Recognisable languages over free algebras

Kei Tsi Daniel Cheng

PhD

University of York
Mathematics

June 2021.

Abstract

This thesis considers notions of recognisability for languages over (universal) algebras. The main motivation here is the body of work on recognisable languages over the free monoid, which in particular connects several, equivalent, approaches. The free monoid X^* on a set X consists of all finite strings of elements of X; these are thought of as words, and hence a subset of X^* is known as a language (i.e. a collection of words). The term is then used for a subset of any (free) algebra.

Our first approach to recognisability is via finite index of syntactic congruences; the latter may be defined for any kind of algebra. We consider how to define syntactic congruences in the most efficient way: absolutely, or with regard to a particular class of algebras or languages. We give examples where only finitely many terms are needed to determine syntactic congruences. For a particular class of free algebras we find an infinite list of terms, each built from the previous, and give an example of a language such that we need to check terms of every kind. Using syntactic congruences we consider closure properties of recognisable languages. We give many examples, including critical examples of languages that are themselves free algebras (in some sense) but are contained in the free inverse monoid.

Our second approach is in the context of unary monoids. We introduce a new kind of formal machine we call a $+$-automaton. Our main result in this regard is to show that a language over a free unary monoid has syntactic congruence of finite index if and only if it is recognised by a $+$-automaton. This result exactly parallels the well known result for languages over free monoids.

Contents

List of Figures

Preface

One of the most celebrated interactions between mathematics and theoretical computer science is the study of *languages*, beginning with and motivated by the classic theory of languages over free monoids, which we briefly recall. The free monoid X^* on a set X consists of all finite strings of elements of X; these are thought of as words, and hence a subset L of X^* is known as a language. The heirarchy now known as the Chomsky Heirarchy [3] classifies languages according to their complexity and was put forward by the American intellectual Noam Chomsky in 1956. At the lowest level of the heirarchy we have the class of *recognisable* languages. From the point of view of monoid and semigroup theory, free monoids play a significant role, since (almost by definition) every monoid is a morphic image of a free one. Free monoids are combinatorially simple devices, and although congruences on monoids are notoriously complex one can hope to handle congruences on free monoids with more ease. One characterisation of recognisability of a language L over a free monoid X^* is that its syntactic congruence $\sim_L$ has finite index, that is, $X^*/\sim_L$ is a finite monoid. Another is that L is recognised by a finite state device we refer to as an automaton; these are the simplest kind of 'abstract machine' and change states according to their inputs from a finite set. If that set is X, then strings of inputs are simply words over X. The sets consisting of words taking an automaton from an initial state to a final state form precisely the class of recognisable languages over X. There are several other characterisations of recognisable languages, but we focus in this thesis on the two given above. For further details on the many approaches to recognisable languages over free monoids, we refer the reader to [10, 21, 26, 30]. As indicated in those texts the most significant names in the early days of establishing the deep connections between automata, recognisable languages over the free monoid, and finite monoids and monoids include M.P. Schützenberger, R. McNaughton, J.A. Brzozowski and I. Simon. There is also a connection with formal logic, explored by authors such as H. Straubing.

Given the body of work on languages over free monoids, it is natural to consider the relation between algorithmic and algebraic properties of subsets of other free algebras, or indeed, of other algebras. For consistency these are also referred to as languages. There is a large body of literature, mostly in the realm of theoretical computer science and logic, on this topic. Elements of free algebras are expressed by terms, and these have a tree-like structure in that they are built up from sub-terms by using the basic operations of the algebra. This has led to a study in theoretical computer science of languages over trees, and tree automata (see, for example, [9, 6]). This direction of study is not concerned with the algebraic properties of free algebras [22, 1].

We take a different viewpoint. A particular motivation for us has been [34] "On free inverse monoid languages" by Pedro V. Silva [34]. This itself builds on ideas of reversible automata [35]; see also [27]. The reasons for taking this as our starting point are several. First, free inverse monoids have a natural description as a type of bi-rooted tree called a Munn tree [29]; this is equivalent to a formulation using prefix closed subsets of reduced words over free groups, and as these are easier to write down, our results are phrased in those terms. An excellent account may be found in [21]. Inverse monoids form a variety of unary algebras where the unary operation is written $a \mapsto a^{-1}$. Free inverse monoids are naturally associated with automata for which one can reverse the transitions [34]. They form the perfect bridge to other varieties of unary and biunary monoids. For example, a monoid congruence on an inverse monoid is a unary monoid congruence, but this is not true of other varieties of unary monoids. From another point of view, free left restriction monoids (which coincide with free left ample monoids) are contained as submonoids of of free inverse monoids, closed under a unary operation $a \to aa^{-1} = a^+$. A similar statement is true for free restriction monoids (which coincide with free ample monoids); these are contained as submonoids of free inverse monoids, closed under the unary operation $a \to aa^{-1} = a^+$ and $a \mapsto a^* = a^{-1}a$.

The variety of left restriction monoids and the bigger variety of left Ehresmann monoids form the main specific varieties of unary monoids that we consider. Similarly, the variety of restriction monoids and the bigger variety of Ehresmann monoids form the main specific varieties of biunary monoids that we consider. These varieties have importance since they arise from many directions (and hence have acquired many names), are very natural in that there are many examples made from mappings. Of particular note is that every left restriction monoid embeds into the full transformation monoid $\mathcal{T}_X$ on a set X, where the unary operation is $\alpha \mapsto I_{\operatorname{im}\alpha}$, and the monoid of binary relations on a set X is Ehresmann. It follows from the work on relation algebras (see, for example, [18]) that not every Ehresmann semigroup is a subalgebra (as a biunary semigroup) of some relation semigroup. For an introduction to the topic of representability by semigroups of relations augmented with extra operations, see [32]. The theory of (left) Ehresmann and (left) restriction semigroups has been pushed forward by many authors in recent years. We recommend [19] for a survey of the development of some of the ideas and [13, 14, 2, 24, 23] for background to the free algebras in these classes.

The structure of this thesis is as follows. In Chapter 1 we give all the necessary premliminaries to follow the work in this thesis, in particular an introduction to (left) ample monoids (Section 1.1), (left) restriction monoids (Section 1.2), (left) Ehresmann monoids (Section 1.3), automata (Section 1.5), the free inverse monoid (Section 1.4), Schützenberger products (Section 1.6) and universal algebra (Section 1.7). We give references to further reading in those sections.

In Chapter 2 we consider syntactic congruences on universal algebras. If $L \subseteq A$ where A is an algebra, then the *syntactic congruence* defined on A by L is the largest congruence such that L is a union of $\sim_L$-classes. We show in Lemma 2.1.5 that $\sim_L$ always exists and in Theorem 2.1.7 that it may be defined by considering only unary term operations. Syntactic congruences have also been considered in [4, 8] and there is some overlap here. However, these articles are focussed on the relation of syntactic congruences to other special congruences. We then consider syntactic congruences on left Ehresmann monoids (and hence also on left restriction and left ample monoids), where here we can reduce the term operations we need to consider to two kinds. We note that [8] also tackles the question of reducing the list of unary term operations one considers, but uses the classification of algebras according to whether the varieties in question are finitely-generated and congruence distributive; we do not know whether the varieties we consider have these properties but prove all our results directly. We then consider (two-sided) Ehresmann monoids which, perhaps surprisingly, are harder to handle, even in the restriction case. We give an infinite (but nevertheless specific) list of unary terms that determine the syntactic congruence in Theorem 2.3.3. We give a number of illustrations, and in Subsection 2.3.3 present an example of a language over a free restriction monoid such that no finite sub-list of the terms will suffice to determine the syntactic congruence.

In Chapter 3 we consider further syntactic congruences on arbitrary universal algebras. In Theorem 3.0.5 we prove a result that allows us to pull back information from an algebra to its preimage, and show how this may be applied. Our next task is to consider the closure properties under Boolean operations of classes of recognisable languages, which we do in Section 3.2. For languages over free unary monoids it makes sense to also consider product. In Proposition 3.2.9, using an adaptation of the construction of Schützenberger product, we show that the class of recognisable languages over unary monoids is closed under product.

Chapter 4 returns to the focus on specific classes of free algebras; here is free unary monoids. We introduce the notion of +-automata, which are finite state automata equipped with an additional binary operation on their state set. As for ordinary automata, they come in two kinds, deterministic and non-deterministic, and we show that this does not matter in the sense the classes of languages accepted are the same. Our main result of this chapter is Theorem 4.2.6, which shows that a language over a free unary monoid has syntactic congruence of finite index if and only if it is accepted by a +-automaton.

Throughout we have illustrated our results and techniques by looking at languages over free (left) restriction monoids. These monoids are contained (in a sense described earlier) in free inverse monoids. In Chapter 5 we consider the syntactic congruences of the free ample monoid, the free left ample monoid and the free monoid on a set X within the free inverse monoid $\mathrm{FIM}(X)$ on X. We also consider the syntactic congruence of the 'linear' subset on $\mathrm{FIM}(X)$. Here we find some nice behaviour: in the first two cases, the congruence is related to the least group congruence on $\mathrm{FIM}(X)$ and in the latter two cases, the syntactic congruence is forced to be trivial.

Acknowledgements

With my full gratitude I would like to express my thanks to God that has made things happen. It is beyond words.

I am thankful to my Ph.D. supervisor Victoria Gould, for her kindness and support, also for her guidance, partience, postive attitude and belief in me. Her suggestion and encouragement have helped me along the way and I am lucky to have her as my supervisor.

I am grateful for my Department's support, particularly the other member of my TAP panel, Brent Everitt, and support staff Nicholas Page.

In addition, I would like to thank Kar Ping Shum, Roland Wong, Chee Chen Tung and Philip Wu from Hong Kong for their private financial sponsorship. I would also like to acknowledge my Department's financial support by scholarships in return for some teaching and The Institute of Mathematics and its Applications for the part-time opportunity. I would like to thank Victoria Gould, Kar Ping Shum and Mee Lin Luk, whom had made great effort in pushing things forward, including the whole applying process in 2014 and 2015.

It has been a pleasure to meet Stuart Jackson-Bayles, Open Door Practitioner in my University, and Ka Lok Chan, social worker in Stewards Take Your Way Clubhouse in Hong Kong, and I am particularly grateful for them talking and listening when I encounter emotional and mental problem. Also, it is so grateful to Glen and Honey Farmer I know in York Vineyard Church. Glen accompanied me every time to see the early intervention team, and the couple took care of my parents when they came to York when I was in hosiptal.

Last but not least, I am fortunate to have such loving family. I would like to thank my family who accompany me and take good care of my living during the Leave of Absence and after resuming study.

Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References.

Chapter 1

Preliminaries

In this chapter we include the definitions, essential properties and results fundamental to the understanding of mathematics in this thesis. We assume the reader has a working knowledge of semigroup theory, as may be found in [21] and [5]. We usually denote a monoid by M and the set of idempotents of M by $E(M)$.

Much of monoid theory (and, more broadly, semigroup theory) focusses on the existence and behaviour of idempotents. We recall that a monoid M is *regular* if for each $a \in M$ there exists $b \in M$ such that $a = aba$. If in addition we have $b = bab$ then we say that b is an *inverse* of a; we may denote an inverse of a by a'. Note that every element in a regular monoid has an inverse: if there exists b such that $aba = a$, then define $a' = bab$ and observe that

$$aa'a = ababa = aba = a, \quad a'aa' = bababab = babab = bab = a'.$$

It is well known that M is regular if and only if every $\mathcal{R}$-class of M contains an idempotent or, equivalently, every $\mathcal{L}$-class contains an idempotent. Indeed, if $a = aba$ then $ab \,\mathcal{R}\, a \,\mathcal{L}\, ba$ and $ab, ba \in E(M)$. Here $\mathcal{R}$ and $\mathcal{L}$ are Green's relations $\mathcal{R}$ and $\mathcal{L}$, which form the backbone of the classical theory of regular semigroups. If M is regular and the idempotents of M commute, so that $E(M)$ is a semilattice (a commutative semigroup of idempotents), then the idempotent in the $\mathcal{R}$-class of a is unique, as is the idempotent in the $\mathcal{L}$-class of a. Further, every element of a has a unique inverse, which we may denote by a^{-1}. So, in an inverse monoid we have a unary operation $a \mapsto a^{-1}$. From this we can also construct unary operations $a \mapsto aa^{-1} = a^+$ and $a \mapsto a^{-1}a = a^*$. Throughout this thesis we will be equipping monoids with additional unary operations. If M has one additional basic[1] unary operation we say that M is a *unary* monoid and if M has two additional basic operations we say it is a *biunary monoid*. Many of the algebras studied in this thesis are unary or biunary monoids, which arose in attempts to generalise the theory of regular monoids.

