gamma' \in \Gamma$ with $\gamma > \gamma'$, that is,

$$\Omega = J \cap \{\omega \in K^* \mid \omega \notin \Gamma K^* \text{ or } \omega = \gamma\gamma' \text{ for } \gamma, \gamma' \in \Gamma \text{ with } \gamma > \gamma'\}.$$

We have $\Gamma \subseteq \Delta$ and $\Omega \subseteq J$. In particular Ω is finite and every word in Ω has length at most $2d$.

Remark 5.16. We claim $K^*\Gamma K^* \cap J \subseteq K\Gamma \cup \Gamma K$. In particular, for $\omega \in K^*\Gamma \cap \Omega$ we obtain $\omega = b\gamma$ with $b \in K$, $\gamma \in \Gamma$ and $b \neq \gamma$. In order to see the claim, we show that every word in $K^*\Gamma K^* \cap J$ has length 2. Words in J have length at least 2, hence (by left-right symmetry) it is enough to consider words $w = bx\gamma y \in J$ with $b \in K$, $x, y \in K^*$ and $\gamma \in \Gamma$. By minimality of J we obtain $x\gamma y \in F$ and hence $x\gamma y \in \gamma^+$ by Equation (5.3). Thus, we can write $w = bz\gamma$ with $z \in \gamma^*$ and $bz \in F$. If $z \neq 1$, then $b \in \gamma^+$, too. This implies $w \in \gamma^+$, but this is impossible due to $w \in J$. Therefore, $w = b\gamma$ and $b \neq \gamma$. ◇

Let us define a "threshold" value $t \in \mathbb{N}$ by

$$t = \max\{\|\omega v_g \omega\| \mid g \in G,\ \omega \in \Omega\}.$$

This is not the optimal bound at this point, but it allows to use the parameter t again later. For the moment we use only the following two properties, which are satisfied by our choice.

(i) If δ^t is a prefix of a word $u\omega$ or a suffix of a word ωu for $\delta \in \Delta$ and $\omega \in \Omega$, then we have $\|u\| > \max\{\|v_g\| \mid g \in G\}$.

(ii) We have $t > 2d$.

Here $t > 2d$ can be seen by

$$t > 2\max\{\|\omega\| \mid \omega \in \Omega\} > 2\max\{\|\delta\| \mid \delta \in \Delta\} \geq 2\max\{|\delta| \mid \delta \in \Delta\} = 2d.$$

The first set of rules over the extended alphabet K deals with long repetitions of short words: The Δ-rules of the system T are

$$T_\Delta = \left\{\delta^{t+n} \to \delta^t \;\middle|\; \delta \in \Delta \text{ and } \delta \text{ is primitive}\right\}.$$

Lemma 5.12 shows that T_Δ is a weighted Church-Rosser system. Note that closure under conjugation is not sufficient to guarantee confluence of T_Δ. Lemma 5.12 exploited the fact that t is large enough. Example 5.17 shows that at least $t > d-2$ is necessary.

Example 5.17. Let $\Delta = \{a, aab, aba, baa\}$ with $d = 3$. Consider $t = d - 2 = 1$ and the system $S = \{(aab)^2 \to aab, (aba)^2 \to aba, (baa)^2 \to baa, a^2 \to a\}$. The set Δ is closed under conjugation and all words in Δ are primitive, but S is not confluent. This can be seen by $abab \underset{S}{\overset{*}{\Longleftarrow}} (aab)^2 \underset{S}{\overset{*}{\Longrightarrow}} ab$. ◇

As we will see next, every sufficiently long word without long Δ-repetitions contains a factor $\omega \in \Omega$.

Lemma 5.18. *There exists a bound $t_0 \in \mathbb{N}$ such that every word $u \in K^*$ with $\|u\| \geq t_0$ contains either a factor $\omega \in \Omega$ or a factor of the form δ^{t+n} for $\delta \in \Delta$ (or both).*

Proof. Let us first assume that $u \notin \Gamma^*$. Then there exists a factorization $u = xay$ with $x \in \Gamma^*$ and $a \notin \Gamma$. If $ay \notin F$, there exists a prefix of ay which is in J and consequently in Ω. Thus, we may assume that $ay \in F$, i.e., ay is a factor of δ^+ for some $\delta \in \Delta$. If $\|ay\| \geq (n + t + 2) \max\{\|\delta\| \mid \delta \in \Delta\}$, then ay contains a factor δ^{t+n}. Thus, without loss of generality we may assume that $u = u'u''$ with $u' \in \Gamma^*$ and $\|u''\| \leq (n + t + 2) \max\{\|\delta\| \mid \delta \in \Delta\}$ (This obviously also holds in the case $u \in \Gamma^*$). If u' contains a factor $\gamma\gamma'$ with $\gamma > \gamma'$ we are finished. Thus, $u' = \gamma_{j_1} \cdots \gamma_{j_k}$ with $\gamma_{j_i} \in \Gamma$ and $\gamma_{j_{i-1}} \leq \gamma_{j_i}$. Since u' has no factor $\gamma_{j_i}^{t+n}$ we obtain $k \leq |\Gamma| \cdot (t + n - 1)$. This gives some bound on k and therefore on t_0 as well. □

Remark 5.19. We can choose the value $t_0 = (|\Gamma| + 1) \cdot (t + n) \cdot \max\{\|\delta\| \mid \delta \in \Delta\}$ of Lemma 5.18 using $|\Gamma| > s \geq 1$:

$$\begin{aligned}
&(n + t + 2) \max\{\|\delta\| \mid \delta \in \Delta\} + |\Gamma|\,(t + n - 1) \max\{\|\gamma\| \mid \gamma \in \Gamma\} \\
&\leq (n + t + 2) \max\{\|\delta\| \mid \delta \in \Delta\} + |\Gamma|\,(t + n - 1) \max\{\|\delta\| \mid \delta \in \Delta\} \\
&= (|\Gamma| + 1)(n + t) \max\{\|\delta\| \mid \delta \in \Delta\} + (2 - |\Gamma|) \max\{\|\delta\| \mid \delta \in \Delta\} \\
&\leq t_0
\end{aligned}$$ ◇

Words in $\mathrm{IRR}_{T_\Delta}(K^*)$ do not contain any factor of the form δ^{t+n} for $\delta \in \Delta$. Every sufficiently long word v can be written as $v = u_1 \cdots u_k$ with $\|u_i\| \geq t_0$ and k sufficiently large. Thus, by repeatedly applying Lemma 5.18, every long enough word $v \in \mathrm{IRR}_{T_\Delta}(K^*)$ contains two occurrences of the same $\omega \in \Omega$ which are far apart. This suggests rules of the form $\omega\, u\, \omega \to \omega\, v_{\psi(u)}\, \omega$; but in order to ensure confluence we have to limit their use. For this purpose, we equip Ω with a linear order $\preceq$ such that $\gamma_m\gamma_0$ is the least element, and every element in $\Omega \cap K\gamma_0$ is less than all elements in $\Omega \setminus K\gamma_0$.

For a word $v \in K^*\Omega K^*$ define the *maximal Ω-factor* to be the maximal $\omega \in \Omega$ with respect to the linear order $\preceq$ such that $v \in K^*\omega K^*$. The following lemma is the principal reason for excluding all words $\omega \in \Gamma K^*$ in the definition of Ω except for $\omega = \gamma\gamma' \in \Gamma^2$ with $\gamma > \gamma'$.

Lemma 5.20. *(i) Let $v = x\delta^{t+n}y \in K^*\Omega K^*$. Then $x\delta^t y$ has the same maximal Ω-factors as v.*

(ii) Let $v = x\omega u\omega y$ with $\omega \in \Omega$ and $v' = x\omega v_{\psi(u)}\omega y$. Then the maximal Ω-factor of v' is not greater than the maximal Ω-factor of v.

Proof. (i): By definition of t we have $t > 2d$ and by Lemma 5.10 we have $|\omega| \leq 2d$ for all $\omega \in \Omega$. Thus, ω does not contain δ^t as a factor and $x\delta^{t+n}y$ and $x\delta^t y$ have the same Ω-factors. Hence, the statement in (i) holds.

(ii): As no Ω-factor can contain ω as a proper factor it suffices to show that ω is the maximal Ω-factor of $\omega v_{\psi(u)}\omega$. The normal form $v_{\psi(u)}$ has $\gamma_m\gamma_0$ as a suffix. In addition, the word $\gamma_m\gamma_0$ is the only element in Ω which is a factor of $v_{\psi(u)}$. The reason is that all other letters in $v_{\psi(u)}$ are in non-decreasing order whereas all $\gamma\gamma' \in \Omega$ are in decreasing order. In particular, if $\gamma_m\gamma_0 v_{\psi(u)}\gamma_m\gamma_0 \in K^*\omega' K^*$ for $\omega' \in \Omega$, then $\omega' = \gamma_m\gamma_0$, i.e., $\gamma_m\gamma_0$ is the only factor of $\gamma_m\gamma_0 v_{\psi(u)}\gamma_m\gamma_0$ which is in Ω.

Let now $\omega \in K^+\gamma_0$. As we have noticed in Remark 5.16, this implies $\omega = b\gamma_0$ with $b \in K \setminus \{\gamma_0\}$. The set of factors of $\omega v_{\psi(u)}\omega$ which are in Ω is therefore $\{\gamma_m\gamma_0, \omega\}$. Since $\gamma_m\gamma_0 \preceq \omega$ we are done in this case, too.

Next, suppose $\omega \in K^+ b$ for $b \in K \setminus \{\gamma_0\}$. Then the set of factors of $\omega v_{\psi(u)}\omega$ which are in Ω is $\{\gamma_m\gamma_0, b\gamma_0, \omega\}$. Since every element ending with γ_0 is smaller than any other element in Ω, the claim holds in this case, too. □

By Lemma 5.13 we deduce that there exists a bound $t_\Omega \in \mathbb{N}$ such that every word $v \in \mathrm{IRR}_{T_\Delta}(K^*)$ with $\|v\| \geq t_\Omega$ contains a factor $\omega u\omega$ for some $\omega \in \Omega$ such that:

- $t < \|\omega u\omega\| < t_\Omega$ for all $g \in G$,
- ω is the maximal Ω-factor of $\omega u\omega$.

We are now ready to define the second set of rules over the extended alphabet K. These rules reduce long words without long repetitions of words in Δ. We denote

$$T'_\Omega = \left\{ \omega\, u\, \omega \to \omega\, v_{\psi(u)}\, \omega \;\middle|\; \begin{array}{l} \|v_{\psi(u)}\| < \|u\| < t_\Omega,\ \omega \in \Omega \text{ and} \\ \omega \text{ is the maximal } \Omega\text{-factor of } \omega u\omega \end{array} \right\}.$$

Whenever there is a shorter rule in $T'_\Omega \cup T_\Delta$ then we want to give preference to this shorter rule. Thus, the Ω-rules are

$$T_\Omega = \left\{ \ell \to r \in T'_\Omega \;\middle|\; \begin{array}{l} \text{there is no rule } \ell' \to r' \in T'_\Omega \cup T_\Delta \\ \text{such that } \ell' \text{ is a proper factor of } \ell \end{array} \right\}.$$

Let $T = T_\Delta \cup T_\Omega$. The set $\mathrm{IRR}_T(K^*)$ is finite by Lemma 5.13. Our goal is to prove confluence of T over K^*. As an auxiliary result we prove the following lemma, which is of independent interest.

Lemma 5.21. *Let $\omega \in \Omega$ and $v = \omega\gamma u\omega$ (resp. $v = \omega u\gamma\omega$) be a word with $\gamma \in \Gamma$ and with $\|\gamma u\| > \max\{\|v_g\| \mid g \in G\}$ such that ω is the maximal Ω-factor of v. Then there exists a derivation $v \overset{*}{\underset{T}{\Longrightarrow}} \omega v_{\psi(\gamma u)}\omega$ (resp. $v \overset{*}{\underset{T}{\Longrightarrow}} \omega v_{\psi(u\gamma)}\omega$).*

Proof. In order to show this, we will first prove three auxiliary claims. It suffices to consider the case $v = \omega\gamma u\omega$ since $v = \omega u\gamma\omega$ is symmetric.

Claim 1. The word v is reducible in T.

If v is reducible in T_Δ we are finished. Thus, assume that v is irreducible in T_Δ. Then either v is the left side of a rule in T'_Ω or $\|v\| > t_\Omega$. If v is the left side of a rule in T'_Ω, then either v is the left side of a rule in T_Ω or it contains a factor which is the left side of such a rule. If $\|v\| > t_\Omega$, then v contains a factor which is a rule in T_Ω by Lemma 5.13. This concludes Claim 1.