[1]See Section 1.7: we mean it is preserved by morphisms, substructures etc.

In Section 1.1 we give the background to (left) ample monoids. These were introduced by Fountain in [11] and [12] and were earlier called (left) type A. In Section 1.2 we take the same approach to weakly (left) E-ample/restriction monoids; these arose from many sources, in particular as an attempt to model partial maps. In Section 1.3 we give a brief introduction to (left) Ehresmann and (left) adequate monoids, which extend the classes of (left) restriction and (left) ample monoids. Lawson in [25] was key to highlighting the significance of (left) Ehresmann monoids. The foregoing classes of monoids may be approached from two directions, one as monoids and the other as biunary or unary monoids. Inverse monoids are also unary monoids; we present in Section 1.4 the free inverse monoid $\mathrm{FIM}(X)$ using the approach of McAlister triples.

We then change tack and in Section1.5 we give a brief recap of the theory of automata over free monoids. In Section 1.6 we give an introduction to Schützenberger product of monoids, which we need to adapt to a specific purpose in Section 3.2. Finally in Section 1.7 we give a brief summary of the notions of universal algebra that we will use.

1.1 (Left) ample monoids

The results here are well known. Readers may refer to [16] for further details and reference. There are three ways to approach left ample monoids. We begin with their representation by maps, and take this as our definition.

Definition 1.1.1. A monoid M is *left ample* if it is isomorphic to a submonoid of a symmetric inverse monoid $\mathcal{I}_X$ which is closed under the unary operation $\alpha \mapsto \alpha^+$, where $\alpha^+ = \alpha\alpha^{-1} = I_{\mathrm{dom}\,\alpha}$, i.e. the identity map on the domain $\mathrm{dom}\,\alpha$ of α. *Right ample* monoids are defined dually. That is, a monoid is right ample if it isomorphic to a submonoid of $\mathcal{I}_{X'}$ which is closed under the unary operation $\alpha \mapsto \alpha^*$, where $\alpha^* = \alpha^{-1}\alpha = I_{\mathrm{im}\,\alpha}$. We say that a monoid M is *ample* if it is both left and right ample; note that we cannot assume $X = X'$.

Clearly inverse monoids are ample, but the latter class is much wider: ample monoids are not in general regular.

We now explain how (left, right) ample monoids have abstract characterisations obtained from the generalizations $\mathcal{R}^*$ and $\mathcal{L}^*$ of Green's relations $\mathcal{R}$ and $\mathcal{L}$ respectively, and as such form quasi-varieties of algebras.

The relation $\mathcal{R}^*$ is defined on a monoid M by the rule that for any $a, b \in M$, $a \mathrel{\mathcal{R}^*} b$ if and only if for all $x, y \in M$,

$$xa = ya \quad \text{if and only if} \quad xb = yb.$$

It is easy to see that $\mathcal{R}^*$ is left congruence, and we show here that $\mathcal{R}^*$ is a generalisation of $\mathcal{R}$.

Lemma 1.1.2. *For any monoid M, we have $\mathcal{R} \subseteq \mathcal{R}^*$, and $\mathcal{R} = \mathcal{R}^*$ if M is regular.*

Proof. Suppose $a \mathcal{R} b$, then $a = bs$ and $b = at$ for some $s, t \in M$. For all $x, y \in M$, if $xa = ya$, then $xb = xat = yat = yb$. Dually, if $xb = yb$, then $xa = xbs = ybs = ya$. So $a \mathcal{R}^* b$ and hence $\mathcal{R} \subseteq \mathcal{R}^*$.

Suppose that M is regular and let $a, b \in M$ with $a \mathcal{R}^* b$. Then for all $x, y \in M$, $xa = ya$ if and only if $xb = yb$. Let $x = 1$, the identity of the monoid, and $y = aa'$, where a' is an inverse of a, as certainly $a = aa'a$, then $a \mathcal{R}^* b$ implies $b = aa'b$. Similary, substitute $x = 1$, and $y = bb'$ gives $a = bb'a$. Hence $a \mathcal{R} b$. $\square$

If M is left ample, then it follows from our definition that $E(M)$ is a semilattice, every $a \in M$ is $\mathcal{R}^*$-related to a unique idempotent and, denoting this idempotent by a^+ we have that $(xe)^+x = xe$, for any $x \in M, e \in E(M)$. Indeed, these conditions provide an alternative description of left ample monoids.

Our third promised description is as a quasi-variety. Let M be a unary monoid, that is, a monoid with an additional basic unary operation, which we denote by $a \mapsto a^+$. Then M is left ample if and only if it satisfies the quasi-identities:

$$x^+x = x,\ x^+y^+ = y^+x^+,\ (x^+y)^+ = x^+y^+,\ xy^+ = (xy)^+x$$

and

$$xz = yz \Rightarrow xz^+ = yz^+.$$

In this case, a^+ is the unique idempotent in the $\mathcal{R}$-class of a, and $E(M) = \{a^+ : a \in M\}$. Note that the only non-identity is $xz = yz \Rightarrow xz^+ = yz^+$. This cannot be replaced by an identity since, if it could, the class of left ample monoids would form a variety and hence be closed under morphic image. To see that the latter could not possibly hold, it is enough to consider the free monoid on a set X^* which is left ample with $a^+ = \epsilon$ for all $a \in X^*$; if left ample monoids formed a variety every monoid would be left ample, which is clearly nonsense.

The relation $\mathcal{L}^*$ is the dual of $\mathcal{R}^*$ and may be used in a dual way to give an abstract characterization of right ample monoids. The unique idempotent in the $\mathcal{L}^*$-class of a, where it exists, would be denoted by a^*. Right ample monoids form a quasi-variety of unary monoids, with defining (quasi)-identities the left/right dual of those above. A monoid is *ample* if it is both left and right ample; hence ample monoids form a quasi-variety of biunary monoids, where we take both sets of (quasi)-identities as our defining set. In the case if M is inverse, then $a^+ = aa^{-1}$ and $a^* = a^{-1}a$ for all $a \in M$; clearly, any inverse monoid is certainly ample.

Note that any submonoid of an inverse monoid that is closed under $^+$ and * is ample. However, it is undecidable whether a finite ample monoid embeds as a submonoid of an inverse monoid in a way that preserves both $+$ and $*$ [17].

1.2 Weakly (left) E-ample/(left) restriction monoids

In this section, we are extending the class of (left) ample monoids in an analogous way to the way in which (left) ample monoids extend the class of inverse monoids. That is, we consider further extensions of Green's relations $\mathcal{R}$ and $\mathcal{L}$. The reader may refer to [14] for further details and references.

Let E be a set of idempotents contained in a monoid M; at this stage we do not insist that $E = E(M)$. The relation $\widetilde{\mathcal{R}}_E$ on M is defined by the rule that for any $a, b \in M$, $a \, \widetilde{\mathcal{R}}_E \, b$ if and only if for all $e \in E$,

$$ea = a \quad \text{if and only if} \quad eb = b,$$

that is, a and b has the same set of left identities from E. The relation $\widetilde{\mathcal{R}}_E$ is certainly an equivalence; however, unlike the cases for $\mathcal{R}$ and $\mathcal{R}^*$, it need not be left compatible. The following shows that $\widetilde{\mathcal{R}}_E$ contains $\mathcal{R}^*$.

Lemma 1.2.1. *For any monoid M and $E \subseteq E(M)$, we have $\mathcal{R} \subseteq \mathcal{R}^* \subseteq \widetilde{\mathcal{R}}_E$, with both inclusions equalities if M is regular and $E = E(M)$.*

Proof. With Lemma 1.1.2 at hand, we only need to prove $\mathcal{R}^* \subseteq \widetilde{\mathcal{R}}_E$ and $\widetilde{\mathcal{R}}_E \subseteq \mathcal{R}$ if M is regular and $E = E(M)$. Also, the proof itself is somewhat similar to Lemma 1.1.2. Suppose $a \, \mathcal{R}^* \, b$, substituting $x = e$ for some $e \in E$ and $y = 1$ in the definition of $\mathcal{R}^*$ will see that $a \, \widetilde{\mathcal{R}}_E \, b$, and hence $\mathcal{R}^* \subseteq \widetilde{\mathcal{R}}_E$.

Suppose that M is regular and $E = E(M)$. Suppose $a \, \widetilde{\mathcal{R}}_E \, b$, so that for all $e \in E$, we have $ea = a$ if and only if $eb = b$. Now substitute $e = aa'$, as certainly $aa'a = a$ then $aa'b = b$. On the other hand, substitute $e = bb'$, giving $bb'a = a$. Hence $a \, \mathcal{R} \, b$, and we can conclude that $\widetilde{\mathcal{R}}_E \subseteq \mathcal{R}$. $\square$

In general, however, the inclusions in Lemma 1.2.1 can be strict. Similarly we have:

Lemma 1.2.2. *If $e, f \in E$, then $e \, \mathcal{R} \, f$ if and only if $e \, \mathcal{R}^* \, f$ if and only if $e \, \widetilde{\mathcal{R}}_E \, f$.*

Proof. From Lemma 1.2.1, we know that

$$e \, \mathcal{R} \, f \Rightarrow e \, \mathcal{R}^* \, f \Rightarrow e \, \widetilde{\mathcal{R}}_E \, f.$$

To prove

$$e \, \widetilde{\mathcal{R}}_E \, f \Rightarrow e \, \mathcal{R} \, f,$$

we see that if $e \, \widetilde{\mathcal{R}}_E \, f$, by definition of $\widetilde{\mathcal{R}}_E$, we have $ef = f$ and $fe = e$, and this in turn implies $e \, \mathcal{R} \, f$. $\square$

Note that for an arbitrary set E of idempotents in M, any idempotent $e \in E$ is a left identity of its $\widetilde{\mathcal{R}}_E$-class, as we now show:

Lemma 1.2.3. *If $a \widetilde{\mathcal{R}}_E\, e$, then $ea = a$.*

Proof. By the definition of $\widetilde{\mathcal{R}}_E$, $a \widetilde{\mathcal{R}}_E\, b$ if and only if

$$\forall e \in E, \quad ea = a \quad \text{if and only if} \quad eb = b.$$

Let $b = e$, the right hand side holds as e is an idempotent. Then left hand side gives us $ea = a$. $\square$

For any monoid where idempotents commute, the set of commutative idempotents form a semilattice. For if e, f are idempotents, and $ef = fe$, then $(ef)^2 = efef = eeff = ef$.

Lemma 1.2.4. *If E is a semilattice, $e, f \in E$ and $e \widetilde{\mathcal{R}}_E\, f$, then $e = f$.*

Proof. By definition of $\widetilde{\mathcal{R}}_E$, since $e \in E$, $ee = e$ implies $ef = f$. As $\widetilde{\mathcal{R}}_E$ is symmetric, $f \widetilde{\mathcal{R}}_E\, e$, and hence $fe = e$. Now since E is commutative, we have $fe = ef$, and hence $e = f$. $\square$

It is then easy to see that if E form a commutative subsemigroup of M, or simply we say E is a semilattice, then any $\widetilde{\mathcal{R}}_E$-class contains at most one idempotent from E. If every $\widetilde{\mathcal{R}}_E$-class does have an idempotent of E, we again have a unary operation $a \mapsto a^+$, where a^+ is now the unique idempotent of E in the $\widetilde{\mathcal{R}}_E$-class of a.