Claim 2. If $\omega\gamma u\omega \underset{T}{\Longrightarrow} v'$, then $v' = \omega\gamma' u'\omega$ where $\gamma' = \gamma$ or $\gamma' = \gamma_0$ and $u' \in K^*$.

There are three cases. The first case is that v' stems from a rule $\delta^{t+n} \to \delta^t \in T_\Delta$ and γ is contained in δ^{t+n}. Note that by $|\omega| \leq 2d < t$ the left side δ^{t+n} cannot be contained in ω. We have $\delta = \gamma$ by Equation (5.3). By Remark 5.16 the overlap of δ^{t+n} and ω is at most γ. As $t > 2d \geq 2$ this overlap and the γ are preserved and the claim is clear.

The second case is that v' stems from a rule $\delta^{t+n} \to \delta^t \in T_\Delta$ and γ is not contained in δ^{t+n}. Again we have that δ^{t+n} cannot be contained in ω. Also δ^{t+n} can at most overlap at the right ω. The overlap with ω is still in δ^t as $t > 2d \geq |\omega|$ and therefore the claim holds in this case. Thus, in the first and second case we have $\gamma' = \gamma$.

In the third case v' stems from a rule $\ell = \omega' u''\omega' \to \omega' v_{\psi(u'')}\omega' = r$ in T_Ω. If ℓ is a prefix of v, then $v' = \omega\gamma_0 u'\omega$ and $v_{\psi(u'')}$ is a prefix of $\gamma_0 u'$. Hence, the claim holds in this case. If the factor γ (in $v = \omega\gamma u\omega$) is not a factor of ℓ, then the claim is trivial. Hence, let γ be a factor of ℓ. Then γ is a factor of ω' by minimality of J. As ω is preserved at the use of the rule $\ell \to r$, the claim holds in this case too. Therefore, $v' = \omega\gamma' u'\omega$ for $\gamma' = \gamma$ or $\gamma' = \gamma_0$. This concludes Claim 2.

Note that if v is the left side of a rule, the statement of the lemma is clear. Thus, we have to study the case that v is not a left side of a rule.

Claim 3. $v \underset{T}{\Longrightarrow} v' = \omega\gamma' u'\omega \neq \omega v_{\psi(\gamma u)}\omega$ implies $\|\gamma' u'\| > \max\{\|v_g\| \mid g \in G\}$.

We therefore may assume that v is reduced to v' by some rule $\ell \to r \in T$ with $\ell \neq v$. We again use case-by-case analysis for rules in T_Δ and T_Ω.

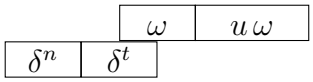
The first case is that $\ell \to r \in T_\Delta$. By definition of T_Δ we have $|r| \geq t$ and thus by $\ell \neq v$ this implies $\|v'\| \geq |v'| = |\omega\gamma' u'\omega| > t = \max\{\|\omega v_g \omega\| \mid g \in G,\ \omega \in \Omega\}$. By cancelation of ω this implies $\|\gamma' u'\| > \max\{\|v_g\| \mid g \in G\}$.

The second case is that $\ell \to r \in T_\Omega$. Thus, we have $\ell = \omega' u''\omega'$. If the rule does not apply to a prefix, then u' must contain some factor v_g and we obtain $\|u'\| \geq \|v_g\|$ for some $g \in G$. This is large enough since $\|\gamma' u'\| \geq \|v_g\| + \kappa > \max\{\|v_g\| \mid g \in G\}$. The remaining case is that the rule $\ell \to r \in T$ applies to a prefix of v. But then we must have $\omega = \omega'$. Thus, $v = \omega u''\omega x$ with $\omega x = x'\omega$ where $x' \neq 1$. This implies $\|x'\| > \kappa$ since ω is a factor of x'^+. This is large enough since $v' = \omega v_{\psi(u'')} x'\omega$ in this case. This concludes Claim 3.

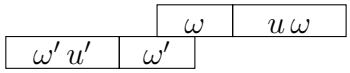
Using these claims we proceed using induction on the weight of γu. By Claim 1 the word v is reducible. Thus, let $v \underset{T}{\Longrightarrow} v'$. By Claim 2 we obtain $v' = \omega\gamma' u'\omega$ for some $\gamma' \in \Gamma$. If $\gamma' u' \neq v_{\psi(\gamma u)}$, then we obtain $\|\gamma' u'\| > \max\{\|v_g\| \mid g \in G\}$ by Claim 3. As the weight of $\gamma' u'$ is smaller than the weight of γu, we have $\psi(\gamma' u') = \psi(\gamma u)$ by construction of the rules and v' satisfies the requirements of the lemma by Claim 2 and Claim 3, we can use induction. This process stops as soon as $\gamma' u' = v_{\psi(\gamma u)}$ which concludes the proof. □

Lemma 5.22. *The system T is locally confluent over K^*.*

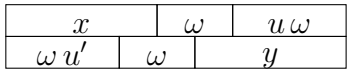
Proof. The system T_Δ is confluent by Lemma 5.12. Suppose we can apply the rules $\ell \to r \in T_\Omega$ and $\ell' \to r' \in T_\Delta$. Then ℓ' is not a proper factor of ℓ by definition of T_Ω. Moreover no ω is a factor of any δ^+, hence ℓ is not a factor of ℓ'. Thus, there are no factor critical pairs in this case. Next, we consider overlap critical pairs. Let $\ell = \omega u \omega$ and $\ell' = \delta^{t+n}$. The maximal overlap between ℓ and ℓ' is a prefix or suffix of ω. By the choice of t we have $t \geq 2d$, hence neither the application of $\ell \to r$ nor the application of $\ell' \to r'$ changes any overlap. Therefore, we can apply the rules in any order and obtain the same result:



It remains to show that T_Ω is locally confluent. By minimality of J, no $\omega \in \Omega$ is a proper factor of another word $\omega' \in \Omega$. Let $\omega u \omega \to r$ and $\omega' u' \omega' \to r'$ be two Ω-rules and first assume $\omega \neq \omega'$. By construction of T'_Ω, the left sides of both rules can overlap at most $\min\{|\omega|, |\omega'|\} - 1$ positions. Thus, the two rules can always be applied independently of one another.



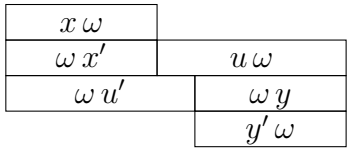
Let finally $\omega u \omega \to \omega v_g \omega$ and $\omega u' \omega \to \omega v_h \omega$ be two Ω-rules. By construction of T_Ω, the left-hand side $\omega u' \omega$ is neither a proper factor of $\omega u \omega$ nor vice versa. Suppose that these two rules are applied to $x\omega u\omega = \omega u' \omega y = \omega u'' \omega$ for $x, y \in K^+$. If $|x| \geq |\omega u'|$, then the two rules can be applied independently of one another.



Thus, we may assume $|x| < |\omega u'|$. We will show

$$x\,\omega\,v_g\,\omega \underset{T}{\overset{*}{\Longrightarrow}} \omega\,v_{\psi(u'')}\,\omega \underset{T}{\overset{*}{\Longleftarrow}} \omega\,v_h\,\omega\,y. \tag{5.4}$$

Let $x\omega = \omega x'$ for some $x' \in K^+$. If $\|x\| \leq \kappa$, then x is a prefix of ω since $\|\omega\| > \kappa$ and ω becomes a prefix of x^+. Due to $\|x\| \leq \kappa$ we have $x \in \Delta$, hence $\omega \in F$. This is a contradiction since $\Omega \subseteq J$. We obtain $\|x\| > \kappa$. Analogously, we also have $\|y\| > \kappa$ and $\omega y = y'\omega$ for some $y' \in K^+$.



Since different words in Ω are not factors of one another, every Ω-factor in $x\omega u\omega$ is either an Ω-factor in $x\omega$ or in $\omega u\omega$. By definition of the rules T_Ω, the maximal Ω-factor in $\omega u\omega$ is ω. Because of $|x\omega| < |\omega u'\omega|$ and the definition of T_Ω, the maximal Ω-factor in $x\omega$ is also ω. In particular, we have that ω is the maximal Ω-factor in $x\omega u\omega = \omega u'\omega y$. Hence, ω is still the maximal Ω-factor in $x\omega v_g\omega$ and in $\omega v_h\omega y$ by Lemma 5.20. Moreover, since $\|x'\| = \|x\| > \kappa$, we have $\|x'v_g\| > \kappa + \|v_g\| > \max\{\|v_g\| \mid g \in G\}$. The last letter of $x'v_g$ is in Γ since v_g ends in γ_0. Thus, the requirements of Lemma 5.21 are satisfied and we obtain $x\,\omega\,v_g\,\omega = \omega x'v_g\omega \underset{T}{\overset{*}{\Longrightarrow}} \omega\, v_{\psi(x'v_g)}\,\omega$. Similarly, $\omega\, v_h\,\omega y = \omega\, v_h\, y'\omega \underset{T}{\overset{*}{\Longrightarrow}} \omega\, v_{\psi(v_hy')}\,\omega$. Finally, $\psi(x'v_g) = \psi(v_hy') = \psi(u'')$ which shows Equation (5.4). □

Since all rules in T are weight-reducing, it follows from Lemma 5.22 that T is confluent. Moreover, all rules $\ell \to r$ in T satisfy $\psi(\ell) = \psi(r)$. We conclude that T is a weighted Church-Rosser system such that K^*/T is finite and $\psi : K^* \to G$ factorizes through T. It remains to study the groups in K^*/T.

Lemma 5.23. *Let $H \subseteq K^*/T$ be a subsemigroup which is a group and identify H with the corresponding elements in $\mathrm{IRR}_T(K^*)$. Then either there exists some $\delta \in \Delta$ such that $H \subseteq \{\delta^t, \ldots, \delta^{t+n-1}\}$ is a cyclic group whose order is divisible by n or there is an injective homomorphism $\eta : H \to G$.*

Proof. Without loss of generality, we may assume that H is non-trivial. Let $e^2 = e \in H$ be the identity element of H. Note that by the definition of the rules T and the set Ω, the corresponding word in $\mathrm{IRR}_T(K^*)$ of every word $w \in K^*\Omega K^*$ also contains an Ω-factor, that is, is in $K^*\Omega K^*$. Thus, by $ex = x$ and $x^{|H|} = e$ for all $x \in H$ either all elements in $H \subseteq K^*/T$ contain some factor in Ω or none of the elements contains an Ω-factor. Additionally, all words $x \in H$ which contain no Ω-factor must have length at least $t > 2d$ by the definition of the rules T_Δ and all words which contain an Ω-factor must have the same maximal Ω-factor (see Lemma 5.20).

Let us first consider the case that none of the elements contain an Ω-factor. We show that there exists some $\delta \in \Delta$ such that for all $x \in H$ there exists $i \in \mathbb{N}$ such that $x = \delta^i$. Let $u\delta^{t+n}v \underset{T_\Delta}{\Longrightarrow} u\delta^t v$ be an application of a rule in T_Δ and let $w \in J$ be a minimal factor of $u\delta^{t+n}v$ which is not in F. By Lemma 5.10 $|w| \leq 2d$ and since $t > 2d$, the factor w is also a factor of $u\delta^t v$. Thus, the number of factors in J does not decrease by an application of a rule in T_Δ. Consider any $x \in H$. Since the number of factors in J does not decrease by some application of a rule in T_Δ, $x^{|H|+1} = x$ and no rule in T_Ω is applicable, we deduce that the number of factors in J of $x^{|H|+1}$ and x is the same. In particular, this number is 0 and we obtain $x \in F$ for all $x \in H$. Next, we show that $x = \delta^i$ for some $\delta \in \Delta$. Since $x \in F$ and Δ is closed under conjugation, there exists a primitive word $\delta \in \Delta$ and $i \in \mathbb{N}$ such that $x = \delta^i\delta'$ for some prefix δ' of δ. In particular, $|\delta|$ is a period of x. Note that $i \geq 2$ since $|x| > 2d$. Consider the word $x^2 \in H$. By the above, we obtain $x^2 \in F$, that is, again there exists a primitive word $\hat{\delta} \in \Delta$, a prefix $\hat{\delta}'$ of $\hat{\delta}$ and a number $j \geq 2$ such that $x^2 = \hat{\delta}^j\hat{\delta}'$. Therefore, $\left|\hat{\delta}\right|$ is a period of x^2 and, hence, also of x. Since $|x| > 2d$, we may use Theorem 2.14 and conclude that $\gcd(|\delta|, |\hat{\delta}|)$ is a period of x. Since δ is primitive, this implies $\gcd(|\delta|, |\hat{\delta}|) = |\delta|$. Since

$\hat{\delta}$ is a prefix of x, this yields that $\hat{\delta}$ is a power of δ which implies $\delta = \hat{\delta}$ by primitivity of $\hat{\delta}$. In particular, $|\delta|$ is a period of x^2 and $\delta'\delta$ is a prefix of δ^2. Since δ is primitive this implies that δ' is not a proper prefix of δ by Lemma 2.15 and we conclude that for every $x \in H$ there exists $\delta \in \Delta$ and $i \in \mathbb{N}$ such that $x = \delta^i$. Thus, consider $\delta_1^i, \delta_2^j \in H$ with $\delta_1 \neq \delta_2$ primitive words in Δ. Again, $|\delta_1|$ is a period of δ_1^i and there must exist a period $p \leq d$ of $\delta_1^i \delta_2^j \in F$. By Theorem 2.14 $\gcd(|\delta_1|, p)$ is a period of δ_1^2. By primitivity of δ_1, this yields that $|\delta_1|$ is a divisor of p. In particular, since p is a period of $\delta_1^i \delta_2^j$, this yields $\delta_1^i \delta_2^j = \delta_1^i \delta_1^k \delta_1'$ for some $k \geq 2$ and δ_1' a prefix of δ_1. Using Theorem 2.14 again, we see that $\gcd(|\delta_1|, |\delta_2|)$ is a period of δ_2^j, that is, $|\delta_2|$ is a divisor of $|\delta_1|$ by primitivity of δ_2. By symmetry, this yields $|\delta_1| = |\delta_2|$ and thus $\delta_1 = \delta_2$.