Definition 1.2.5. Let M be a monoid and $E \subseteq E(M)$. Then M is *weakly left E-ample* (or *left restriction*) if and only if E is a semilattice, every $\widetilde{\mathcal{R}}_E$-class contains an idempotent of E, the relation $\widetilde{\mathcal{R}}_E$ is a left congruence, and the left ample identity (AL) holds:

$$ae = (ae)^+a \quad \forall a \in M \text{ and } e \in E \qquad (AL).$$

As in the previous section, we can define left restriction monoids by a representation. It is a fact that M is left restriction if and only if M is a submonoid of some partial transformation semigroup on X, $\mathcal{PT}_X$, closed under $+$, where here again α^+ is the identity in the domain of α. It is clear that a left ample monoid is left restriction.

It is important to note that if M is a weakly left E-ample monoid, then $E = \{a^+ : a \in M\}$. We refer to E as the *distinguished semilattice* or the *semilattice of projections* of M. Moreover, the identity of M must lie in E, for we must have that $1^+ = 1$. In the case that $E = E(M)$, we drop the "E" from the notation and terminology, for example, we write $\widetilde{\mathcal{R}}_{E(M)}$ more simply as $\widetilde{\mathcal{R}}$.

The relation $\widetilde{\mathcal{L}}$ and $\widetilde{\mathcal{L}}_E$ are the dual of $\widetilde{\mathcal{R}}$ and $\widetilde{\mathcal{R}}_E$; Similar to the ample cases, weakly right E-ample monoids (right restriction monoids) may be defined in terms of these relations, where again we denote the dual of the operation $^+$ by *. Combining together, a monoid is *weakly E-ample* if it is both left and right weakly E-ample where

$$E = \{a^+ : a \in M\} = \{a^* : a \in M\}.$$

The latter condition ensures that the semilattices of projections of M as a left and as a right restriction monoid coincide.

Now we give some technical results which will be useful in subsequent chapters. Note since all ample monoids are weakly E-ample, results for the latter also apply to the former. The first follows immediately from the fact that in a weakly left (right) E-ample monoid, $\widetilde{\mathcal{R}}_E$ ($\widetilde{\mathcal{L}}_E$) is a left (right) congruence. The relation $\leq$ appearing in its statement is the natural partial order on E : given $e, f \in E$, we define $e \leq f$ if there exists $g \in E$ such that $e = gf$.

Lemma 1.2.6. *Let M be a weakly left E-ample monoid. Then for any $a, b \in M$ and $e \in E$:*

(i) $e^+ = e$;

(ii) $(ab)^+ = (ab^+)^+$;

(iii) $(ea)^+ = ea^+$;

(iv) $(ab)^+ \leq a^+$.

Proof. (i) e^+ and e are both idempotent in the $\widetilde{\mathcal{R}}_E$-class of e, by Lemma 1.2.4, they must be the same.

(ii) b has a unique idempotent from E in its $\widetilde{\mathcal{R}}_E$-class, namely b^+. So $b \;\widetilde{\mathcal{R}}_E\; b^+$. As $\widetilde{\mathcal{R}}_E$ is a left congruence, $ab \;\widetilde{\mathcal{R}}_E\; ab^+$. This means they have the same idempotent from E in their $\widetilde{\mathcal{R}}_E$-class, so $(ab)^+ = (ab^+)^+$.

(iii) Substituting $a = e$ and $b = a$ in (ii), we have $(ea)^+ = (ea^+)^+$. However as E is a semilattice, $ea^+ \in E$. So $(ea)^+ = (ea^+)^+ = ea^+$.

(iv) Since $ab \,\widetilde{\mathcal{R}}_E\, (ab)^+$ we have

$$a^+(ab) = ab \quad \Leftrightarrow \quad a^+(ab)^+ = (ab)^+.$$

But $a^+(ab) = (a^+a)b = ab$, so that $a^+(ab)^+ = (ab)^+$. Hence we have $(ab)^+ \leq a^+$. $\square$

Lemma 1.2.7. *Let M be a weakly right E-ample monoid. Then for any $a, b \in M$ and $e \in E$:*

(i) $e^* = e$;

(ii) $(ab)^* = (a^*b)^*$;

(iii) $(ae)^* = a^*e$;

(iv) $(ab)^* \leq b^*$.

Proof. Dual of Lemma 1.2.6. □

It is worth noting that the condition for $^+$ in Lemma 1.2.6 (ii) above is actually equivalent to saying Ker^+ is a left congruence. Here $\mathrm{Ker}^+ = \{(a,b) : a^+ = b^+\}$ is the kernel of the $^+$-operation. If M is a left restriction monoid, the $^+$ operation maps every element to the idempotent of its $\widetilde{\mathcal{R}}_E$-class. Thus $\mathrm{Ker}^+ = \widetilde{\mathcal{R}}_E$, and the later is a left congruence by the definition of left restriction monoid. However, even if we relax the condition that requires M to be a left restriction monoid, but only requires the $^+$ operation to be an idempotent operation ($(x^+)^+ = x^+$), the equation in Lemma 1.2.6 (ii) still equivalent to saying Ker^+ is a left congruence. This is summed up by the following:

Lemma 1.2.8. *If $x \mapsto x^+$ is a unary operation on a monoid and $(x^+)^+ = x^+$, then $(xy)^+ = (xy^+)^+$ if and only if Ker^+ is a left congruence.*

Proof. Recall that $a\ (\mathrm{Ker}^+)\ b \Leftrightarrow a^+ = b^+$.

We prove the ($\Leftarrow$) first. If Ker^+ is a left congruence, then for all a we have

$$a^+ \ \mathrm{Ker}^+ \ a$$

which implies that for all a, b,

$$ba^+ \ \mathrm{Ker}^+ \ ba$$

and so

$$(ba^+)^+ = (ba)^+.$$

Note the above is not true without using the condition $(x^+)^+ = x^+$.

Now we proceed with the other way ($\Rightarrow$). Suppose that $(ba^+)^+ = (ba)^+$, for all $a, b \in M$. If $a \ \mathrm{Ker}^+ \ b$, we have $a^+ = b^+$. So for any c,

$$\begin{aligned}(ca)^+ &= (ca^+)^+ = (cb^+)^+ \\ &= (cb)^+,\end{aligned}$$

so $ca \ \mathrm{Ker}^+ \ cb$. □

Similar to left ample monoids, we have another description of left restriction monoids, this time, as a variety. Let M be a unary monoid, then M is left restriction if and only if it satisfies the identities:

$$x^+x = x,\ x^+y^+ = y^+x^+,\ (x^+y)^+ = x^+y^+,\ xy^+ = (xy)^+x.$$

In this case, a^+ is the unique idempotent in the $\widetilde{\mathcal{R}}_E$-class of a, and we have that $E = \{a^+ : a \in M\}$. Dually, M is right restriction if and only if satisfies the left/right dual of the above, with $^+$ replaced by $*$, and restriction if it satisfies both sets of identities together with

$$(x^+)^* = (x^*)^+ \text{ and } (x^*)^+ = x^+.$$

The latter identities are to guarantee that the semilattices projections of M as a left/right restriction monoid coincide.

If M is an inverse monoid, the natural partial order of M is defined by

$$u \leq v \Leftrightarrow u = uu^{-1}v.$$

In a left ample monoid or left restriction monoid M, we have something similar, in which the *natural partial order* of M is defined by

$$u \leq v \quad \Leftrightarrow \quad u = u^+v.$$

In the above we can replace u^+ by any $e \in E$, since if $u = ev$ then $u^+v = (ev)^+v = ev^+v = ev = u$. Clearly then the restriction of $\leq$ to E coincides with the usual semilattice ordering.

Lemma 1.2.9. *Let M be a left restriction monoid. The natural partial order defined above is actually a partial order compatible with the multiplication.*

Proof. 1. (reflexivity) $u \leq u$, since $u^+u = u$.

2. (antisymmetry) If $u \leq v$ and $v \leq u$, $u = u^+v$ and $v = v^+u$. So we have $u = u^+v^+u$. Since E is a semilattice,

$$u = v^+u^+u = v^+u = v.$$

3. (transitivity) If $u \leq v$ and $v \leq w$, $u = u^+v$ and $v = v^+w$ then we have $u = u^+v^+w$. Since E is a semilattice, $u^+v^+ \in E$ so by the above observation we have $u \leq w$.

It is clear that $\leq$ is right compatible. To see that it is left compatible suppose $u \leq v$ so that $u = ev$ or some $e \in E$. Then if $w \in M$ we have

$$wu = w(ev) = (we)v = (we)^+wv,$$

so that $wu \leq wv$, as required. $\square$

Note that if M is restriction and $u = ev$, where $e \in E$, then $u = v(ev)^*$; together with the dual observation we see that the natural order in M may be defined as a left or as a right restriction monoid, with no ambiguity.

1.3 (Left) Ehresmann monoids and (left) adequate monoids

In this section, we define the classes of (left) Ehresmann monoids and (left) adequate monoids. The former are varieties and the latter quasi-varieties. (Left) Ehresmann monoids extend the class of left restriction monoids and (left) adequate monoids extend the class of (left) ample monoids. Essentially, we obtain these classes by dropping the conditions allowing us to change the position of idempotents ($ae = (ae)^+a$, etc.). However, in doing so, we need to lengthen our list of (quasi)-identities. Note that we do not have the neat representation theorems, even in the one-sided case, that we saw in Section 1.1 or Section 1.2.

Definition 1.3.1. Let M be a monoid. Then M is a *left Ehresmann monoid* if and only if there is a subset $E \subseteq E(M)$ such that E is a semilattice, every $\widetilde{\mathcal{R}}_E$-class contains an idempotent of E, and the relation $\widetilde{\mathcal{R}}_E$ is a left congruence. Right Ehresemann monoids are defined dually and a monoid is Ehresmann if it is left and right Ehresmann with respect to the same E.

We say that E is the *distinguished semilattice* of M, or *the semilatice of projections.*

Also, similarly, we have another description of left Ehresmann monoids, this time, as a variety with signature (2,1,0). According to [15], let M be a unary monoid, then M is left Ehresmann if and only if it satisfies the identities:

$$x^+x = x,\ (x^+)^+ = x^+,\ x^+y^+ = y^+x^+,\ (x^+y^+)^+ = x^+y^+,$$

$$x^+(xy)^+ = (xy)^+,\ (xy)^+ = (xy^+)^+.$$

Putting $E = \{a^+ : a \in M\}$ it follows from the identities that E is a semilattice, called the distinguished semilattice or the semilattice of projections. We have also that a^+ is the unique idempotent in the $\widetilde{\mathcal{R}}_E$-class of a.

A unary monoid (where we denote the unary operation by $a \mapsto a^*$) is right Ehresmann if it satisfies the left/right dual of the identities governing left Ehresmann monoids. A binunary monoid is Ehresmann if it satisfies the identities of both left and right Ehresmann monoids, together with $(a^+)^* = a^+$ and $(a^*)^+ = a^*$, which again give that the semilattices of projections coincide.

For completeness we give the definition of a (left) adequate monoid, although we will not need to use this in what follows.

Definition 1.3.2. Let M be a monoid. Then M is a left adequate monoid if and only if $E(M)$ is a semilattice and every $\mathcal{R}^*$-class contains an idempotent of E. Right adequate monoids are defined dually and a monoid is adequate if it is left and right adequate.

Clearly, (left) ample monoids are (left) adequate. The converse is not true in general. We do not comment further here on (left) adequate monoids, although they may be defined by quasi-identities.

1.4 The free inverse monoid $\mathrm{FIM}(X)$ on X

We begin by recalling the construction of the free inverse monoid $\mathrm{FIM}(X)$, implicitly using the construction of an E-unitary inverse semigroup from a McAlister triple. Our account follows that in [21] and [14]. The reader is also referred to [29] and [31]. We first outline the construction of the free monoid and the free group for clarity and completeness.

To begin with, let X be a non-empty set, which is often referred as an *alphabet*. By a *word* w over X we mean a finite string $w = x_1 \cdots x_n$, where $x_i \in X$, $1 \leq i \leq n$ and $n \geq 0$; the length of w is n. The empty string, which has length 0, is also considered as a word, which is normally denoted by ϵ or 1. The free monoid, which is denoted by X^*, is given by

$$X^* = \{w \mid w \text{ is a word over } X\},$$

where the binary operation is juxtaposition. We often associate $x \in X$ with the corresponding word of length 1 in X^* by the standard embedding.

We can define a partial order relationship $\leq$ in X^*. Given $v, w \in X^*$, we say that

$$w \leq v \quad \text{if and only if} \quad w = vw' \text{ for some } w' \in X^*.$$

In this case we say v is a *prefix* of w.

To describe free groups, we get the help from the description of free monoid. Given a non-empty set X, let $X^{-1} = \{x^{-1} : x \in X\}$ be a set in one-one correspondence with X in a way such that $X \cap X^{-1} = \emptyset$. Consider the free monoid on $X \cup X^{-1}$. A word $w \in (X \cup X^{-1})^*$ is *reduced* if it contains no sub-word of the form xx^{-1} or $x^{-1}x$. If we can turn $w \in (X \cup X^{-1})^*$ into another $v \in (X \cup X^{-1})^*$ through a process of insertion and deletion of sub-words of the form xx^{-1} or $x^{-1}x$, then we call w and v to be equivalent. It turns out that any word in $w \in (X \cup X^{-1})^*$ is equivalent to a unique reduced word w^r. The *free group* $\mathrm{FG}(X)$ on X is then the set of reduced word in $(X \cup X^{-1})^*$, equipped with the binary operation $\cdot$ where

$$w \cdot v = (wv)^r.$$

Note that we may consider X^* as a submonoid of $\mathrm{FG}(X)$. We are now armed with the description of free group we need in the construction of free inverse monoid.

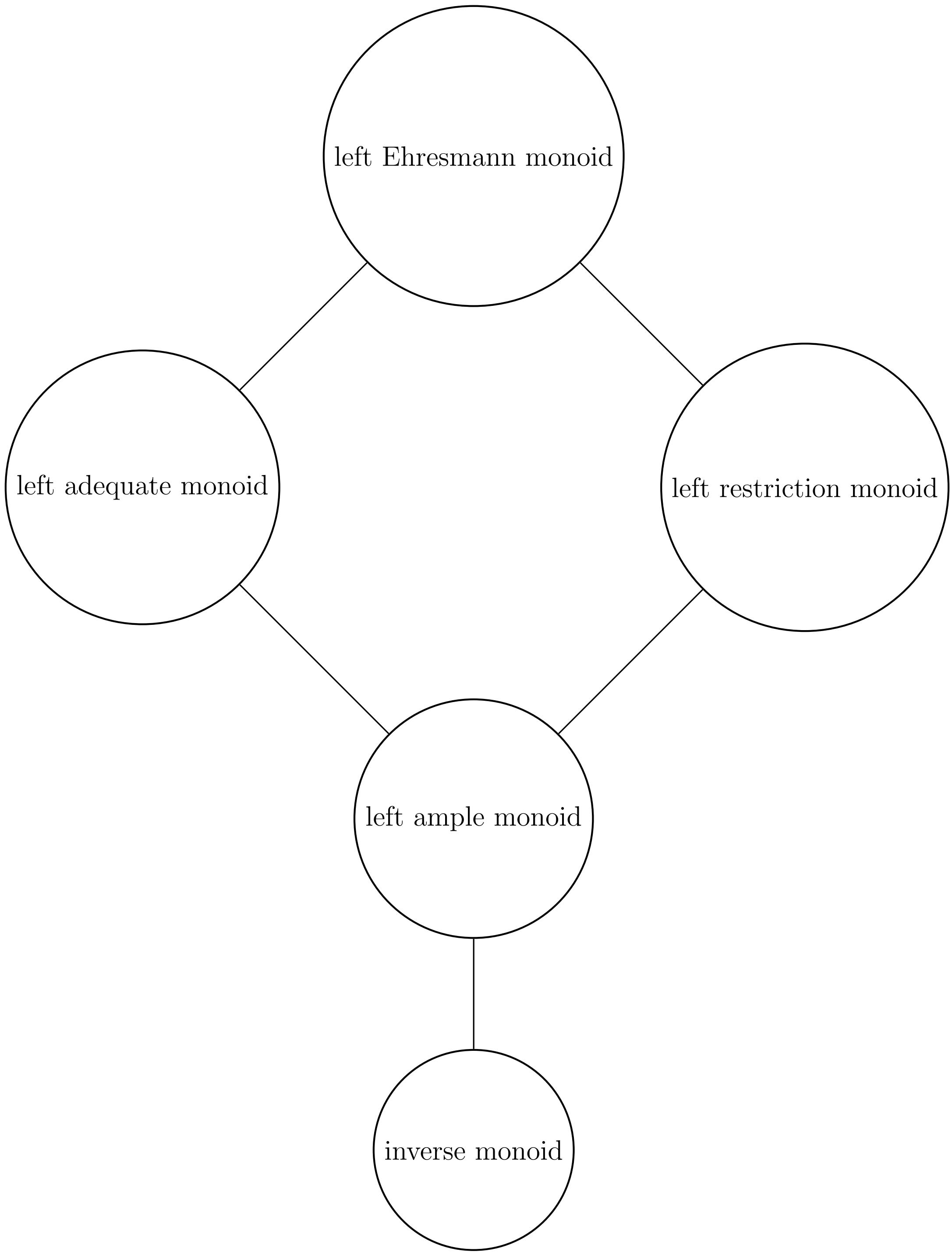

Figure 1.1: relation between various type of monoid

For a reduced word $w \in \mathrm{FG}(X)$, let $w = x_1 \cdots x_n$, we define

$$w^{\downarrow} = \{1, x_1, x_1x_2, \ldots, x_1 \cdots x_n\},$$

to be the set of prefixes of w in $(X \cup X^{-1})^*$. We also say that a finite non-empty subset A of $\mathrm{FG}(X)$ is *prefix closed* if

$$w \in A \Rightarrow w^{\downarrow} \subseteq A.$$

We then define

$$g \cdot A = \{g \cdot w : w \in A\}.$$

For later use, we remark it is well-known ([21, Section 5.10, p.203], [14]) that if $w, z \in \mathrm{FG}(X)$, then

$$(w \cdot z)^{\downarrow} \subseteq w^{\downarrow} \cup w \cdot (z^{\downarrow}),$$

and

$$w^{-1} \cdot w^{\downarrow} = (w^{-1})^{\downarrow}.$$

Lemma 1.4.1. *For any $w \in \mathrm{FG}(X)$, $w^{\downarrow}$ is prefix closed.*

Proof. Let $w = x_1 \cdots x_n$ in its reduced form, where $x_1, \ldots, x_n \in X \cup X^{-1}$. If $g \in w^{\downarrow}$, then $g = x_1 \cdots x_i$ for some $i \leq n$. Then $g^{\downarrow} = \{1, x_1, x_1x_2, \ldots, x_1 \cdots x_i\} \subseteq \{1, x_1, x_1x_2, \ldots, x_1 \cdots x_n\} = w^{\downarrow}$. So $w^{\downarrow}$ is prefix closed. □

Lemma 1.4.2. *If $A, B \subseteq \mathrm{FG}(X)$ are prefix closed sets, then we have $A \cup B$ is also prefix closed. In other words, The union of two prefix closed sets is prefix closed.*

Proof. The union of two finite non-empty sets is must be finite and non-empty. Now let $w \in A \cup B$, without loss of generality, let $w \in A$. Since A is prefix closed, $w^{\downarrow} \subseteq A$. So $w^{\downarrow} \subseteq A \cup B$. □

Lemma 1.4.3. *The intersection of two prefix closed sets is prefix closed.*

Proof. Note that 1 is always in a prefix closed set, so the intersection must be non-empty. Let A and B are two prefix closed sets. Since they are both finite, so is $A \cap B$. Suppose $w \in A \cap B$. Since $w \in A$, this implies $w^{\downarrow} \subseteq A$. Dually, $w^{\downarrow} \subseteq B$. Therefore, we have $w^{\downarrow} \subseteq A \cap B$, and hence $A \cap B$ is prefix closed. □

Lemma 1.4.4. *If A is prefix closed, then for any $w \in \mathrm{FG}(X)$, we have $w^{\downarrow} \cup w \cdot A$ is also prefix closed.*

Proof. The set $w^{\downarrow} \cup w \cdot A$ is finite and non-empty as both $w^{\downarrow}$ and A are prefix closed. Now let $v \in w^{\downarrow} \cup w \cdot A$. If $v \in w^{\downarrow}$ then $v^{\downarrow} \subseteq w^{\downarrow}$ as $w^{\downarrow}$ is prefix closed. Otherwise $v \in w \cdot A$, so $v = w \cdot w'$, where $w' \in A$. Then $v^{\downarrow} = (w \cdot w')^{\downarrow} \subseteq w^{\downarrow} \cup w \cdot (w')^{\downarrow} \subseteq w^{\downarrow} \cup w \cdot A$ as A is prefix closed. In any case $v^{\downarrow} \subseteq w^{\downarrow} \cup w \cdot A$ and hence the later is prefix closed. □

Let $\mathcal{Y}$ denote the set of subset of $\mathrm{FG}(X)$ that are prefix closed. In other words,

$$\mathcal{Y} = \{A \subseteq \mathrm{FG}(X) \mid A \text{ is prefix closed.}\}$$

We note that if $A \in \mathcal{Y}$, then $1 \in A$. There is a natural action of $\mathrm{FG}(X)$ on $\mathcal{Y}$. For $g \in \mathrm{FG}(X)$, $A \in \mathcal{Y}$ we define

$$g \cdot A = \{g \cdot h \mid h \in A\};$$

Note that $g \cdot A$ need not be in $\mathcal{Y}$.

Lemma 1.4.5. *Let $A \in \mathcal{Y}$ and $g \in \mathrm{FG}(X)$. Then*

$$g^{-1} \cdot A \in \mathcal{Y} \text{ if and only if } g \in A.$$

Proof. See [21, Section 5.10, P.204] □

Definition 1.4.6. The free inverse monoid $\mathrm{FIM}(X)$ on X is then given by

$$\mathrm{FIM}(X) = \{(A, g) \in \mathcal{Y} \times \mathrm{FG}(X) \mid g^{-1} \cdot A \in \mathcal{Y}\} = \{(A, g) \mid A \in \mathcal{Y}, g \in A\},$$

with multiplication given by

$$(A, g)(B, h) = (A \cup g \cdot B, gh).$$

Here we need to show that $\mathrm{FIM}(X)$ is closed under this operation. By 1.4.4, we have $g^{\downarrow} \cup g \cdot B \in \mathcal{Y}$. As $g \in A$, we know that $g^{\downarrow} \subseteq A$. So by 1.4.2, $A \cup g \cdot B = A \cup g^{\downarrow} \cup g \cdot B \in \mathcal{Y}$. On the other hand, as $h \in B$, we have $gh \in g \cdot B \subseteq A \cup g \cdot B$.

Once again we can consider X^* as a submonoid of $\mathrm{FIM}(X)$, and the standard embedding of X into $\mathrm{FIM}(X)$ is given by $\iota : X \to \mathrm{FIM}(X)$, where

$$x\iota = (\{1, x\}, x).$$

By routine checking, we can see the following. As usual in an inverse monoid, s^+ means ss^{-1} and s^* means $s^{-1}s$.