Fix some primitive word $\delta \in \Delta$ such that $H \subseteq \delta^+$. Since $ex = x$ for all $x \in H$ and the right side of rules in T_Δ have length at least t and since δ^{t+n} is reducible, we conclude $H \subseteq \{\delta^t, \ldots, \delta^{t+n-1}\}$ and thus H is a subgroup of the cyclic group $\{\delta^t, \ldots, \delta^{t+n-1}\}$ of order n which finishes this case. The second case is that all words in H contain an Ω-factor. Consider the maximal Ω-factor of e and factorize $e = e_1 \omega e_2 \omega e_3$ with $\omega \in \Omega$ maximal for e such that $e_1\omega$ and ωe_3 contains no other factor ω. Since $e^2 = e$, we conclude that e_2 is some normal form v_g. By $ex = x = xe$ for all $x \in H$, there must exist a factorization $x = e_1 \omega \hat{x} \omega e_3$ such that $\hat{x} = v_{\psi(\hat{x})}$ is a normal form. In particular, $\widehat{xy} = v_g$ for $g = \psi(\hat{x}\omega e_3 e_1 \omega \hat{y})$ by Lemma 5.21. Consider the function $\eta : H \to G$ given by $\eta(x) = \psi(\hat{x}) \cdot \psi(\omega e_3 e_1 \omega)$. Note that $\psi(\widehat{xy}) = \psi(\hat{x})\psi(\omega e_3 e_1 \omega)\psi(\hat{y})$ and thus $\eta(x)\eta(y) = \eta(xy)$, i.e., η is a homomorphism. Since G is a group, it holds $\eta(x) = \eta(y)$ if and only if $\psi(\hat{x}) = \psi(\hat{y})$. By the definition of the normal forms v_g, it holds $\psi(\hat{x}) = \psi(\hat{y})$ if and only if $\hat{x} = \hat{y}$ and therefore η is injective. □

This finishes the proof of Proposition 5.15.

5.5 Parikh-reducing Church-Rosser systems

5.5.1 Commutative Groups have Parikh-reducing Church-Rosser systems

In this section we study Parikh-reducing Church-Rosser systems for abelian groups. Let $\varphi : A^* \to G$ be a homomorphism in an abelian group G. We construct a system for G by sorting the letters a and then reducing them modulo their order. Thus, we actually construct a Church-Rosser representation for the group $\prod_{a \in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$. The situation obtained in Theorem 5.24 is shown in the commutative diagram Figure 5.3.

Theorem 5.24. *Let $\varphi : A^* \to G$ be a homomorphism to a finite commutative group G. Then there exists a Parikh-reducing Church-Rosser system S of finite index which factorizes through φ. Further, all groups contained in A^*/S are isomorphic to some subgroup of $\prod_{a \in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$.*

Proof. Let n be the least common multiple of $\operatorname{ord}(\varphi(a))$ for $a \in A$. We do an inductive proof on the number of letters $|A|$. If $A = \{c\}$, then we may set $S = \{c^n \to 1\}$.

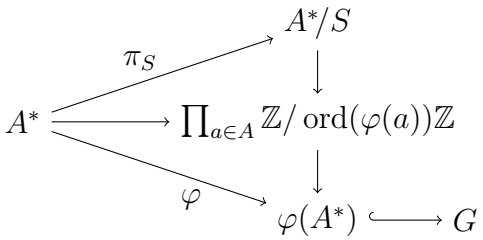


Figure 5.3: Commutative diagram in the situation of Theorem 5.24.

This system is Parikh-reducing and locally confluent and $A^*/S \simeq \mathbb{Z}/n\mathbb{Z}$. Thus, we may assume that $|A| > 1$. Let $A = \{a_1, \ldots, a_s, c\}$ be the alphabet and $c \in A$ be an arbitrary letter of A. We consider the alphabet $B = A \setminus \{c\}$. Inductively, B is smaller than A, we get a Parikh-reducing Church-Rosser system $R \subseteq B^* \times B^*$ of finite index which factorizes through $\varphi_{|B^*} : B^* \to G$. The idea is to first reduce the words over B^* and then work over a new alphabet K. Let $K = \mathrm{IRR}_R(B^*)c$ be the new alphabet of irreducible words over B^* appended by the letter c which poses as a separator. We will first construct a Parikh-reducing (over A^*) Church-Rosser system $T \subseteq K^* \times K^*$ of finite index. Note that this system T is not Parikh-reducing over K^*. We will use two different sets of rules. One for long repetitions of short words and one for longer words which are not repetitions of such short words. Let us first define the set of short words as $\Delta = K^{\leq n} \setminus \{1\}$, that is, as the set of nonempty words of length at most n. Let further be

$$T_\Delta = \left\{ \delta^{t+n} \to \delta^t \;\middle|\; \delta \in \Delta \right\}$$

with $t = 3n(s+4) + n$. The choice of the parameter t will be explained later. For now, the fact that $t > 2n$ is sufficient to obtain that T_Δ is a Parikh-reducing (over K^*, and thus also over A^*) Church-Rosser system by Lemma 5.12. Next, we will introduce marker words. They basically mark the absence of a long repetition of words in Δ, i.e., a long enough word in K^* will either contain a marker word or a rule in T_Δ. Let $F = \bigcup_{\delta\in\Delta, i\in\mathbb{N}} \mathrm{Factors}(\delta^i)$. By Lemma 5.10 we obtain $K^* \setminus F = K^*JK^*$ for some $J \subseteq K^{\leq 2n}$. In order to ensure that we find such a marker which does not start with a $c \in K$, we increase the length of a marker to $3n$. Formally, let $\Omega = K^{3n} \setminus (cK^* \cup F)$ be the set of markers.

Let $\preceq$ be a total preorder on Ω with the following properties:

- $\omega, \eta \in \Omega$ with $\omega \in K^*(K \setminus \{c\})c^i, \eta \in K^*(K \setminus \{c\})c^j$ and $i > j$ implies $\omega \preceq \eta$.
- $\preceq$ is a total order on $\Omega \setminus Kc^{3n-1}$.
- $\omega, \eta \in \Omega \cap Kc^{3n-1}$ implies $\omega \preceq \eta$.

Thus, the larger the block of c's at the suffix of an ω, the smaller it is with respect to $\preceq$. Additionally, all elements in Ω with a maximal block of c's at the suffix are equivalent with respect to $\preceq$. In particular, $\omega \preceq \eta$ and $\eta \preceq \omega$ implies either $\eta = \omega$ or there exists

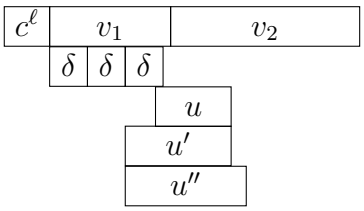


Figure 5.4: Construction of a factor in Ω as used in Lemma 5.25.

$b_1, b_2 \in K$ with $\omega = b_1 c^{3n-1}$ and $\eta = b_2 c^{3n-1}$. Let $u \in K^*\omega K^*$ for some $\omega \in \Omega$. We say that ω is a *maximal Ω-factor* of u, if $u \in K^*\eta K^*$ with $\eta \in \Omega$ implies $\eta \preceq \omega$.

Lemma 5.25. *There exists a number t_0 such that for every word $v \in K^*$ with length at least t_0 has a factor δ^{t+n} for some $\delta \in \Delta$ or a factor $\omega \in \Omega$.*

Proof. Let $t_0 = (t+n+3)(n+1)$. If $v \notin \mathrm{IRR}_{T_\Delta}(K^*)$ the statement is true. Thus, we assume that there is no factor δ^{t+n} of v for some $\delta \in \Delta$. There is a factorization $v = c^\ell v_1 v_2$ such that $v_1 \in F$ is maximal and v_1 has no c as a prefix. Hence we obtain $\ell < t+n$ and $|v_1| < (t+n)n$ which implies $|v_2| \geq 3n+3 > 3n-1$ by definition of t_0. As $v_1 \in F$, there is some $\delta \in \Delta$ which does not have c as prefix and v is a prefix of δ^+. Consider the first factor u of length $2n$ of $v_1 v_2$ which is not in F. Since v_1 is a prefix of δ^+, one must take at most $n-1$ additional letters left from u in order to obtain a factor u' of $v_1 v_2$ which is not in F, has length at most $3n$ and does not start with a c. Filling up u' with letters from the right, we obtain a factor u'' of $v_1 v_2$ which is not in F, has length $3n$ and does not start with a c, that is, $u'' \in \Omega$. □

Lemma 5.25 shows that the prerequisites of Lemma 5.13 are satisfied. Thus, there exists a number t_Ω such that every $v \in \mathrm{IRR}_{T_\Delta}(K^*)$ with $|v| \geq t_\Omega$ contains a factor $\omega\, u\, \omega'$ with ω, ω' being Ω-maximal for this factor and $t < |\omega u \omega'| < t_\Omega$. The idea is to reduce u to a normal form $\gamma(u)$. This is the part where commutativity of G is needed. Let $a \in A$ be a letter and $|u|_a$ be the number of occurrences of a in u. Define $\gamma_a(u) = a^{|u|_a \bmod \mathrm{ord}(\varphi(a))} c^{3n}$ and

$$\gamma(u) = c^{3n}\gamma_{a_1}(v) \ldots \gamma_{a_s}(v)\gamma_c(v).$$

The mapping γ is a normal form in the group $\prod_{a\in A} \mathbb{Z}/\operatorname{ord}(a)\mathbb{Z}$, i.e., let $\psi : A^* \to \prod_{a\in A} \mathbb{Z}/\operatorname{ord}(a)\mathbb{Z}$ be the homomorphism counting the different letters a modulo $\operatorname{ord}(a)$, then $\psi(u) = \psi(v)$ if and only if $\gamma(u) = \gamma(v)$. By the choice of $\gamma_a(u)$ we have $\gamma(u) \in K^*$. Since $|\gamma_a(u)| = 3n$ for $a \in B$ and $3n \leq |\gamma_c(u)| < 4n$, we obtain

$$t - 7n = 3n(s+2) \leq |\gamma(u)| < 3n(s+2) + n = t - 6n.$$

In particular, $\varphi(u) = \varphi(\gamma(u))$ and $\gamma(u\gamma(u')) = \gamma(uu') = \gamma(u'u) = \gamma(\gamma(u')u)$. Additionally, if $u \in K^*$ with $|u| \geq 3n(s+2) + n = t - 6n$, then $u \mapsto \gamma(u)$ is Parikh-reducing over A^* since at least the number of c decreases. Note that the inequality $t - n \leq |\omega\gamma(u)\omega'| < t$ is actually the reason for the definition of t. Let

$$T_\Omega = \{\omega u \omega' \to \omega\gamma(u)\omega' \mid t \leq |\omega u \omega'| < t_\Omega \text{ and } \omega, \omega' \text{ are } \Omega\text{-maximal for } \omega u \omega'\}$$

be the set of Ω-rules. By definition of γ the set of Ω-rules is Parikh-reducing over A^*. Note that for a Ω-rule, either ω and ω' are minimal elements in Ω or $\omega = \omega'$. By Lemma 5.13 the system $T = T_\Delta \cup T_\Omega$ has only finitely many irreducible elements. It remains to prove that T is Church-Rosser. By Lemma 5.12 the set T_Δ of Δ-rules is (locally) confluent. Next, we will study properties of Ω-rules which are crucial for showing that T is Church-Rosser. First, we show that T-rules preserve Ω-maximal elements.

Lemma 5.26. *Let $u \underset{T}{\Longrightarrow} v$ and let ω be a maximal Ω-factor of u. Then $\eta \preceq \omega$ for every Ω-factor η of v.*

Proof. As $T = T_\Delta \cup T_\Omega$ there are two cases for the rule set of $u \underset{T}{\Longrightarrow} v$.

In the case that $u \underset{T_\Delta}{\Longrightarrow} v$ there must exists a $\delta \in \Delta$ and a factorization $u = u_1\delta^{t+n}u_2$ such that $v = u_1\delta^t u_2$. By construction, we have $t > 3n = |\omega|$. Thus, every element of Ω is a factor of u if and only if it is also a factor of v. Since ω is Ω-maximal for u, it is also Ω-maximal for v.

If $u \underset{T_\Omega}{\Longrightarrow} v$, there is a factorization $u = u_1\omega_1\hat{u}\omega_2u_2$ such that $v = u_1\omega_1\gamma(\hat{u})\omega_2u_2$ and ω_1, ω_2 are maximal Ω-factors of $\omega_1\hat{u}\omega_2$. Since every marker in Ω has fixed length $3n$, it remains to show that $\omega_1\gamma(\hat{u})\omega_2$ has no Ω-factors larger than ω_1 (and by $\omega_1 \preceq \omega$, also no Ω-factors larger than ω). Note that $\gamma(\hat{u})$ has c^{3n} as prefix and suffix. Every Ω-factor of $\omega_1\gamma(\hat{u})$ which is not an Ω-factor of $\gamma(\hat{u})$ has the form ζc^i for some $i \geq 0$ and ζ is a suffix of ω_1. Since the block of c's at the suffix of ζc^i may only increase, we obtain $\zeta c^i \preceq \omega_1$ by definition of $\preceq$. Since every element of Ω has length $3n$ and does not have c as a prefix, there is no Ω-factor in $\gamma(\hat{u})\omega_2$ which is neither in $\gamma(\hat{u})$ nor equals ω_2. By construction, every Ω-factor of $\gamma(\hat{u})$ is of the form $\gamma_a(\hat{u})$ for some $a \in B$. However, $\gamma_a(\hat{u})$ is a minimal element of Ω by construction. In particular, $\eta \preceq \omega_1 \preceq \omega$ for every Ω-factor η of $\omega_1\gamma(\hat{u})\omega_2$. □

Next, as an intermediate step, we show local confluence in the case of a left side $\omega u\omega'$ of a rule in T_Ω. In particular, we show that every word of this form can be reduced to a fixed normal form.

Lemma 5.27. *Let $\omega u\omega'$ be a word such that ω and ω' are maximal Ω-factors of $\omega u\omega'$ and $|\omega u\omega'| \geq t$. Then $\omega u\omega' \underset{T}{\Longrightarrow} v$ implies $v \overset{*}{\underset{T}{\Longrightarrow}} \omega\gamma(u)\omega'$.*

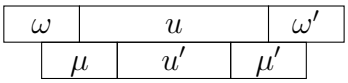
Proof. The statement is clear if $v = \omega\gamma(u)\omega'$ which is why we may assume $v \neq \omega\gamma(u)\omega'$. We show the lemma inductively on the length of $\omega u\omega'$. In order to apply the lemma on v we show that $v = \omega v'\omega'$ and $|v| \geq t$. The precondition that ω and ω' are maximal Ω-factors of v is satisfied by Lemma 5.26.

In the case of $\omega u\omega' \underset{T_\Omega}{\Longrightarrow} v$, some rule $\mu u'\mu' \to \mu\gamma(u')\mu' \in T_\Omega$ was applied. As such rules preserve the prefixes and suffixes of length $3n$, the word v must have the correct form. In the case of $\omega u\omega' \underset{T_\Delta}{\Longrightarrow} v$, some rule $\delta^{t+n} \to \delta^t$ was applied. Since $t > 6n$ and elements of Ω all have length $3n$, the Ω-factors ω and ω' are preserved by the application of the Δ-rule $\delta^{t+n} \to \delta^t$. In both cases we conclude that $v = \omega v'\omega'$ for some word v'.

It remains to show, that $|v| \geq t$. Since $|\delta^t| \geq t$, the case of an application of a rule in T_Δ is trivial. Let v stem from the application of a rule $\mu u'\mu' \to \mu\gamma(u')\mu' \in T_\Omega$. If either $\mu u'$ or $u'\mu'$ is a factor of u, we have that either $\mu\gamma(u')$ or $\gamma(u')\mu'$ is a factor of v'. Thus, using $|\gamma(u')| > t - 7n$ and $|\omega| = 3n$ for every element $\omega \in \Omega$, we obtain

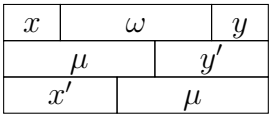
$$|v| = |\omega v'\omega'| \geq |\omega| + |\mu\gamma(u')| + |\omega'| > t + 2n > t.$$

It remains to prove $|v| \geq t$ for the situation which is depicted below.



If $\omega \neq \omega'$, then there exists $b_1, b_2 \in K \setminus \{c\}$ such that $\omega = b_1c^{3n-1}$ and $\omega' = b_2c^{3n-1}$. However, as no element of Ω starts with the letter c, we can conclude $\omega = \mu$ and thus by $\mu' \preceq \mu$ we obtain $\omega' = \mu'$ by the same argument. In this case we have $\omega u\omega' = \mu u'\mu'$ and henceforth $v = \omega\gamma(u)\omega'$. The case that $\mu \neq \mu'$ is similar: ω' has no c as prefix and thus $\mu' = \omega'$. Again, $\omega = \mu$ and $v = \omega\gamma(u)\omega'$ holds. Hence, we may assume $\omega = \omega'$ and $\mu = \mu'$.

Combining both overlaps, we obtain the following picture.

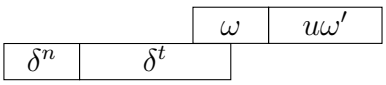


In the notation of the picture above we have $u = yu'x$. Thus, $v = \omega y\gamma(u')x\omega$ and by $\gamma(u') > t - 7n$ and $|\omega| = 3n$ it suffices to show $|x'| = |yx| \geq n$. By $\mu y' = x'\mu$ we have that μ is a factor of x'^+. We conclude $x' \notin \Delta$ which implies $|x'| > n$. In summary, $v = \omega v'\omega'$ and $|v| \geq t$ holds. If $|v| < t_\Omega$, then we can directly apply the T_Ω-rule with left side v. Else, v must be reducible by Lemma 5.13 and we can apply induction. □

Combining the previous lemmas we show that T is locally confluent.

Lemma 5.28. *T is locally confluent.*

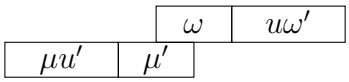
Proof. Let $\ell \to r, \ell' \to r' \in T$ be two rules. We have to show that every overlap of the left sides of those rules resolves. The system T_Δ is locally confluent by Lemma 5.12. Hence, we may assume that $\ell \to r \in T_\Omega$. Let $\omega u\omega' = \ell$ and consequently $r = \omega\gamma(u)\omega'$. Consider first the case that $\delta^{t+n} = \ell' \to r' \in T_\Delta$. If ℓ' is a factor of ℓ, that is, if $\ell = x\ell' y$, then $\ell \underset{T}{\Longrightarrow} xr'y \overset{*}{\underset{T}{\Longrightarrow}} r$ by Lemma 5.27. By definition of Ω, the left side ℓ which contains an element of Ω cannot be a factor of δ^{t+n}. Hence, the system resolves in the case of factor critical pairs. Consider thus the case of an overlap critical pair $x\ell = \ell' y$ (the case $x\ell' = \ell y$ is symmetric). Since ω is no factor of δ^+ and $t \geq 3n$ by definition, we have the following situation:



Let $\delta^t = z_1 z_2$ and $\omega = z_2 z_3$ be the overlap, then

$$x\ell \underset{T}{\Longrightarrow} xr = x\omega\gamma(u)\omega' = \delta^{t+n} z_3\gamma(u)\omega' \underset{T}{\Longrightarrow} \delta^t z_3\gamma(u)\omega' = z_1 z_2 z_3\gamma(u)\omega'$$
$$\ell' y \underset{T}{\Longrightarrow} r' y = \delta^t y = z_1\omega u\omega' \underset{T}{\Longrightarrow} z_1\omega\gamma(u)\omega' = z_1 z_2 z_3\gamma(u)\omega'$$

Consider the case that $\ell' \to r' \in T_\Omega$ and let $\ell' = \mu v \mu'$. Again, if $\ell' = x\ell y$, then $\ell' \underset{T}{\Longrightarrow} xry \underset{T}{\overset{*}{\Longrightarrow}} r'$ by Lemma 5.27. Hence, by symmetry, it suffices to consider the case $x\ell = \ell' y$. If ℓ and ℓ' overlap at most $3n$ positions,



then the rules can be applied independently; let again be $\mu' = z_1 z_2$ and $\omega = z_2 z_3$ be the overlap, then

$$x\ell \underset{T}{\Longrightarrow} xr = x\omega\gamma(u)\omega' = \mu u'\mu' z_3\gamma(u)\omega' \underset{T}{\Longrightarrow} \mu\gamma(u')\mu' z_3\gamma(u)\omega' = \mu\gamma(u') z_1 z_2 z_3\gamma(u)\omega'$$
$$\ell' y \underset{T}{\Longrightarrow} r' y = \mu\gamma(u')\mu' y = \mu\gamma(u') z_1\omega u\omega' \underset{T}{\Longrightarrow} \mu\gamma(u') z_1\omega\gamma(u)\omega' = \mu\gamma(u') z_1 z_2 z_3\gamma(u)\omega'$$

and the system resolves in this case.

Hence, we assume that ℓ and ℓ' overlap more than $3n$ positions. In this case μ' is a factor of ℓ and ω is a factor of ℓ'. This implies that μ and ω' are maximal Ω-factors of $x\ell = \ell' y = \mu u''\omega'$. We conclude $x\ell \underset{T}{\Longrightarrow} xr \underset{T}{\overset{*}{\Longrightarrow}} \mu\gamma(u'')\omega'$ and $\ell' y \underset{T}{\Longrightarrow} r' y \underset{T}{\overset{*}{\Longrightarrow}} \mu\gamma(u'')\omega'$ by Lemma 5.27. □

By construction, the system T is φ-invariant and thus the system

$$T' = \{c\ell \to cr \in A^* \times A^* \mid \ell \to r \in T\}$$

is φ-invariant. By Lemma 5.13 the system T is of finite index over K^*. We can apply Lemma 5.8 and obtain a φ-invariant Parikh-reducing Church-Rosser system S of finite index over A^*. This concludes the proof of the first part of Theorem 5.24. It remains to study the groups in A^*/S. As an intermediate step, we study the groups in K^*/T.

Lemma 5.29. *Let $H \subseteq K^*/T$ be a subsemigroup which is a group and identify H with the corresponding elements in $\mathrm{IRR}_T(K^*)$. Then either there exists some $\delta \in \Delta$ such that $H \subseteq \{\delta^t, \ldots, \delta^{t+n-1}\}$ is a cyclic group whose order is divisible by n or there is an injective homomorphism $\eta : H \to \prod_{a\in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$.*

Proof. Again, we may assume that H is non-trivial. Let $e^2 = e \in H$ be the identity element of H. Note that by the definition of the rules T and the set Ω, the irreducible word of every word $w \in K^*\Omega K^*$ also contains an Ω-factor. Thus, by $ex = x$ and $x^{|H|} = e$ for all $x \in H$ either all elements in $H \subseteq K^*/T$ contain some factor in Ω or none of the elements contains an Ω-factor. All words $x \in H$ must have length at least $t - n > 2n$ by the definition of the rules T.