Lemma 1.4.7. *In* $\mathrm{FIM}(X)$*:*

(i) the identity is $(\{1\}, 1)$*;*

(ii) the semilattice of idempotents is $E(\mathrm{FIM}(X)) = \{(A, 1) | A \in \mathcal{Y}\}$*;*

and for any $(A, g) \in \mathrm{FIM}(X)$ *we have that*

(iii) $(A, g)^{-1} = (g^{-1} \cdot A, g^{-1})$*;*

(iv) $(A, g)^+ = (A, g)(A, g)^{-1} = (A, 1)$*;*

(v) $(A,g)^* = (A,g)^{-1}(A,g) = (g^{-1} \cdot A, 1)$.

It is a consequence of the above that for any $(A,g),(B,h) \in \mathrm{FIM}(X)$ we have

$$(A,g)\,\mathcal{R}\,(B,h) \text{ if and only if } A = B$$

and

$$(A,g)\,\mathcal{L}\,(B,h) \text{ if and only if } g^{-1}A = h^{-1}B.$$

1.4.1 The free left ample and free ample monoids

Inside $\mathrm{FIM}(X)$ sits both the free left ample monoid $\mathrm{FLA}(X)$ and free ample monoid $\mathrm{FA}(X)$ on X, which are unary and biunary submonoids of the free inverse monoid. Remarkably, the free (left) ample monoid coincides with the free (left) restriction monoid; see [14].

Specifically, the unary monoid $\mathrm{FLA}(X)$ has elements

$$\mathrm{FLA}(X) = \{(A,a) \in \mathrm{FIM}(X) \mid a \in X^*, A \subseteq X^*\}$$

so that as $a \in A$ above, we must have

$$\mathrm{FLA}(X) = \{(A,a) \in \mathrm{FIM}(X) \mid A \subseteq X^*\};$$

the multiplication as in $\mathrm{FIM}(X)$ and unary operation

$$(A,a)^+ = (A,1).$$

The biunary monoid $\mathrm{FA}(X)$ has elements

$$\mathrm{FA}(X) = \{(A,a) \in \mathrm{FIM}(X) \mid a \in X^*\}$$

with multiplication as in $\mathrm{FIM}(X)$, and unary operations given by

$$(A,a)^+ = (A,1) \text{ and } (A,a)^* = (a^{-1}A,1).$$

1.5 Automata

The term finite state automata describes a class of models of computation that are characterised by having a finite number of states. With input strings from a finite alphabet, that is, words from a free monoid on a finite set, the system transits from one state to another. This is standard material and may be found in [26], [20] and [10].

Definition 1.5.1. An *alphabet* is a finite non-empty set X. A *letter* is an element of X.

Definition 1.5.2. Let X be a finite non-empty set of alphabet. A *finite state automaton* is a quintuple $\mathcal{A} = (X, Q, E, I, T)$ where

- Q is a finite set called states,
- $E \subseteq Q \times X \times Q$,
- $I \subseteq Q$ is a set of initial states,
- $T \subseteq Q$ is a set of final states.

Elements in E have the form of a triple (p, x, q) where $p, q \in Q$ and $x \in X$. These are called *edges*. The edge (p, x, q) begins at p, ends at q, and carries the label x.

A path in $\mathcal{A}$ (of length $n \geq 1$) is a finite sequence of edges

$$(p_1, x_1, q_1), (q_1, x_2, q_2), \ldots, (q_{i-1}, x_i, q_i), (q_i, x_{i+1}, q_{i+1}), \ldots, (q_{n-1}, x_n, q_n).$$

Definition 1.5.3. Given a finite state automaton $\mathcal{A} = (X, Q, E, I, T)$, the *reverse automaton* is $\mathcal{A}^{\varrho} = (X, Q, E^{\varrho}, T, I)$ with

$$(p, x, q) \in E^{\varrho} \Leftrightarrow (q, x, p) \in E.$$

Definition 1.5.4. A finite state automaton $\mathcal{A} = (X, Q, E, I, T)$ is *accessible* if for any $q \in Q$, there exists a path starting from an initial state $q_0 \in I$ ending at q.

Definition 1.5.5. An automaton is [30, Chapter 2]:

1 trim - if both $\mathcal{A}$ and $\mathcal{A}^{\varrho}$ are accessible;

2 deterministic - if

   - $\mathcal{A}$ has at most one initial state.
   - for all $(q, x) \in Q \times X$, there is at most one edge (q, x, p) in $\mathcal{A}$;

3 complete - if

   - $\mathcal{A}$ has exactly one initial state;
   - for all $(q, x) \in Q \times X$, there is exactly one edge (q, x, p) in $\mathcal{A}$.

If $\mathcal{A}$ is deterministic, for all $p \in Q, x \in X$, we can define a partial function, which is called the *state transition function*, or *next state function* $\delta : Q \times X \to Q$ by assigning $\delta(p, x) = q$ if $(p, x, q) \in E$. If $\mathcal{A}$ is complete, then it is a function. In this case we may denote $\mathcal{A}$ by a quintuple

$$\mathcal{A} = (X, Q, \delta, q_0, T)$$

where δ is the next state function and q_0 is the unique initial state. Throughout this thesis, we will assume a deterministic finite state automata (DFA) to be trim and complete.

We now extend the next state function δ to have the domain $Q \times X^*$. We set $\delta(q, \epsilon) = q$ for all $q \in Q$, and if $\delta(q, w)$ is defined for all $q \in Q$ and $|w| = n$, then $\delta(q, wx) = \delta(\delta(q, w), x)$, $\forall x \in X$. By induction, δ is defined in $Q \times X^*$. The reader can check that for any $w, v \in X^*$,

$$\delta(q, wv) = \delta(\delta(q, w), v).$$

This is because if $wv = x_1 \cdots x_n$, then both sides equal

$$\delta(\cdots \delta(q, x_1), \cdots x_n).$$

Next we talk about languages.

Definition 1.5.6. A *language* (over X) is a subset of X^*. A language L is *finite* if $|L| < \infty$.

Definition 1.5.7. (i) Let q_0 be the initial state of a DFA $\mathcal{A}$. A word $w \in X^*$ is *accepted* by $\mathcal{A}$ if $\delta(q_0, w) \in T$, and $w \in X^*$ is *rejected* by $\mathcal{A}$ if $\delta(q_0, w) \notin T$.

(ii) The language *recognised* by $\mathcal{A}$ is

$$L(\mathcal{A}) = \{w \in X^* \mid \delta(q_0, w) \in T\},$$

that is, the set of words that $\mathcal{A}$ accepts.

(iii) A language $L \subseteq X^*$ is *recognisable* if there exists a DFA $\mathcal{A}$ with $L = L(\mathcal{A})$.

Let L be a language over X. We now define $\sim_L$ on X^*, which will be a crucial concept in this work. We give it here via a formula, but we will see there is an equivalent abstract formulation.

Definition 1.5.8. Let $u, v \in X^*$. Then $u \sim_L v$ if and only if for all $x, y \in X^*$,

$$xuy \in L \Leftrightarrow xvy \in L.$$

One can check that $\sim_L$ is a congruence, which is called the *syntactic congruence* of L.

The set of congruence classes $M(L) = \{[w] \mid w \in X^*\}$ then becomes a monoid under

$$[u][v] = [uv],$$

called the *syntactic monoid* of L. In fact, $\sim_L$ is the largest congruence such that L is a union of classes.

The following is well-known.

Theorem 1.5.9. *Let L be a language over X. Then L is recognised by a DFA if and only if its syntactic congruence has a finite index, i.e. $|M(L)| < \infty$.*

1.6 The Schützenberger product of monoids

In [33] Schützenberger introduced a product $M \diamond N$ of monoids M and N. In [37] Straubing extended it into a n-ary product. Here we focus on the binary product case. Consider the set $M \times N$ to be the set of all pairs (x, y), $x \in M$, $y \in N$. We define an action of $m \in M$ on the left of $M \times N$, given by $m(x, y) = (mx, y)$; an action of $n \in N$ on the right of $M \times N$ is defined dually by $(x, y)n = (x, yn)$. For $P \subseteq M \times N$, $m \in M$, $n \in N$ we let $mP = \{m(x, y) : (x, y) \in P\}$ and $Pn = \{(x, y)n : (x, y) \in P\}$.

The *Schützenberger product* $M \diamond N$ has the underlying set

$$M \diamond N = \left\{ \begin{pmatrix} m & P \\ 0 & n \end{pmatrix} : m \in M, n \in N, P \subseteq M \times N \right\}$$

equipped with multiplication, which is given by

$$\begin{pmatrix} m & P \\ 0 & n \end{pmatrix} \begin{pmatrix} m' & P' \\ 0 & n' \end{pmatrix} = \begin{pmatrix} mm' & mP' \cup Pn' \\ 0 & nn' \end{pmatrix}.$$

It is not hard to verify that the Schützenberger product $M \diamond N$ is a monoid with identity $\begin{pmatrix} 1 & \emptyset \\ 0 & 1 \end{pmatrix}$.

The product has been used in a number of problems about recognizable sets [33], [37]. To understand this, first we define the notion of recognisability by a monoid:

Definition 1.6.1. We say L is *recognised* by M if there exists a morphism $\varphi_1 : X^* \to M$ such that $L = (L\varphi_1)\varphi_1^{-1}$.

Definition 1.6.2. If $L, K \subseteq X^*$, then $LK = \{w_1w_2 \mid w_1 \in L, w_2 \in K\}$.

One of the results is that if $L, K \subseteq X^*$, and M, N are monoids, in which L is recognised by M, and K is recognised by N, then LK is recognised by $M \diamond N$.

To show this, we first let φ_1 be a morphism from X^* to M, and φ_2 be a morphism from X^* to N. For $w \in X^*$, define

$$\Omega(w) = \{(w_1\varphi_1, w_2\varphi_2) \mid w_1w_2 = w\} \subseteq M \times N.$$

For example, let $X = \{a, b, c\}$, and $w = abc$. Then

$$\Omega(w) = \{((abc)\varphi_1, 1), ((ab)\varphi_1, c\varphi_2), (a\varphi_1, (bc)\varphi_2), (1, (abc)\varphi_2)\}.$$

Now define a map $\varphi : X^* \to M \diamond N$ by

$$w\varphi = \begin{pmatrix} w\varphi_1 & \Omega(w) \\ 0 & w\varphi_2 \end{pmatrix}.$$

Lemma 1.6.3. *The map φ is a homomorphism.*

Proof. Let $v, w \in X^*$. Then

$$v\varphi w\varphi = \begin{pmatrix} v\varphi_1 & \Omega(v) \\ 0 & v\varphi_2 \end{pmatrix} \begin{pmatrix} w\varphi_1 & \Omega(w) \\ 0 & w\varphi_2 \end{pmatrix} = \begin{pmatrix} (vw)\varphi_1 & v\varphi_1\Omega(w) \cup \Omega(v)w\varphi_2 \\ 0 & (vw)\varphi_2 \end{pmatrix},$$

whereas

$$(vw)\varphi = \begin{pmatrix} (vw)\varphi_1 & \Omega(vw) \\ 0 & (vw)\varphi_2 \end{pmatrix}.$$

So, it is suffices to verify that $v\varphi_1\Omega(w) \cup \Omega(v)w\varphi_2 = \Omega(vw)$. If $x \in \Omega(w)$, there exist $w_1, w_2 \in \Sigma^*$, with $w_1w_2 = w$ such that $x = (w_1\varphi_1, w_2\varphi_2)$. Then $(v\varphi_1)x = v\varphi_1(w_1\varphi_1, w_2\varphi_2) = ((vw_1)\varphi_1, w_2\varphi_2)$ and $vw_1w_2 = vw$. So $(v\varphi_1)x \in \Omega(vw)$ and we have $(v\varphi_1)\Omega(w) \subseteq \Omega(vw)$. Similarly, $\Omega(v)(w\varphi_2) \subseteq \Omega(vw)$, hence $v\varphi_1\Omega(w) \cup \Omega(v)w\varphi_2 \subseteq \Omega(vw)$. For the opposite inclusion, let $(u_1\varphi_1, u_2\varphi_2) \in \Omega(vw)$. Then $u_1u_2 = vw$. This implies that either $u_1 = vy$, $w = yu_2$ or $v = u_1y$, $u_2 = yw$. In the former case $(u_1\varphi_1, u_2\varphi_2) = v\varphi_1(y\varphi_1, u_2\varphi_2) \in v\varphi_1\Omega(w)$ and in the latter case $(u_1\varphi_1, u_2\varphi_2) = (u_1\varphi_1, y\varphi_2)w\varphi_2 \in \Omega(v)w\varphi_2$. As a result, $\Omega(vw) \subseteq v\varphi_1\Omega(w) \cup \Omega(v)w\varphi_2$. □

Now is the time to prove the main result of this section.