The proof in the case that none of the elements contain an Ω-factor is similar to the proof of Lemma 5.23.[5]

The second case is that all words in H contain an Ω-factor. This case works as in the proof of Lemma 5.23, but we have to account for the different construction of Ω. Consider the maximal Ω-factors of e and factorize $e = e_1\omega e_2\omega' e_3$ with $\omega, \omega' \in \Omega$ maximal for e such that $e_1\omega$ and $\omega' e_3$ contains no other maximal Ω-factors of e. Since $e^2 = e$, we conclude that e_2 is some normal form. By $ex = x = xe$ for all $x \in H$ and Lemma 5.27, there must exist a factorization $x = e_1\omega\hat{x}\omega' e_3$ such that $\hat{x} = \gamma(\hat{x})$ is a normal form. In particular, $\widehat{xy} = \gamma(\hat{x}\omega' e_3 e_1 \omega \hat{y})$ by Lemma 5.27. Consider the homomorphism $\psi : A^* \to \prod_{a\in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$ which counts the number of $a \in A$ modulo $\operatorname{ord}(a)$ and the function $\eta : H \to \prod_{a\in A} \mathbb{Z}/\operatorname{ord}(a)\mathbb{Z}$ given by $\eta(x) = \psi(\hat{x}) \cdot \psi(\omega' e_3 e_1 \omega)$. Note that $\psi(\widehat{xy}) = \psi(\hat{x})\psi(\hat{y})\psi(\omega' e_3 e_1 \omega)$ implies that η is a homomorphism. It holds $\eta(x) = \eta(y)$ if and only if $\psi(\hat{x}) = \psi(\hat{y})$. By the definition of the normal forms $\gamma(\cdot)$, it holds $\psi(\hat{x}) = \psi(\hat{y})$ if and only if $\hat{x} = \hat{y}$ and therefore η is injective. □

By Lemma 5.8, we obtain that A^*/S is a Rees-extension monoid $\mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$ for some $\rho : B^*/R \to K^*/T$. By Proposition 3.6, the subgroups in A^*/S are isomorphic to subgroups of B^*/R and K^*/T. By induction, all groups in B^*/R are isomorphic to some subgroup of $\prod_{a\in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$. All groups in K^*/T are either cyclic of order divisible by n or isomorphic to some subgroup of $\prod_{a\in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$ by Lemma 5.29. However, since n is defined as the least common multiple of $\operatorname{ord}(\varphi(a))$, the cyclic group of order n is a subgroup of $\prod_{a\in A} \mathbb{Z}/\operatorname{ord}(\varphi(a))\mathbb{Z}$. This proves the statement. □

5.5.2 Group languages over an alphabet of size two

The same technique as in Subsection 5.5.1 can be used to obtain Parikh-reducing Church-Rosser systems which factorize through homomorphisms $\varphi : \{a, b\}^* \to G$ for an arbitrary group G. We will only sketch the proof, as it is essentially the proof of Theorem 5.24.

Theorem 5.30. *Let $A = \{a, b\}$ be an alphabet of size two and let $\varphi : A^* \to G$ be a homomorphism into a finite group G. Then there exists a Parikh-reducing Church-Rosser system S of finite index which factorizes through φ. All groups in A^*/S are subgroups of G or of $\mathbb{Z}/n\mathbb{Z}$ where n is the exponent of G.*

Sketch of proof. Let n be the exponent of G and let $R = \{a^n \to 1\} \subseteq \{a\}^* \times \{a\}^*$ be the set of rules over the alphabet $\{a\}$. Set $K = \mathrm{IRR}_R(a^*)b = \{a^i b \mid 0 \leq i < n\}$. In the remainder of the sketch, we have to construct a system over K^*. As the set of short words we choose $\Delta = K^{\leq n^2} \setminus \{1\}$. The corresponding set of rules is $T_\Delta = \{\delta^{t+n} \to \delta^t \mid \delta \in \Delta\}$ for $t = n^2(3n + 7)$. Note that since $t > 2n^2$ the system T_Δ is confluent by Lemma 5.12.

Let $F = \bigcup_{\delta\in\Delta, i\in\mathbb{N}} \mathrm{Factors}(\delta^i)$ and set $\Omega = K^{3n^2} \setminus (bK^* \cup F)$. Choose a preorder $\preceq$ on Ω such that

[5] Change every occurrence of d to n.

- $\omega, \eta \in \Omega$ with $\omega \in K^*(K \setminus \{b\})b^i, \eta \in K^*(K \setminus \{b\})b^j$ and $i > j$ implies $\omega \preceq \eta$.
- $\preceq$ is a total order on $\Omega \setminus Kb^{3n^2-1}$.
- $\omega, \eta \in \Omega \cap Kb^{3n^2-1}$ implies $\omega \preceq \eta$.

In order to complete the construction, it remains to choose the normal forms v_g. Note that every representation of $g \in G$ needs less than n a's by the pigeonhole principle. Thus, for every $g \in G$ there exists a word $v_g = b^{3n^2}v_1b^{3n^2}\cdots b^{3n^2}v_{n-1}b^{3n^2} \in K^*$ with $\varphi(v_g) = g$ and $v_i \in \left\{ab^k, b^k \;\middle|\; 1 \leq k \leq n\right\}$. For every $g \in G$ we choose such a word v_g such that the number of a's is minimal. Note that by construction $||v_g| - |v_h|| < n^2$ as a word over K. This is the reason for the choice of Δ. Furthermore, $t - 7n^2 < |v_g| < t - 6n^2$, which explains the choice of the parameter t. The choice of v_g also yields that there are no Ω-factors in v_g apart from ab^{3n^2}, which is Ω-minimal.

Adapting the proof of Lemma 5.25, we prove the existence of a number t_0 such that every word $v \in K^*$ of length at least t_0 has a factor δ^{t+n} for a $\delta \in \Delta$ or a factor $\omega \in \Omega$. Lemma 5.13 yields the existence of a number t_Ω such that every $v \in \mathrm{IRR}_{T_\Delta}(K^*)$ contains a factor $\omega\, u\, \omega'$ with ω, ω' being Ω-maximal for this factor and $t < |\omega u \omega'| < t_\Omega$. Again, let

$$T_\Omega = \left\{\omega u \omega' \to \omega v_{\varphi(u)} \omega' \;\middle|\; t \leq |\omega u \omega'| < t_\Omega \text{ and } \omega, \omega' \text{ are } \Omega\text{-maximal for } \omega u \omega'\right\}$$

and $T = T_\Delta \cup T_\Omega$. We want to apply Lemma 5.8 to obtain a system $S \subseteq \{a, b\}^* \times \{a, b\}^*$. Confluence of T follows along the lines of Lemma 5.26, Lemma 5.27 and Lemma 5.28, whereas the statement about the groups in A^*/S is analogously to Lemma 5.29. □

5.6 Beyond Groups

In this section we apply the local divisor technique in order to lift the construction of Church-Rosser systems for groups to the general case of monoids. Instead of directly constructing a system over $K = \mathrm{IRR}_R(B^*)c$, we obtain a system inductively by going over to the local divisor. This decreases the size of the monoid, but increases the size of alphabet.

Theorem 5.31. *Let* $\mathbf{H}$ *be a group variety such that for every homomorphism* $\varphi : A^* \to G$ *for* $G \in \mathbf{H}$ *there exists a Parikh-reducing (weight-reducing, subword-reducing) Church-Rosser system* S *of finite index which factorizes through* φ*. Let* $\varphi : A^* \to M$ *be a homomorphism with* $M \in \overline{\mathbf{H}}$*.*

1. *There exists a* φ*-invariant Parikh-reducing (weight-reducing, subword-reducing) Church-Rosser system* S *of finite index.*
2. *If every homomorphism* $\varphi : A^* \to G$ *in a group* $G \in \mathbf{H}$ *has a Church-Rosser representation in* $\overline{\mathbf{H}}$*, then* $A^*/S \in \overline{\mathbf{H}}$*.*

Proof. 1. We use induction on $(|M|, |A|)$, ordered lexicographically. Since $\overline{\mathbf{H}}$ is closed under taking submonoids, we can restrict ourselves on surjective homomorphisms φ. If M is a group, then $M \in \mathbf{H}$ and there exists such a system S by the preconditions. Thus, we can assume that there is a letter $c \in A$ such that $\varphi(c)$ is not a unit. Let $B = A \setminus \{c\}$. By induction the restriction

$$\varphi|_{B^*} : B^* \to M$$

admits a Parikh-reducing (weight-reducing, subword-reducing) Church-Rosser system $R \subseteq B^* \times B^*$. Consider the set

$$K = \mathrm{IRR}_R(B^*)c.$$

This is a prefix code and will be considered as a new alphabet (in the case of weight-reducing, the weight of a letter in K is the weight of the corresponding words over A^*). Let $\psi : K^* \to M_{\varphi(c)}$ be the homomorphism to the local divisor at $\varphi(c)$ induced via $\psi(uc) = \varphi(cuc)$. We have $\left|M_{\varphi(c)}\right| < |M|$ and $M_{\varphi(c)} \in \overline{\mathbf{H}}$ and thus, by induction, there exists a Parikh-reducing (weight-reducing, subword-reducing) Church-Rosser system $T' \subseteq K^* \times K^*$ of finite index, such that T' factorizes through ψ. In particular, we have $\psi(\ell) = \psi(r)$ for a rule $(\ell, r) \in T'$. We show that $\varphi(c\ell) = \varphi(cr)$. For this let $\ell = u_1 c \dots u_n c$ and $r = v_1 c \dots v_m c$. It holds

$$\begin{aligned}
\varphi(c\ell) &= \varphi(cu_1c) \circ \dots \circ \varphi(cu_nc) \\
&= \psi(u_1c) \circ \dots \circ \psi(u_nc) \\
&= \psi(\ell) = \psi(r) \\
&= \psi(v_1c) \circ \dots \circ \psi(v_mc) \\
&= \varphi(cv_1c) \circ \dots \circ \varphi(cv_mc) = \varphi(cr).
\end{aligned}$$

Hence, the rule $c\ell \to cr$ is φ-invariant. We set

$$T = \{c\ell \to cr \mid \ell \to r \in T'\}.$$

The system $S = R \cup T$ has the required properties by Lemma 5.8.

2. The statement is clear if M is a group. Consequently, the construction above is applied and A^*/S is isomorphic to $\mathrm{Rees}(\mathrm{B}^*/\mathrm{R}, \mathrm{K}^*/\mathrm{T}, \rho)$ for some $\rho : B^*/R \to K^*/T$ by Lemma 5.8 . By induction we may assume that $B^*/R, K^*/T \in \overline{\mathbf{H}}$ and Proposition 3.6 implies that $A^*/S \in \overline{\mathbf{H}}$. □

Corollary 5.32 ([DKW12])**.** *Every star-free language is a union of equivalence classes $[u]_S$ of some subword-reducing Church-Rosser system S of finite index.*

Proof. The star-free languages correspond to aperiodic monoids. Let $\mathbf{H} = \mathbf{I}$ be variety which contains only the trivial group. Obviously, the system $S = \{a \to 1 \mid a \in A\}$ satisfies the conditions for any homomorphism $\varphi : A^* \to \{1\}$. It is $\overline{\mathbf{I}} = \mathbf{A}$ and the corollary follows by Theorem 5.31. □

A direct combination of Theorem 5.24 and Theorem 5.31 yields the following corollary.

Corollary 5.33. *Let $M \in \overline{\mathbf{Ab}}$ be a monoid and $\varphi : A^* \to M$ be a homomorphism, then there exists a Parikh-reducing Church-Rosser system $S \subseteq A^* \times A^*$ such that S factorizes through φ and $A^*/S \in \overline{\mathbf{Ab}}$. In particular, every language $L \subseteq A^*$ recognized by φ is given as a finite union $L = \bigcup_{u \in L} [u]_S$.*

Corollary 5.34. sCRCL = REG.

Proof. The inclusion sCRCL $\subseteq$ REG is clear. Let $L \subseteq A^*$ be a regular language and let $\varphi : A^* \to M$ be a recognizing homomorphism of L. Choose length as the weight function of A^*. By Theorem 5.14, the prerequisites of Theorem 5.31 are satisfied and there exists a Church-Rosser system $S \subseteq A^* \times A^*$ of finite index which factorizes through φ. In particular, $L = \bigcup_{u \in L} [u]_S$. □

We have seen that there exist Church-Rosser representations of groups $G \in \mathbf{H}$ which are in $\overline{\mathbf{H}}$. In particular, one can control the groups in the Church-Rosser representation. However, in general one may not preserve other properties, for instance, commutativity.