Theorem 1.6.4. *[30, Chapter 5] Let $L, K \subseteq X^*$ and let M, N be monoids. If L is recognised by M, and K is recognised by N, then LK is recognised by $M \diamond N$.*

Proof. Let $\varphi_1 : X^* \to M$ be a morphism such that $L = (L\varphi_1)\varphi_1^{-1}$, and $\varphi_2 : X^* \to N$ be a morphism such that $K = (K\varphi_2)\varphi_2^{-1}$. Now let $\varphi : X^* \to M \diamond N$ be the morphism

$$w\varphi = \begin{pmatrix} w\varphi_1 & \Omega(w) \\ 0 & w\varphi_2 \end{pmatrix}.$$

We prove that $LK = ((LK)\varphi)\varphi^{-1}$. Obviously $LK \subseteq ((LK)\varphi)\varphi^{-1}$. To prove the opposite inclusion, let $w \in ((LK)\varphi)\varphi^{-1}$. Then $w\varphi \in (LK)\varphi$, so that $w\varphi = (uv)\varphi$ for some $u \in L$ and $v \in K$. Now

$$\begin{aligned} w\varphi &= (uv)\varphi \\ &= \begin{pmatrix} (uv)\varphi_1 & \Omega(uv) \\ 0 & (uv)\varphi_2 \end{pmatrix}. \end{aligned}$$

This implies $\Omega(w) = \Omega(uv)$. In particular, $(u\varphi_1, v\varphi_2) \in \Omega(uv) = \Omega(w)$. As a result, there exists $(w_1, w_2) \in X^*$, $w_1w_2 = w$ such that $(w_1\varphi_1, w_2\varphi_2) = (u\varphi_1, v\varphi_2)$. Then

$w_1\varphi_1 = u\varphi_1$ implies $w_1 \in u\varphi_1\varphi_1^{-1} \subseteq L\varphi_1\varphi_1^{-1} = L$. Similarly $w_2 \in K$ and hence $w = w_1w_2 \in LK$. □

1.7 Universal algebra

A (universal) algebra is a set together with a collection of finitary operations, which are considered as basic in the sense they must be preserved by morphisms and congruences. We give the full defininitions below. Our main examples will be semigroups, monoids, inverse semigroups and unary and biunary monoids. Our account follows that in [7] and [28].

Definition 1.7.1. We denote the set of natural number $\{1, 2, 3, \ldots\}$ by $\mathbb{N}$ and the set $\mathbb{N} \cup \{0\}$ by $\mathbb{N}^0$.

For a set A and $n \in \mathbb{N}$ we denote by A^n the n-fold direct power of A, that is, the set of all n-tuples of elements of A; we interpret A^0 as a one-element set.

Definition 1.7.2. Let B, C be sets. A function f from B to C, denoted by $f : B \to C$, is a subset of $B \times C$ such that for each $b \in B$, there is exactly one $c \in C$ such that $(b, c) \in f$. We may write $bf = c$ and $b \mapsto c$. Let A be a set and $n \in \mathbb{N}^0$. An operation of rank n on A is a function from A^n to A.

Binary operations, such as the addition and multiplication of numbers that we are familiar with, are operations of rank 2. Semigroups, monoids and groups are equipped with a binary operation (that is associative). We call operations of rank 1 on A unary operations and identify them with the functions from A into A. One example is such as the operation of taking inverses when studying inverse semigroups, or the operation of $a \mapsto a^+$ in a left ample semigroup. We call operations of rank 0 nullary or constants and identify them with their unique values. A common example of a nullary operation that we consider is the identity of a monoid.

An algebra is a set equipped with a collection of operations:

Definition 1.7.3. Let A be a non-empty set and let $F = \{F_i : i \in I\}$ be a set where F_i is an operation of finite rank on A for each $i \in I$. Then the ordered pair $\mathbf{A} = (A, F)$ is called an algebra. We shall also write as

$$\mathbf{A} = (A, F_i : i \in I).$$

Here A is called the universe of (A, F), the operations F_i are referred to as *fundamental* or *basic operations* of (A, F) for each $i \in I$, and I is called the *index set* of (A, F).

Definition 1.7.4. Any operation t (of any finite arity) on A that is made up from the basic operations, projections and composition, is called a *term function* of $\mathbf{A}$.

In universal algebras, we need to consider the signature of an algebra.

Definition 1.7.5. Let I be the index set of algebra $\mathbf{A} = (A, F)$, and $\rho : I \to \mathbb{N}^0$ be a function given by $i \mapsto \rho_i$, where ρ_i is the rank of F_i. Then $(\rho_i)_{i\in I}$ is the signature of $\mathbf{A}$. If I is finite, say $I = \{1, \cdots, n\}$, we may write $(\rho_1, \cdots, \rho_n)$ for the signature.

Note that if $\rho_i = 0$, then $F_i : A^0 \to A$ and as we have remarked it is associated with some $a_i \in A$.

So, an algebra has signature (2) if it has a single binary operation (and no others). For example, a semigroup, which can be written as

$$\mathbf{S} = (S, \cdot).$$

Of course, for S to be a semigroup, it must also satisfy the identity for associativity, that is, $(xy)z = x(yz)$. We mean by the latter that for any $a, b, c \in S$ we have $(ab)c = a(bc)$. Notice that we tend to drop $\cdot$ for the binary operation and use juxtaposition. A monoid has signature $(2, 0)$,

$$\mathbf{M} = (M, \cdot, 1),$$

and if it is a unary monoid, it has signature $(2, 1, 0)$, like an inverse monoid

$$\mathbf{I} = (I, \cdot, ^{-1}, 1).$$

In the same way a biunary monoid has signature $(2, 1, 1, 0)$, and so on.

Note that there can be more than one type of algebra with the same signature. A group is an algebra with signature $(2, 1, 0)$, written as

$$\mathbf{G} = (G, \cdot, ^{-1}, 1),$$

where the $^{-1}$ in the signature in this case refers to the group inverse.

An algebra of a certain signature can also be considered as an algebra of another signature. For example, an inverse monoid can be considered as a monoid, which itself can be considered as a semigroup. We will be careful to specify which signatures we are using.

Definition 1.7.6. Let $\mathbf{A} = (A, F)$ and $\mathbf{B} = (B, G)$ be algebras of the same signature, where $F = \{F_i : i \in I\}$ and $G = \{G_i : i \in I\}$ are sets of basic operations such that for each $i \in I$, F_i and G_i have the same rank ρ_i. Let f be a function from A to B. Then f is *a morphism* if for any $i \in I$ and $a_1, a_2, ..., a_{\rho_i} \in A$,

$$(F_i(a_1, a_2, ..., a_{\rho_i}))f = G_i(a_1 f, a_2 f, ..., a_{\rho_i} f).$$

If $\rho_i = 0$, that means f is taking a constant in $\mathbf{A}$ to constant in $\mathbf{B}$. For example, if

$\mathbf{A}$ and $\mathbf{B}$ are both monoids, then a monoid morphism f should send the identity of $\mathbf{A}$ into that of $\mathbf{B}$. That is, $1_A f = 1_B$.

The following follows from induction on the number of basic operations needed to build a term function.

Corollary 1.7.7. *Let A and B be algebras of the same type and $t(x_1, ..., x_n)$ be a term function. Suppose $\theta : A \to B$ is a morphism and $a_1, ..., a_n \in A$. Then*

$$(t(a_1, ..., a_n))\theta = t(a_1\theta, ..., a_n\theta).$$

Without further mention, we shall assume morphisms are between algebras of the same signature. A morphism $\theta : S \to T$, where S and T are monoids, is a $(2, 0)$-morphism if

(i) $(a\theta)(b\theta) = (ab)\theta$,

(ii) $1_S\theta = 1_T$,

for $a, b \in S$.

If S, T are left ample monoids, a map $\theta : S \to T$ is a morphism if it satisfies (i), (ii) and

(iii) $(a^+)\theta = (a\theta)^+$,

for all $a \in S$.

Inverse monoids are special. Let S, T be inverse monoids and let $\theta : S \to T$ satisfy (i) and (ii), that is, it is a $(2, 0)$-morphism. Then (by judicious use of Lallement's Lemma), it is a *consequence* that

(iii) $a^{-1}\theta = (a\theta)^{-1}$

for all $a \in S$, that is, θ is a $(2, 1, 0)$-morphism.

The counterpart to morphisms are congruences on algebras, which we now define. Roughly speaking, an equivalence relation on an algebra $\mathbf{A} = (A, F_i : i \in I)$ is a congruence if it is compatible with all the basic operations, as we explain below.

Definition 1.7.8. Let $\mathbf{A} = (A, F_i : i \in I)$ be an algebra and let σ be an equivalence relation on A. Then σ is a *congruence* if for each basic operation F_i, if the rank of F_i is ρ_i and $a_1, \ldots, a_{\rho_i}, b_1, \ldots, b_{\rho_i} \in A$ and $a_j \; \sigma \; b_j$ for all $1 \leq j \leq \rho_i$, then

$$F_i(a_1, \ldots, a_{\rho_i}) \; \sigma \; F_i(b_1, \ldots, b_{\rho_i}).$$

We note that in the above, if $\rho_i = 0$ then the given condition is automatically satisfied.

The following follows from induction.

Corollary 1.7.9. *Let* $\boldsymbol{A} = (A, F_i : i \in I)$ *be an algebra and let* σ *be a congruence on* A. *Let* $t(x_1, \ldots, x_n)$ *be an* n*-ary term function on* A. *If* $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ *and* $a_j \ \sigma \ b_j$ *for all* $1 \leq j \leq n$, *then*

$$t(a_1, ..., a_n) \ \sigma \ t(b_1, ..., b_n).$$

For example, on an inverse semigroup S, a $(2,1)$-congruence σ must satisfy:
For any $a, b, c, d \in A$, if $a \ \sigma \ b$ and $c \ \sigma \ d$, then

(i) $ac \ \sigma \ bd$;

(ii) $a^{-1} \ \sigma \ b^{-1}$.

Again, inverse monoids are special in the sense that if (i) holds then (ii) follows. But, this is not the case for a general $(2,1)$-congruence.

In general, a *binary relation* H on an algebra $\mathbf{A}$ is a subset of $A \times A$. If $H \subseteq A \times A$, then $u \ \langle H \rangle \ v$ if $u = v$ or $\exists$ a sequence $u_0, u_1, \ldots, u_n$ such that $u = u_0$ and $u_n = v$, where for each $1 \leq i \leq n$, we have $u_{i-1} = t_i(a_1, \ldots, a_{j-1}, p, a_{j+1}, \ldots, a_{m_i})$ and $u_i = t_i(a_1, \ldots, a_{j-1}, q, a_{j+1}, \ldots, a_{m_i})$, where (p, q) or $(q, p) \in H$ and $t_i(x_1, \ldots, x_{m_i})$ is a term function.