Proposition 5.35. *Let $\varphi : A^* \to \mathbb{Z}/2\mathbb{Z}$ be the homomorphism mapping each letter to the generator of $\mathbb{Z}/2\mathbb{Z}$. If $|A| > 1$, there is no abelian Church-Rosser representation of φ.*

Proof. Assume that there exists a Church-Rosser system S of finite index such that A^*/S is abelian and there exists a homomorphism $\psi : A^*/S \to \mathbb{Z}/2\mathbb{Z}$ with $\varphi = \psi \circ \pi_S$. Let $a, b \in A$ be letters such that $a \neq b$. Since S factorizes through φ, we have $|r| \equiv |\ell| \bmod 2$ for every rule $(\ell, r) \in S$ and it holds $a \neq b$ in A^*/S. Since A^*/S is abelian, we obtain $ab = ba$ in A^*/S. In particular, $ab \to_S 1 \leftarrow_S ba$ and A^*/S must be a group. Let $2n$ be the order of a and b. Then $a^n = a^n b^n b^n = b^n$ holds in A^*/S and thus there must be a irreducible word w with $a^n \overset{*}{\underset{S}{\Longrightarrow}} w \overset{*}{\underset{S}{\Longleftarrow}} b^n$. By the argumentation above, there exists a number $k < n$ such that $w \in \{a^k, b^k\}$. Thus, either $a^{n-k} = 1$ or $b^{n-k} = 1$, a contradiction to the definition of n. □

5.7 Complexity of Church-Rosser systems

In this section we analyze the size of a Church-Rosser representation as constructed by Theorem 5.31 and Theorem 5.24. We will restrict our analysis on the construction of the Parikh-reducing Church-Rosser representation. Similiar calculations can be made for the system constructed in the proof of Theorem 5.14 and for the analysis of the size of the Church-Rosser system.

Before we prove upper bounds for the size of the constructed Church-Rosser systems, we reconsider the construction. All constructions used Lemma 5.8 as the basic building block of the construction. Let $\varphi : A^* \to M$ be a homomorphism. For $B = A \setminus \{c\}$ and a system $R \subseteq B^* \times B^*$ one needs a system $T \subseteq K^* \times K^*$ for the alphabet

$K = \mathrm{IRR}_R(B^*)c$. Now, unlike in the general case, we are able to reduce the alphabet itself by exploiting the structure of the alphabet. Let $b_1 \cdots b_k c \in K$ with $b_i \in B$ and $k > |M|$. By the pigeonhole principle there exist $i < j$ such that $\varphi(b_1 \cdots b_i) = \varphi(b_1 \cdots b_j)$ and $i + (k - j) \leq n$. Thus, we may introduce the subword-reducing[6] rule $b_1 \cdots b_k c \to b_1 \cdots b_i b_{j+1} \cdots b_k c$. If $b_1 \cdots b_i b_{j+1} \cdots b_k$ is reducible in R, reduce it further in R. Repeating this process yields a new alphabet for K which is a subset of $B^{\leq n}c$ and therefore, if $|B| > 1$, has at most $(|B|^{n+1} - 1)/(|B| - 1)$ elements. One can check, that the proofs of Theorem 5.31 and Theorem 5.24 also work adding this reduction technique of the alphabet K. We refrained from directly adding it to the theorems, as they are already quite technical.

Proposition 5.36. *Let $\varphi : A^* \to G$ be a homomorphism in $G \in \mathbf{Ab}$, $n = |G|$ and $m = |A| > 1$, then there exists a Parikh-reducing Church-Rosser system S such that S factorizes through φ and*

$$|A^*/S| \in 2^{2^{m^{\mathcal{O}(n^2)}}}.$$

Proof. Let S be the Parikh-reducing Church-Rosser system constructed using Theorem 5.24 and the reduction technique described above. Lemma 5.8 shows that for $m > 1$ the representation A^*/S is isomorphic to a Rees-extension monoid and thus

$$|A^*/S| = |B^*/R| + |B^*/R|^2 \cdot |K^*/T| \leq 2\,|B^*/R|^2 \cdot |K^*/T|$$

where $B = A \setminus \{c\}$. In the case of Theorem 5.24, R is constructed inductively whereas T is constructed directly. By Lemma 5.13, every irreducible word in $\mathrm{IRR}_T(K^*)$ has length less than t_Ω and therefore $|K^*/T| \leq |K|^{t_\Omega}$. The construction of t_Ω shows that $t_\Omega = 2^{|\Omega|}(t_0 + t)$ whereas $t_0 + t \in \mathcal{O}(n^2 m)$. Since $\Omega \subseteq K^{3n}$ we obtain

$$|K^*/T| \leq |K|^{\mathcal{O}(n^2 m) \cdot 2^{|K|^{3n}}}.$$

Using the alphabet reduction technique, we can assume $|K| \leq m^{n+1}$. Note that $|K|^{3n} \leq (m^{n+1})^{3n} = m^{(n+1)3n}$ does not yield another exponential jump. A straightforward calculation yields the existence of a constant $c \in \mathbb{N}$ such that

$$2\,|K^*/T| \leq 2^{2^{m^{cn^2}}}.$$

Now let $\mathrm{ms}(\varphi)$ denote the smallest size of a Parikh-reducing Church-Rosser representation of φ and set

$$\mathrm{ms}(n, m) = \max\{\mathrm{ms}(\varphi) \mid \varphi : A^* \to G, |A| \leq m, G \in \mathbf{Ab}, |G| \leq n\}$$

to be the complexity over all possible homomorphisms with $|A| \leq m$ and $|G| \leq n$. We have seen that the recursion

$$\mathrm{ms}(n, m) \leq \mathrm{ms}(n, m - 1)^2 \cdot 2^{2^{m^{cn^2}}}$$

[6] subword-reducing seen as a rule over A^*, not over K^*.

holds and show $\mathrm{ms}(n,m) \leq 2^{2^{m^{cn^2+2}}}$ inductively using this recursion. Note that $\mathrm{ms}(n,1) = n$ and thus the inequality is true in the base case $m = 2$. Also $\mathrm{ms}(1,m) = 1$ and therefore we assume $n > 1$. For $m > 2$ and $n > 1$ it holds

$$\begin{aligned}
\mathrm{ms}(n,m) &\leq \mathrm{ms}(n,m-1)^2 \cdot 2^{2^{m^{cn^2}}} \\
&\leq 2^{2^{(m-1)^{cn^2+2}+1}} \cdot 2^{2^{m^{cn^2}}} \\
&= 2^{2^{(m-1)^{cn^2+2}+1}+2^{m^{cn^2}}} \\
&\leq 2^{2^{(m-1)^{cn^2+2}+1+m^{cn^2}}} \\
&\leq 2^{2^{m^{cn^2+2}}}.
\end{aligned}$$

The last inequality holds since

$$\begin{aligned}
(m-1)^{cn^2+2} + 1 + m^{cn^2} &\leq (m-1)m^{cn^2+1} + 1 + m^{cn^2} \\
&= m^{cn^2+2} + m^{cn^2} \underbrace{(1-m)}_{<0} + 1 \\
&\leq m^{cn^2+2}.
\end{aligned}$$

□

The triple exponential upper bound given by Proposition 5.36 seems huge, however there is already a single exponential lower bound which is fairly easy to see. The lower bound comes from the fact that Church-Rosser systems cannot directly represent group identities which preserve length, such as commutation.

Proposition 5.37. *For every $n \in \mathbb{N}$ there exists a homomorphism $\varphi : A^* \to G$ into an abelian group G of size n such that for every length-reducing Church-Rosser system S which factorizes through φ all words of length smaller than n are irreducible, that is, $A^{<n} \subseteq \mathrm{IRR}_S(A^*)$. In particular, if $|A| > 1$:*

$$|A^*/S| \geq (|A|^n - 1)/(|A| - 1).$$

Proof. Consider the cyclic group G of order n and the homomorphism $\varphi : A^* \to G$ which maps all letters $a \in A$ to the same generator g of G. Let $S \subseteq A^* \times A^*$ be a length-reducing Church-Rosser system which factorizes through φ. We show that every word of length less than n is irreducible in S. Let $w \in A^*$ be a word with $|w| < n$. Assume that $w \underset{S}{\Longrightarrow} v$ for some word v. Since S is length-reducing, $|v| < |w|$. However, $\varphi(w) = \varphi(v)$ implies $g^{|w|-|v|} = 1$. Since the order of g is n, this is a contradiction to $0 < |w| - |v| < n$ and w must be irreducible. □

Note that this proof does not use the Church-Rosser property and thus one could expect a larger size of the Church-Rosser representation.

Let us consider two classes of examples on which we can give smaller upper bounds on the size of the Church-Rosser system.

Example 5.38. Niemann and Waldmann constructed an explicit system S for the case $\varphi : A^* \to \mathbb{Z}/2\mathbb{Z}$ with $\varphi(a) = 1$ for all $a \in A$ [NW02, Nie02]. Their system is given by $S = \{xyz \to \max(x, z) \mid x, y, z \in A, y = \min(x, y, z)\}$ for some arbitrary order on A. The irreducible elements in A^*/S are exactly the sequences which are first strictly increasing and then strictly decreasing, that is

$$\mathrm{IRR}_S(A^*) = \{a_1 \cdots a_i \cdots a_n \mid a_1 < \cdots < a_i \geq a_{i+1} > \cdots > a_n\}.$$

This yields $|A^*/S| = |\mathrm{IRR}_S(A^*)| = 1 + \sum_{i=1}^{|A|} 2^{2i-1} = (2^{2|A|+1}+1)/3$ which is significantly larger than the lower bound $|A| + 1$ given in Proposition 5.37. ◇

Another example where we know a class of simpler systems are the case of simple groups, see Proposition 5.6 and Corollary 5.7.

Example 5.39. Consider the construction of Proposition 5.6. We choose length as the weight function. Let $\varphi : A^* \to G$ be a homomorphism such that $\gcd\{|w| \mid \varphi(w) = 1\} = 1$ and let $n = |G|$. We first restrict the size of the set $\{u \mid \varphi(u) = 1\}$. We call a word $w \in \{u \mid \varphi(u) = 1\}$ *simple*, if no non-trivial factor of w is in $\{u \mid \varphi(u) = 1\}$.[7] In fact, if $w = xyz$, then $\gcd(|xz|, |y|, |xyz|) = \gcd(|xz|, |y|)$, which shows that one can restrict the set to simple words. Every simple word has length at most n. Let $X \subseteq \{w \mid \varphi(w) = 1, |w| \leq n\}$ such that $\gcd\{|w| \mid w \in X\} = 1$ but the greatest common divisor of every proper subset of X is greater than 1. Let $x \in X$ and p_x be a prime number which divides $\gcd\{|w| \mid w \in X \setminus \{x\}\}$. Then $p_x \leq n$ and p_x does not divide $|x|$. In particular, the numbers p_x are pairwise distinct and $\prod_{x \neq y \in X} p_y \leq n$. We conclude $|X| \in \mathcal{O}(\log(n))$ by [HW75, Theorem 415]. There exist words u, v with $|u| - |v| = 1$, $\varphi(u) = \varphi(v) = 1$ and $|u|, |v| \in n^{\mathcal{O}(\log(n))}$ by the extended Euclidean algorithm. Following the proof of Proposition 5.6, this implies the existence of normal forms v_g for $g \in G$ with $\varphi(v_g) = g$ and $|v_g| = |v_h| \in n^{\mathcal{O}(\log(n))}$ for all $g, h \in G$. Thus, this yields $|A^*/S| \in |A|^{n^{\mathcal{O}(\log(n))}}$, that is, a sub-double exponential upper bound for the size of the Church-Rosser representation in this case. ◇

In the monoid case, the minimal size of a Church-Rosser representation is bounded by a quadruple exponential function. This increase in complexity, compared to the group case, comes from the fact that, unlike in the group case, the system $T \subseteq K^* \times K^*$ is constructed by induction. However, this is also the reason that the alphabet reduction technique is even more powerful in this case. Consider the function $f : \mathbb{N}^2 \to \mathbb{N}$ given by $f(1, m) = 1$, $f(n, 1) = n$ and $f(n, m) = 2f(n, m-1)^2 \cdot f(n-1, f(n, m-1))$ for $n, m > 1$. This function gives an upper bound for the maximal size of a Church-Rosser representation of a monoid of size n and an alphabet of size m without any optimization. Consider further the hyperoperation function $A_1(n) = 2n$, $A_k(1) = 2$ and $A_k(n) = A_{k-1}(A_k(n-1))$.[8] For fixed k, the function A_k is primitive recursive, however the two-variable function A grows faster than any primitive recursive function, see e.g. [DW83].