Lemma 1.7.10. *Let* $\mathbf{A}$ *be an algebra and let* H *be a subset of* $A \times A$. *Then* $\langle H \rangle$ *is a congruence containing* H *and is the smallest such congruence.*

Proof. To prove $\langle H \rangle$ is reflexive, we see that for any $u \in A$, $u = u$. So $u \ \langle H \rangle \ u$.

To prove $\langle H \rangle$ is symmetric, let $u, v \in A$. Then $u \ \langle H \rangle \ v$ if and only if $u = v$ or $\exists$ a sequence $u_0, u_1, \ldots, u_n$ such that $u = u_0$ and $u_n = v$, where for each $1 \leq i \leq n$, we have $u_{i-1} = t_i(a_1, \ldots, a_{j-1}, p, a_{j+1}, \ldots, a_{m_i})$ and $u_i = t_i(a_1, \ldots, a_{j-1}, q, a_{j+1}, \ldots, a_{m_i})$, where (p, q) or $(q, p) \in H$. If $u = v$, then $v = u$ and so $v \ \langle H \rangle \ u$. For the other case, $v = u_n, \ldots, u_1, u_0 = u$ is a sequence where for each $1 \leq i \leq n$, we have $u_i = t_i(a_1, \ldots, a_{j-1}, q, a_{j+1}, \ldots, a_{m_i})$ and $u_{i-1} = t_i(a_1, \ldots, a_{j-1}, p, a_{j+1}, \ldots, a_{m_i})$ where (p, q) or $(q, p) \in H$.

To prove $\langle H \rangle$ is transitive, let $u, v, w \in A$ such that $u \ \langle H \rangle \ v$ and $v \ \langle H \rangle \ w$. If either $u = v$ or $v = w$, then $u \ \langle H \rangle \ w$. Otherwise, $\exists$ a sequence $u_0, u_1, \ldots, u_n$ such that $u = u_0$ and $u_n = v$, and $\exists$ a sequence $v_0, v_1, \ldots, v_n$ such that $v = v_0$ and $v_n = w$. Then we have a sequence $u_0, u_1, \ldots, u_n = v_0, v_1, \ldots, v_n$, where if for each pair of adjacent term in the sequence, they are in the form of $t_i(a_1, \ldots, a_{j-1}, p, a_{j+1}, \ldots, a_{m_i})$ and $t_i(a_1, \ldots, a_{j-1}, q, a_{j+1}, \ldots, a_{m_i})$, where (p, q) or $(q, p) \in H$.

We have shown that $\langle H \rangle$ is an equivalence relation. We must now prove that $\langle H \rangle$ is compatible with the basic operations, or, equivalently, the term functions. Let $t(x_1, \ldots, x_l)$ be a term function and elements $p_k, q_k \in A$ where $(p_k, q_k) \in \langle H \rangle$ for $1 \leq k \leq l$. We need to prove

$$t(p_1, \ldots, p_l) \ \langle H \rangle \ t(q_1, \ldots, q_l).$$

By transitivity, it suffice to prove: for any fixed $c_2, \dots c_l$ and $(p', q') \in \langle H \rangle$, we have

$$t(p', c_2, \dots c_l) \ \langle H \rangle \ t(q', c_2, \dots c_l).$$

Having the other variables fixed, we can consider consider t as having a single variable. So we have to prove

$$t(p') = t(p', c_2, \dots c_l) \ \langle H \rangle \ t(q', c_2, \dots c_l) = t(q').$$

If $p' = q'$, certainly $t(p') = t(q')$. Otherwise $\exists$ a sequence $u_0, u_1, \dots, u_n$ such that $p' = u_0$ and $u_n = q'$, where for each $1 \leq i \leq n$, we have $u_{i-1} = t_i(a_1, \dots, a_{j-1}, p, a_{j+1}, \dots, a_{m_i})$ and $u_i = t_i(a_1, \dots, a_{j-1}, q, a_{j+1}, \dots, a_{m_i})$, where (p, q) or $(q, p) \in H$. Letting $s_i(x) = t(t_i(a_1, \dots, a_{j-1}, x, a_{j+1}, \dots, a_{m_i}))$, we have $t(u_{i-1}) = s_i(p)$ and $t(u_i) = s_i(q)$. So we get the sequence $t(u_0), t(u_1), \dots, t(u_n)$ we want. As $t(p') = t(u_0)$ and $t(u_n) = t(q')$, from the definition of $\langle H \rangle$, we deduce $t(p') \ \langle H \rangle \ t(q')$.

Note if $(u, v) \in H$, we can let $n = 1$, $u_0 = u = t(u)$ and $u_1 = v = t(v)$ where $t(x) = x$. Then $(u, v) \in \langle H \rangle$, and $H \subseteq \langle H \rangle$.

Let σ be a congruence in $\mathbf{A}$ that contains H, and $u \ \langle H \rangle \ v$. Then if $u = v$, then $u \ \sigma \ v$. Otherwise, by Corollary 1.7.9, we know that for each $1 \leq i \leq n$, we have

$$u_{i-1} = t(a_1, \dots, a_{j-1}, p, a_{j+1}, \dots, a_{m_i}) \ \sigma \ t(a_1, \dots, a_{j-1}, q, a_{j+1}, \dots, a_{m_i}) = u_i,$$

as (p, q) or $(q, p) \in H \subseteq \sigma$. Since σ is transitive, we have $u = u_0 \ \sigma \ u_n = v$. As a result, $\langle H \rangle \subseteq \sigma$ and hence $\langle H \rangle$ is the smallest congruence containing H. $\square$

Let σ be a congruence on an algebra $\mathbf{A} = (A, F_i : i \in I)$, and let

$$A/\sigma = \{[a] \mid a \in A\}.$$

Then on A/σ we can define operations $\bar{F}_i$, corresponding to F_i, for each $i \in I$ by

$$\bar{F}_i([a_1], \cdots, [a_n]) = [F_i(a_1, \cdots, a_n)]$$

where $\rho_i = n$, and $[a_i]$ is the σ-class of a_i. If $i = 0$, the constant associated with $\bar{F}_i$ is $[a]$, where a is the constant associated with F_i. The fact that σ is a congruence easily yields that each $\bar{F}_i$ is well defined. In this way, we turn A/σ into an algebra of the same signature as $\mathbf{A}$.

For example, if S is an inverse semigroup and σ is a congruence then S/σ becomes a $(2, 1)$-algebra where

(i) $[a][b] = [ab]$;

(ii) $[a]^{-1} = [a^{-1}]$,

for $a, b \in S$. In fact, S/σ is then an inverse semigroup; [21]. Note that we may denote the congruence class of $a \in S$ by $a\sigma$ rather than $[a]$.

Finally we connect morphisms and congruences. Let $\mathbf{A}$ be an algebra and suppose ρ is a congruence on $\mathbf{A}$. Then we can define a morphism, the natural map $\rho^\natural : \mathbf{A} \to \mathbf{A}/\rho$ by

$$a\rho^\natural = [a].$$

Lemma 1.7.11. *Let $\rho^\natural$ be defined above. Then $\rho^\natural$ is indeed a morphism with* $\ker \rho^\natural = \rho$.

Proof. Let $F = \{F_i : i \in I\}$ be the set of basic operations of $\mathbf{A}$ such that for each $i \in I$, F_i has rank ρ_i. For any $i \in I$ and $a_1, a_2, ..., a_{\rho_i} \in A$,

$$\begin{aligned}
(F_i(a_1, a_2, ..., a_{\rho_i}))\rho^\natural &= [F_i(a_1, a_2, ..., a_{\rho_i})] \\
&= F_i([a_1], [a_2], ..., [a_{\rho_i}]) \\
&= F_i((a_1)\rho^\natural, (a_2)\rho^\natural, ..., (a_{\rho_i})\rho^\natural).
\end{aligned}$$

Also, let $a, b \in A$. Then $a \ker \rho^\natural\, b$, if and only if $a\rho^\natural = b\rho^\natural$, which is equivalent to $[a] = [b]$, and hence to $a \;\rho\; b$. □

For the proof of the next result we refer the reader to any standard text. For example, [28].

Proposition 1.7.12. *Let $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$ be algebras of the same signature. Let $\theta : A \to B$ and $\psi : A \to C$ be morphisms where ψ is onto and* $\ker \psi \subseteq \ker \theta$. *Then there exists a unique morphism $\varphi : C \to B$ such that for all $a \in A$, $(a\psi)\varphi = a\theta$.*

Corollary 1.7.13. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be algebras of the same signature. Let $\theta : A \to B$ be a morphism. Then*

$$\boldsymbol{A}/\ker\theta \cong \boldsymbol{A}\theta.$$

Proof. In Proposition 1.7.12 let $\mathbf{C}$ be $\mathbf{A}/\ker\theta$ and $\psi : \mathbf{A} \to \mathbf{A}/\ker\theta$ be the natural map $(\ker\theta)^\natural$. That is, $a\psi = [a]$ where $[a]$ is the congruence class of a with respect to $\ker\theta$. Since ψ is onto and $\ker\psi = \ker\theta$, from Proposition 1.7.12 there exists a unique morphism $\varphi : \mathbf{A}/\ker\theta \to \mathbf{B}$ such that for all $a \in A$, $(a\psi)\varphi = a\theta$. So $([a])\varphi = a\theta$. Note that for all $b \in A\theta \subseteq B$, $b = a\theta = ([a])\varphi$ for some $a \in A$. Also if $([a'])\varphi = ([a])\varphi$, then $a'\theta = a\theta$ and hence $[a'] = [a]$ as $\ker\psi = \ker\theta$. As a result φ is 1-1 and onto between $\mathbf{A}/\ker\theta$ and $\mathbf{A}\theta$ and the result follows. □

Chapter 2

Syntactic congruences

In Chapter 1 we defined a syntactic congruence on a free monoid. In this chapter we show how to extend this notion to arbitrary universal algebras.

2.1 Syntactic congruences on universal algebras

It is well known and easy to see that the notion of a syntactic congruence of a subset of a free monoid can be extended to arbitrary monoids (see, for example, [34]). We give a short account of how this works.

Definition 2.1.1. Let M be a monoid and let $L \subseteq M$ be a subset. The *syntactic congruence* $\sim_L$ of L is the largest congruence such that L is a union of congruence classes.

To see that this definition does not clash with that of Chapter 1.5 we prove the following.

Proposition 2.1.2. *[21]. Let M be a monoid and let $L \subseteq M$. Then $u \sim_L v$ if and only if for any $x, y \in M$ we have*

$$xuy \in L \Leftrightarrow xvy \in L.$$

Proof. For the moment, let κ be the relation defined on M as in the statement. Clearly κ is an equivalence relation. Now, if $u, v \in M$ with $u \,\kappa\, v$ and $p \in M$, then for any $x, y \in M$ we have:

$$x(pu)y \in L \Leftrightarrow (xp)uy \in L \Leftrightarrow (xp)vy \in L \Leftrightarrow x(pv)y \in L,$$

so that $pu \,\kappa\, pv$. Thus κ is left compatible with the monoid multiplication and dually it is right compatible. It follows easily that κ is a congruence.

If $u \in L$ and $u \,\kappa\, v$, then as $1u1 \in L$ we have $v = 1v1 \in L$. Thus L is a union of κ-classes. Finally, if L is a union of ρ-classes for some congruence ρ, then given any $u, v \in M$ with $u \,\rho\, v$, we have for any $x, y \in M$ that $xuy \,\rho\, xvy$, so that as L is a union of ρ-classes,

$$xuy \in L \Leftrightarrow xvy \in L,$$

so that $u \,\kappa\, v$.

We have demonstrated that κ is $\sim_L$, as required. $\square$

We now turn our attention to arbitrary (universal) algebras. Here we cannot hope for a simple form, involving just one explicit condition where we can explicitly give the term functions that describe the syntactic congruence, so we will give a definition along the lines of Definition 2.1.1, aiming for simple forms in some special cases of interest.