[7] The motivation of the notion *simple word* is, that a simple word corresponds to a simple path in the Cayley graph.

[8] The notation A comes from Ackermann, since the function A is a modified *Ackermann function*.

An induction shows that $f(n,m) \geq A_{n-1}(m)$ for $n > 1, m \geq 1$. Hence, without the alphabet reduction the recursive formula would yield a non-primitive recursive function.

Proposition 5.40. *Let $\varphi : A^* \to M$ be a homomorphism in $M \in \overline{\mathbf{Ab}}$, $n = |M|$ and $m = |A|$. Then there exists a Parikh-reducing Church-Rosser system S such that S factorizes through φ and*

$$|A^*/S| \in 2^{2^{m^{\mathcal{O}((n+1)!)}+n}}.$$

Proof. If $M \in \mathbf{Ab}$, we know that there exists such a system S with $|A^*/S| \in 2^{2^{m^{\mathcal{O}(n^2)}}}$ by Proposition 5.36. If $m = 1$, then there exists a system S such that $|A^*/S| \leq n$. In the other case we will use the local divisor construction of Theorem 5.31. Note that by the alphabet reduction technique we may assume that $|K| < m^{n+1}$.

Let $\mathrm{ms}(\varphi)$ denote the smallest size of a Parikh-reducing Church-Rosser representation of φ and set

$$\mathrm{ms}(n,m) = \max\left\{\mathrm{ms}(\varphi) \;\middle|\; \varphi : A^* \to M, |A| \leq m, M \in \overline{\mathbf{Ab}}, |M| \leq n\right\}$$

to be the complexity over all possible homomorphisms with $|A| \leq m$ and $|M| \leq n$.

The base cases are $m = 1$ or M is a group. For $m = 1$ there exists a system of size n. In all other cases we have the following recursion formula for $\mathrm{ms}(n,m)$:

$$\mathrm{ms}(n,m) \leq 2\mathrm{ms}(n,m-1)^2 \cdot \mathrm{ms}(n-1,m^{n+1}).$$

Note that $n > 1$ since M is not a group. Choose $c \in \mathbb{N}$ such that $\mathrm{ms}(n,m) \leq 2^{2^{m^{c(n+1)!}+n}}$ for all base cases. This is possible since the group case is in $2^{2^{m^{\mathcal{O}(n^2)}}}$. We show that

$$\mathrm{ms}(n,m) \leq 2^{2^{m^{c(n+1)!}+n}}$$

in general. Inductively, it holds

$$\begin{aligned}
\mathrm{ms}(n,m) &\leq 2\mathrm{ms}(n,m-1)^2 \cdot \mathrm{ms}(n-1,m^{n+1}) \\
&\leq 2 \cdot 2^{2^{(m-1)^{c(n+1)!}+n+1}} \cdot 2^{2^{(m^{n+1})^{cn!}+n-1}} \\
&= 2^{1+2^{(m-1)^{c(n+1)!}+n+1}+2^{m^{c(n+1)!}+n-1}} \\
&\leq 2^{2^{m^{c(n+1)!}+n}}.
\end{aligned}$$

The last inequality holds because for $n, m > 1$

$$\begin{aligned}
(m-1)^{c(n+1)!} &\leq (m-1)^2 \cdot m^{c(n+1)!-2} \\
&= m^{c(n+1)!} - (2m-1)m^{c(n+1)!-2} \\
&\leq m^{c(n+1)!} - 3
\end{aligned}$$

and thus $(m-1)^{c(n+1)!} + n + 1 < m^{c(n+1)!} + n - 1$. □

Chapter 6

Conclusion and Future Work

In this thesis we studied the theory and applications of local divisors in formal language theory. The concept of Rees extensions arises naturally in the study of local divisors. In Chapter 3 we examined these Rees extensions. A monoid M which is not a group is a divisor of a Rees extension of a proper submonoid and a proper local divisor of M. In particular, the variety $\overline{\mathbf{H}}$ is generated by $\mathbf{H}$ and closure under Rees extensions. This led to the notion Rees decomposition trees. We have shown that there exists such a tree of size at most $\mathcal{O}(3^{|M|/3})$.

In Chapter 4 we studied the language class associated with $\overline{\mathbf{H}}$ over finite and infinite words. We gave two characterizations for the language class $\overline{\mathbf{H}}(A^\infty)$. The first characterization is the localizable closure of $\mathbf{H}$. This characterization was obtained by analyzing the usual proof scheme when using local divisors as one takes the closure under all operations needed in this proof scheme. The second characterization is the language class $\mathrm{SD}_{\mathbf{H}}(A^\infty)$. It gives a language description which is mainly based on group-controlled stars, a concept build on prefix codes of bounded synchronization delay.

In Chapter 5 we considered Church-Rosser congruential languages as an example of the local divisor technique. We have shown that all regular languages are Church-Rosser congruential. Since local divisors of groups are the group itself, this is a two step process. First, one has to show the result in the group case, only. Second, one can use the local divisor technique to obtain the general result rather easily. Moreover, the construction yields that for a monoid $M \in \mathbf{V}$ there exists a Church-Rosser representation in $\overline{\mathbf{G} \cap \mathbf{V}}$. Mostly, this is because the inductive construction in Subsection 5.3.1 directly yields a Rees extension of smaller systems.

Parikh-reducing Church-Rosser systems are a stronger variant of Church-Rosser systems, requiring that the rules are Parikh-reducing. We adapted the construction from the result that groups have a Church-Rosser representation in order to show that all abelian groups have a Parikh-reducing Church-Rosser representation. This adaption is quite technical and with slight changes is also used to show that groups have a Parikh-reducing Church-Rosser representation in the two generator case.

The last part of Chapter 5 dealt with the size of Church-Rosser representations. A priori, the analysis of the recursion yields that the size of our construction in the monoid case is bounded by a non-primitive function. However, using an alphabet reduction technique we were able to show that there exists a Church-Rosser representation whose

size is bounded by a quadruple exponential function.

For future work, we will briefly present some open problems.

1.) The synthesis theorem, stated as Theorem 3.2, decomposes finite semigroups into Rees matrix semigroups. This decomposition satisfies natural algebraic properties, see [RA73]. Which algebraic properties hold for the decomposition in Rees extensions as stated in Lemma 3.7?

2.) Is there a Rees decomposition tree of sub-exponential size?

3.) We have seen that $\mathrm{Rees}(\mathbf{V}, \mathbf{V}) = \mathbf{V}$ is equivalent to $\mathbf{V} = \overline{\mathbf{V} \cap \mathbf{G}}$. Are there similar results for one-sided application of Rees extensions, that is, is $\overline{\mathbf{H}}$ the smallest variety $\mathbf{V}$ such that $\mathrm{Rees}(\mathbf{H}, \mathbf{V}) = \mathbf{V}$ or $\mathrm{Rees}(\mathbf{V}, \mathbf{H}) = \mathbf{V}$?

4.) In Corollary 4.13 we have seen that languages described by $(\mathrm{FO} + \mathrm{MOD}_q)[<]$ are exactly the languages in $\mathrm{SD}_{\mathbf{Gsol_P}}$ for $P = \left\{ d \in \mathbb{N} \;\middle|\; d \mid q^d \right\}$. Is there a direct proof of this result, avoiding Straubings result $(\mathrm{FO} + \mathrm{MOD}_q)[<] = \overline{\mathbf{Gsol_P}}$ which is based on the Krohn-Rhodes decomposition?

5.) It is known that $\mathbf{A} \circledcirc{m} \mathbf{H} \subsetneq \overline{\mathbf{H}}$ by [Ste05]. Is there a language characterization of $\mathbf{A} \circledcirc{m} \mathbf{H}$ which does not need complementation but relies on prefix codes with bounded synchronization delay?

6.) Does there exist a finite Parikh-reducing Church-Rosser representation for every homomorphism into a finite group? (The case for every finite monoid can then be deduced with Theorem 5.31)

7.) Which algebraic properties can be preserved by Church-Rosser representations? For example, it seems unlikely that every homomorphism into a finite group has a Church-Rosser representation which is a group again, although it may happen in some special cases.

8.) Are there constructions for Church-Rosser representations which yield a better upper bound?

9.) The lower bound of Proposition 5.37 is not sharp. What is a good lower bound for the size of a Church-Rosser representation?

Bibliography

[AK16] Jorge Almeida and Ondřej Klíma. On the irreducibility of pseudovarieties of semigroups. *Journal of Pure and Applied Algebra*, 220(4):1517–1524, 2016. (Cited on pages 26, 28, and 32.)

[Arn85] André Arnold. A syntactic congruence for rational ω-languages. *Theoretical Computer Science*, 39:333–335, 1985. (Cited on page 15.)

[Bir35] Garrett Birkhoff. On the structure of abstract algebras. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:433–454, 1935. (Cited on page 16.)

[Bir88] Jean-Camille Birget. The synthesis theorem for finite regular semigroups, and its generalization. *Journal of Pure and Applied Algebra*, 55(1):1–79, 1988. (Cited on page 26.)

[BO93] Ron Book and Friedrich Otto. *String-Rewriting Systems*. Springer-Verlag, 1993. (Cited on pages 11 and 21.)

[BO98] Gerhard Buntrock and Friedrich Otto. Growing context-sensitive languages and Church-Rosser languages. *Information and Computation*, 141:1–36, 1998. (Cited on page 48.)

[BR84] Jean-Camille Birget and John L. Rhodes. Almost finite expansions of arbitrary semigroups. *Journal of Pure and Applied Algebra*, 32(3):239–287, 1984. (Cited on page 44.)

[BR89] Jean-Camille Birget and John L. Rhodes. Group theory via global semigroup theory. *Journal of Algebra*, 120(2):284–300, 1989. (Cited on page 44.)

[CB71] Rina S. Cohen and Janusz A. Brzozowski. Dot-depth of star-free events. *Journal of Computer and System Sciences*, 5(1):1–16, 1971. (Cited on page 48.)

[CP61] Alfred H. Clifford and Gordon B. Preston. *The Algebraic Theory of Semigroups, Volume I*. Number 7 in Mathematical Surveys. American Mathematical Society, 1961. (Cited on page 26.)

[CS14] Alfredo Costa and Benjamin Steinberg. The Schützenberger category of a semigroup. *Semigroup Forum*, pages 1–17, 2014. (Cited on page 31.)

[DG06] Volker Diekert and Paul Gastin. Pure future local temporal logics are expressively complete for Mazurkiewicz traces. *Information and Computation*, 204:1597–1619, 2006. Conference version in LATIN 2004, LNCS 2976, 170–182, 2004. (Cited on page 9.)

[DK15a] Volker Diekert and Manfred Kufleitner. Omega-rational expressions with bounded synchronization delay. *Theory of Computing Systems*, 56:686–696, 2015. (Cited on pages 9, 14, 34, and 36.)

[DK15b] Volker Diekert and Manfred Kufleitner. A survey on the local divisor technique. *Theoretical Computer Science*, 610:13–23, 2015. (Cited on pages 9 and 36.)

[DKRH16] Volker Diekert, Manfred Kufleitner, Gerhard Rosenberger, and Ulrich Hertrampf. *Discrete Algebraic Methods. Arithmetic, Cryptography, Automata and Groups*. Walter de Gruyter, 2016. (Cited on page 31.)

[DKRW12] Volker Diekert, Manfred Kufleitner, Klaus Reinhardt, and Tobias Walter. Regular languages are Church-Rosser congruential. In Artur Czumaj, Kurt Mehlhorn, Andrew Pitts, and Roger Wattenhofer, editors, *International Colloquium Automata, Languages and Programming (ICALP) 2012, Conference Proceedings, Part II*, volume 7392 of *Lecture Notes in Computer Science*, pages 177–188. Springer-Verlag, 2012. (Cited on pages 6 and 52.)

[DKRW15] Volker Diekert, Manfred Kufleitner, Klaus Reinhardt, and Tobias Walter. Regular languages are Church-Rosser congruential. *J. ACM*, 62:39:1–39:20, November 2015. (Cited on pages 6, 22, 47, 48, 50, and 52.)

[DKS12] Volker Diekert, Manfred Kufleitner, and Benjamin Steinberg. The Krohn-Rhodes theorem and local divisors. *Fundamenta Informaticae*, 116(1-4):65–77, 2012. (Cited on page 9.)

[DKW12] Volker Diekert, Manfred Kufleitner, and Pascal Weil. Star-free languages are Church-Rosser congruential. *Theoretical Computer Science*, 454:129–135, 2012. (Cited on pages 9, 10, 26, 49, 52, and 75.)

[DR95] Volker Diekert and Grzegorz Rozenberg, editors. *The Book of Traces*. World Scientific, Singapore, 1995. (Cited on page 18.)

[DW83] Martin D. Davis and Elaine J. Weyuker. *Computability, Complexity, and Languages*. Academic Press, 1983. (Cited on page 79.)

[DW16] Volker Diekert and Tobias Walter. Characterizing classes of regular languages using prefix codes of bounded synchronization delay. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages,*

and Programming (ICALP 2016), Leibniz International Proceedings in Informatics (LIPIcs), pages 129:1–129:13, 2016. (Cited on pages 6, 11, 14, 25, 33, and 36.)

[Eil76] Samuel Eilenberg. *Automata, Languages, and Machines*, volume B. Academic Press, New York and London, 1976. (Cited on pages 11 and 18.)

[FW65] Nathan J. Fine and Herbert S. Wilf. Uniqueness theorems for periodic functions. *Proc. Amer. Math. Soc.*, 16:109–114, 1965. (Cited on page 20.)

[GG65] Solomon W. Golomb and Basil Gordon. Codes with bounded synchronization delay. *Information and Control*, 8(4):355–372, 1965. (Cited on page 33.)

[Gre51] James A. Green. On the structure of semigroups. *Annals of Mathematics*, 54:163–172, 1951. (Cited on page 25.)

[HU79] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison-Wesley, 1979. (Cited on page 11.)

[HW75] Godfrey H. Hardy and Edward M. Wright. *Introduction to the Theory of Numbers*. Oxford University Press, 1975. (Cited on page 79.)

[KB70] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford, 1970. (Cited on page 22.)

[KR65] Kenneth Krohn and John L. Rhodes. Algebraic theory of machines. I: Prime decomposition theorem for finite semigroups and machines. *Transactions of the American Mathematical Society*, 116:450–464, 1965. (Cited on page 26.)

[KRT68] Kenneth Krohn, John L. Rhodes, and Bret Tilson. The prime decomposition theorem of the algebraic theory of machines. In Michael A. Arbib, editor, *Algebraic Theory of Machines, Languages, and Semigroups*, chapter 5, pages 81–125. Academic Press, New York and London, 1968. (Cited on page 26.)

[Kuf14] Manfred Kufleitner. Star-free languages and local divisors. In *DCFS 2014, Proceedings*, volume 8614 of *Lecture Notes in Computer Science*, pages 23–28. Springer, 2014. (Cited on page 9.)

[LS62] Roger C. Lyndon and Marcel-Paul Schützenberger. The equation $a^M = b^N c^P$ in a free group. *Michigan Math. J.*, 9(4):289–298, 1962. (Cited on page 20.)

[Mey72] Kurt Meyberg. Lectures on algebras and triple systems. Technical report, University of Virginia, Charlottesville, 1972. (Cited on page 9.)

[MNO88] Robert McNaughton, Paliath Narendran, and Friedrich Otto. Church-Rosser Thue systems and formal languages. *J. ACM*, 35(2):324–344, 1988. (Cited on pages 48 and 51.)

[Nar84] Paliath Narendran. *Church-Rosser and related Thue systems*. PhD thesis, Dept. of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, NY, USA, 1984. (Cited on page 48.)

[Nie00] Gundula Niemann. Regular Languages and Church-Rosser Congruential Languages. In Rudolf Freund and Alica Kelemenova, editors, *Proceedings of the International Workshop Grammar Systems 2000*, pages 359–370, Silesian University at Opava, Faculty of Philosophy and Science, Institute of Computer Science, 2000. (Cited on page 48.)

[Nie02] Gundula Niemann. *Church-Rosser Languages and Related Classes*. Kassel University Press, 2002. PhD thesis. (Cited on pages 47, 48, and 79.)

[NO05] Gundula Niemann and Friedrich Otto. The Church-Rosser languages are the deterministic variants of the growing context-sensitive languages. *Information and Computation*, 197:1–21, 2005. (Cited on page 48.)

[NW02] Gundula Niemann and Johannes Waldmann. Some regular languages that are Church-Rosser congruential. In *DLT'01, Proceedings*, volume 2295 of *LNCS*, pages 330–339. Springer, 2002. (Cited on pages 47, 48, 50, 51, and 79.)

[Pin86] Jean-Éric Pin. *Varieties of Formal Languages*. North Oxford Academic, London, 1986. (Cited on pages 11 and 17.)

[PP04] Dominique Perrin and Jean-Éric Pin. *Infinite words*, volume 141 of *Pure and Applied Mathematics*. Elsevier, Amsterdam, 2004. (Cited on pages 16 and 34.)

[PS65] Luigi Petrone and Marcel-Paul Schützenberger. Sur un problème de McNaughton. manuscrit, 12 pages, 1965. Euratom. (Cited on page 19.)

[RA73] John L. Rhodes and Dennis Allen. Synthesis of the classical and modern theory of finite semigroups. *Advances in Mathematics*, 11(2):238–266, 1973. (Cited on pages 26 and 82.)

[Ree40] David Rees. On semi-groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 36:387–400, 1940. (Cited on page 26.)

[Rho70] John L. Rhodes. Algebraic theory of finite semigroups. Algebre Theorie Nombres, Sem. P. Dubreil, M.-L. Dubreil-Jacotin, L. Lesieur et C. Pisot 23(1969/70), no. 10, 1970. (Cited on page 26.)

[Rho86a] John L. Rhodes. Infinite iteration of matrix semigroups I. Structure theorem for torsion semigroups. *Journal of Algebra*, 98(2):422–451, 1986. (Cited on page 26.)

[Rho86b] John L. Rhodes. Infinite iteration of matrix semigroups II. Structure theorem for arbitrary semigroups up to aperiodic morphism. *Journal of Algebra*, 100(1):25–137, 1986. (Cited on page 26.)

[RS09] John L. Rhodes and Benjamin Steinberg. *The $\mathfrak{q}$-theory of finite semigroups.* Springer Monographs in Mathematics. Springer, 2009. (Cited on page 26.)

[RT68] John L. Rhodes and Bret Tilson. Local structure theorems for finite semigroups. In Michael A. Arbib, editor, *Algebraic Theory of Machines, Languages, and Semigroups*, chapter 7, pages 147–190. Academic Press, New York and London, 1968. (Cited on page 26.)

[RT03] Klaus Reinhardt and Denis Thérien. Some more regular languages that are Church Rosser congruential. In *13. Theorietag, Automaten und Formale Sprachen, Herrsching, Germany*, pages 97–103, 2003. (Cited on page 49.)

[Sch65] Marcel-Paul Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8:190–194, 1965. (Cited on pages 18 and 19.)

[Sch74] Marcel-Paul Schützenberger. Sur les monoides finis dont les groupes sont commutatifs. *Rev. Française Automat. Informat. Recherche Opérationnelle Sér. Rouge*, 8(R-1):55–61, 1974. (Cited on pages 34, 37, and 42.)

[Sch75] Marcel-Paul Schützenberger. Sur certaines opérations de fermeture dans les langages rationnels. In *Symposia Mathematica, Vol. XV (Convegno di Informatica Teorica, INDAM, Roma, 1973)*, pages 245–253. Academic Press, 1975. (Cited on pages 9, 10, and 34.)

[Ste05] Benjamin Steinberg. On Aperiodic Relational Morphisms. *Semigroup Forum*, 70(1):1–43, 2005. (Cited on pages 33 and 82.)

[Str79a] Howard Straubing. Aperiodic homomorphisms and the concatenation product of recognizable sets. *Journal of Pure and Applied Algebra*, 15(3):319–327, 1979. (Cited on page 33.)

[Str79b] Howard Straubing. Families of recognizable sets corresponding to certain varieties of finite monoids. *Journal of Pure and Applied Algebra*, 15(3):305–318, 1979. (Cited on page 34.)

[Str94] Howard Straubing. *Finite Automata, Formal Logic, and Circuit Complexity.* Birkhäuser, Boston, Basel and Berlin, 1994. (Cited on page 39.)

[STT95] Howard Straubing, Denis Thérien, and Wolfgang Thomas. Regular languages defined with generalized quantifiers. *Information and Computation*, 118(2):289–301, 1995. (Cited on page 39.)

[Sus28] Anton Suschkewitsch. Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit. *Mathematische Annalen*, 99(1):30–50, 1928. (Cited on page 26.)

[Tho90] Wolfgang Thomas. Automata on infinite objects. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, chapter 4, pages 133–191. Elsevier Science Publishers B. V., 1990. (Cited on pages 15 and 16.)

[Thu10] Axel Thue. Die Lösung eines Spezialfalles eines generellen logischen Problems. *Skr. Vid. Kristianaia I. Mat. Naturv. Klasse*, 8, 1910. (Cited on page 20.)

[Thu14] Axel Thue. Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln. *Skr. Vid. Kristianaia I. Mat. Naturv. Klasse*, 10/34, 1914. (Cited on page 20.)

[Woi01] Jens R. Woinowski. *Church-Rosser Languages and Their Application to Parsing Problems*. PhD thesis, TU Darmstadt, 2001. (Cited on page 48.)

[Woi03] Jens R. Woinowski. The context-splittable normal form for Church-Rosser language systems. *Information and Computation*, 183:245–274, 2003. (Cited on page 48.)

[Zei67] Paul Zeiger. Yet another proof of the cascade decomposition theorem for finite automata. *Mathematical Systems Theory*, 1(3):225–228, 1967. (Cited on page 26.)

Nomenclature

$*$ semidirect product

1 identity element of a monoid

2^M power set of M

$[u]_S$ set of $\overset{*}{\underset{S}{\Longleftrightarrow}}$ equivalent words to u

$[w]_\varphi$ set of $\approx_\varphi$ equivalent words to w

$\|\cdot\|$ weight

$|\cdot|$ length

$|\cdot|_c$ number of c's

$\mathbf{A}$ variety of finite aperiodic monoids

Exp(M) Birget-Rhodes expansion

CRCL set of Church-Rosser congruential languages

$\overset{*}{\underset{S}{\Longleftrightarrow}}$ reflexive, symmetric, transitive closure of the rewriting relation

Δ set of short words

$\diamondsuit_\varphi M$ Schützenberger product of M

$\exp(G)$ exponent of a group G

Factors(w) set of factors of w

Gsol variety of solvable groups

$\ker\varphi$ kernel of φ

$\mathrm{Loc}_{\mathbf{H}}(A^\infty)$ localizable closure on $\mathbf{H}$

$\mathrm{Loc}_G(A^\infty)$ localizable closure on G

LocRees($\mathbf{H}$) closure of $\mathbf{H}$ under local Rees extensions

LocRees(N, $\mathrm{M_c}$) local Rees extension

$\circledcirc$ Mal'cev product

$\mathbb{N}$ set of all natural numbers

$\mathbb{Z}$ set of all integers

$\mathcal{A}$ finite deterministic automaton

$\mathcal{O}$ BigO class

TM($\mathcal{A}$) transition monoid of $\mathcal{A}$

Ω set of marker words

ord(g) order of a group element g

$\overrightarrow{L}$ arrow language of L

$\preceq$ divisor relation

Prefixes(w) set of prefixes of w

$\prod$ direct product, Cartesian product

$\overset{}{\underset{S}{\Longrightarrow}}$ rewriting relation

Rees($\mathbf{H}$) closure of $\mathbf{H}$ under Rees extensions

Rees(N, M, ρ) Rees extension on ρ

REG regular languages

sCRCL set of strongly Church-Rosser congruential languages

$\mathrm{SD}_{\mathbf{H}}$ synchronized delay class on $\mathbf{H}$

SD_G synchronized delay class on G

$\sim_\varphi, \approx_\varphi$ recognizability relation

$\simeq$ isomorphism relation

$\mathrm{Synt}(L)$ syntactic monoid of L

$\times$ direct product, Cartesian product

I trivial variety

Ab variety of abelian groups

H some variety of finite groups

$\mathbf{V}(A^\infty)$ class of languages recognized by some monoid in $\mathbf{V}$

$\mathbf{V}, \mathbf{W}$ varieties

G variety of all finite groups

φ, ψ, γ homomorphisms

A, B alphabets

a, b, c letters

A^* set of finite words over A

A^∞ set of finite and infinite words over A

A^ω set of infinite words over A

$A^{\leq n}$ set of words of length at most n

e idempotent

G, H groups

$L(\mathcal{A})$ language recognized by $\mathcal{A}$

L, K languages

M, N monoids

M_c local divisor of M at c

S, T rewriting systems

T_Δ set of Δ-rules

T_Ω set of Ω-rules

u, v, w words

v_g normal form of g

Index