Let $\mathbf{A}$ be an algebra, with universe A. Associated with $\mathbf{A}$ are two lattices: the lattice of equivalence relations on A, which is denoted by $\mathcal{E}(A)$, and the lattice of congruences on A, which is denoted by $\mathcal{C}(A)$. Of course $\mathcal{E}(A)$ contains $\mathcal{C}(A)$ as a set. As the intersection of equivalences (congruences) is again an equivalence (congruence), it is clear that $\mathcal{C}(A)$ is a meet sublattice of $\mathcal{E}(A)$. What is more remarkable is that $\mathcal{C}(A)$ is a join sublattice of $\mathcal{E}(A)$. This follows from standard results in universal algebra, that tell us that the join, that is, the least upper bound, in $\mathcal{E}(A)$ of a set of congruences is indeed a congruence [28]. As a consequence, the join of a collection of congruences in $\mathcal{E}(A)$ coincides with the join in $\mathcal{C}(A)$.

A subset $L \subseteq A$ is said to be an *A-language* or a *language over A*. Let $\mathcal{C}_L = \{\nu_i : i \in I\}$ be the collection of all congruences on A such that L is a union of ν_i-classes for each ν_i. If we can prove that the join of all the congruences in $\mathcal{C}_L$ is still in $\mathcal{C}_L$, i.e. such that L is a union of congruence classes, then clearly this join will be the largest congruence such that L is a union of classes.

Theorem 2.1.3. *Let $\mathbf{A}$ be an algebra, with universe A, and $L \subseteq A$. Let $\mathcal{C}_L = \{\nu_i : i \in I\}$ be the collection of all congruences in $\mathbf{A}$ such that L is a union of ν_i-classes for each ν_i. Then the join $\rho = \bigvee_{i \in I} \nu_i$ is the largest congruence such that L is a union of ρ-classes.*

Proof. Since the join of a collection of congruences in the lattice of equivalences is a congruence, it follows that ρ is a congruence. As ρ is a join in the lattice of equivalences, it folllows that ρ is the product (in the semigroup of binary relations) of the relations $\nu_i, i \in I$. Thus $a \;\rho\; b$ if and only if $\exists n$ s.t.

$$a = a_0 \;\nu_1\; a_1 \;\nu_2\; a_2 \;\nu_3 \ldots \nu_n\; a_n = b,$$

where $\nu_i \in \mathcal{C}_L$ for all $1 \leq i \leq n$ [28]. Suppose $a \in L$ and $a \;\rho\; b$. Then $a_0 = a \in L$ and since $\nu_1 \in \mathcal{C}_L$, L is a union of ν_1-classes, so that $a_1 \in L$. Similarly, $a_2 \in L$ and so on. Finally, we have $b = a_n \in L$. As a result , L is a union of ρ-classes. We have shown that $\rho \in \mathcal{C}_L$. As the join of all congruence is in $\mathcal{C}_L$, ρ must be the largest congruence in $\mathcal{C}_L$. $\square$

We can now define a syntactic congruence on A. We refer the reader here to the work of Clark, Davey, Freese, Jackson, Maróti and McKenzie [4, 8].

Definition 2.1.4. Let $\mathbf{A}$ be an algebra, and $L \subseteq A$. The *syntactic congruence* of L, $\sim_L$, is defined as the largest congruence in $\mathbf{A}$ such that L is a union of congruence classes.

We can say that L is *saturated by* a congruence if L is a union of congruence classes, but we tend not to use this terminology.

Proposition 2.1.5. *Let $\mathbf{A}$ be an algebra, with universe A, and $L \subseteq A$. Then $\sim_L$ always exists.*

Proof. We have shown that the join of elements in $\mathcal{C}_L$ is still in $\mathcal{C}_L$. The result follows by observing that the equality relation is a congruence on $\mathbf{A}$ such that L is a union of congruence classes, so that $\mathcal{C}_L$ is always non-empty. $\square$

Given that $\sim_L$ always exists, the natural question second is to ask, how can we describe $\sim_L$?

We now outline a general process for finding $\sim_L$, which we will later specialise.

First we consider unary term functions. Let $t(x_1, \cdots, x_n)$ be a term with n free variables in the free term algebra on the signature of $\mathbf{A}$, where $n \geq 1$. Choosing elements $a_2, \ldots, a_n \in A$ we define

$$t(x) : A \to A \text{ by } t(x) = t(x, a_2, \ldots, a_n).$$

We refer to $t(x)$ as a *unary term function.*

For example, if M is an Ehresmann monoid, then $t(x)$ given by $t(x) = ((mx)^+n)^*u$ where $m, n, u \in M$ is a unary term function.

Proposition 2.1.6. *Let $\mathbf{A}$ be an algebra, and $L \subseteq A$. If ρ is a congruence on A such that L is a union of ρ-classes, then for any $u, v \in A$ with $u \; \rho \; v$, and for any unary term function $t(x)$, we have*

$$t(u) \in L \Leftrightarrow t(v) \in L.$$

Proof. To see this, suppose $t(x, x_2, \ldots, x_n)$ is a term in the signature of A. Then if $a_2, \ldots, a_n \in A$ and $u, v \in A$ with $u \, \rho \, v$ we must have

$$t(u, a_2, \ldots, a_n) \, \rho \, t(v, a_2, \ldots, a_n)$$

as ρ is a congruence. Hence as L is a union of ρ-classes, $t(u, a_2, \ldots, a_n) \in L$ if and only if $t(v, a_2, \ldots, a_n) \in L$. In other words, (with some abuse of notation,) $t(u) \in L$ if and only if $t(v) \in L$. $\square$

Theorem 2.1.7. *(cf. [8]) Let* $\mathbf{A}$ *be an algebra, and* $L \subseteq A$*. Then for any* $u, v \in A$ *we have* $u \sim_L v$ *if and only if for any unary term function* $t(x)$

$$t(u) \in L \Leftrightarrow t(v) \in L.$$

Proof. We know that $\sim_L$ is defined as the largest congruence in $\mathbf{A}$ such that L is a union of congruence classes. From Proposition 2.1.6, in particular, if $u \sim_L v$, then $t(u) \in L$ if and only if $t(v) \in L$.

On the other hand, suppose that $L \subseteq A$ and ρ is defined by the rule that for any unary term function $t(x)$, we have $u \,\rho\, v$ if and only if

$$t(u) \in L \Leftrightarrow t(v) \in L.$$

Clearly this is an equivalence relation. Suppose that $F(x_1, \cdots, x_n)$ is a basic operation, $t(x)$ is a unary term function and $a_i \,\rho\, b_i$ for $1 \leq i \leq n$. For $1 \leq i \leq n$ let $F_i(x) = t(F(a_1, \cdots, a_{i-1}, x, b_{i+1}, \cdots, b_n))$. Then

$$\begin{aligned} t(F(a_1, \cdots, a_n)) \in L &\Leftrightarrow F_n(a_n) \in L \\ &\Leftrightarrow F_n(b_n) \in L \\ &\Leftrightarrow F_{n-1}(a_{n-1}) \in L \\ &\ \vdots \\ &\Leftrightarrow F_1(a_1) \in L \\ &\Leftrightarrow F_1(b_1) \in L \\ &\Leftrightarrow t(F(b_1, \cdots, b_n)) \in L. \end{aligned}$$

Thus ρ is a congruence as it is an equivalence and respects all basic operations.

Note that $t(x) = x$ is also a term. Let $a \in L$ and suppose that $a \,\rho\, b$. Then $t(a) = a \in L$, so $t(b) = b \in L$. Hence L is a union of congruence classes. As $\sim_L$ is the largest congruence on A such that L is a union of congruence classes, $\rho \subseteq \sim_L$. But $\sim_L \subseteq \rho$ as $\sim_L$ itself satisfies the condition that $t(u) \in L \Leftrightarrow t(v) \in L$ for any unary term function $t(x)$. Hence the equality follows. $\square$

Now the game becomes limiting different kinds of $t(x)$ that one needs for different kinds of algebra. We do this directly, without recourse to properties of the lattice of congruences or the nature of the varieties concerned, as in [8]. Moreover, we look for specific (lists of) terms, rather than arguing for their existence.

From Proposition 2.1.2 we know that for a general monoid M, which is a (2,0)-algebra, the syntactic congruence is given by the rule that for all $u, v \in M, u \sim_L v$ if and only if for all term functions of the kind $t(x) = pxq$, where $p, q \in M$, we have that

$$t(u) \in L \quad \Leftrightarrow \quad t(v) \in L.$$

Corollary 2.1.8. *Let M be an inverse monoid and let $L \subseteq M$. Regarding M as a $(2,1,0)$-algebra, the syntactic congruence $\sim_L$ is given by the rule that for all $u, v \in M$, we have $u \sim_L v$ if and only if for all term functions of the kind $t(x) = pxq$, where $p, q \in M$, that*

$$t(u) \in L \quad \Leftrightarrow \quad t(v) \in L.$$

Proof. From the above, the relation described is the largest *monoid* congruence such that L is a union of classes. But by the result of Chapter 1.7, a monoid congruence on an inverse monoid is a unary monoid congruence (and certainly the converse is true). □

2.2 Syntactic congruences on one sided Ehresmann monoids

We consider the case of left Ehresmann monoids; the case for (right) Ehresmann monoid is the left/right dual, where we replace $^+$ by *.

Definition 2.2.1. Let M be a left Ehresmann monoid. Given an M-language L, we define $\approx_L$ by the rule that for all $u, v \in M$ we have

$$u \approx_L v$$

if and only if for all $x, y, s, t \in M$:

1. $$xuy \in L \quad \Leftrightarrow \quad xvy \in L$$

2. $$x(sut)^+y \in L \quad \Leftrightarrow \quad x(svt)^+y \in L$$

We are going to show that this $\approx_L$ is equal to the relation $\sim_L$.

Proposition 2.2.2. *The relation $\approx_L$ is an unary monoid congruence.*

Proof. To show that a relation is a unary monoid congruence, we need to show that it is an equivalence, and respects both multiplication and $^+$ operation. That is, if $u \approx_L v$ and $u' \approx_L v'$, then $uu' \approx_L vv'$ and $u^+ \approx_L v^+$.

It is easy to show that $\approx_L$ is an equivalence. We now show that $\approx_L$ is compatible with multiplication.

Let $u \approx_L v$ and $u' \approx_L v'$. Then

$$\begin{aligned}
x(uu')y \in L &\Leftrightarrow xu(u'y) \in L \\
&\Leftrightarrow xv(u'y) \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow (xv)u'y \in L \\
&\Leftrightarrow (xv)v'y \in L \quad \text{as } u' \approx_L v' \\
&\Leftrightarrow x(vv')y \in L.
\end{aligned}$$

Also,

$$\begin{aligned}
x(suu't)^+y \in L &\Leftrightarrow x(su(u't))^+y \in L \\
&\Leftrightarrow x(sv(u't))^+y \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow x((sv)u't)^+y \in L \\
&\Leftrightarrow x((sv)v't)^+y \in L \quad \text{as } u' \approx_L v' \\
&\Leftrightarrow x(svv't)^+y \in L.
\end{aligned}$$

Hence $uu' \approx_L vv'$.

Finally we must show that $\approx_L$ respects the $^+$ operation. Let $u \approx_L v$. Then

$$\begin{aligned}
xu^+y \in L &\Leftrightarrow x(1u1)^+y \in L \\
&\Leftrightarrow x(1v1)^+y \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow xv^+y \in L.
\end{aligned}$$

By Lemma 1.2.6 and the fact that idempotents commute,

$$\begin{aligned}
x(su^+t)^+y \in L &\Leftrightarrow x(su^+t^+)^+y \in L \quad \text{as } (ab)^+ = (ab^+)^+ \\
&\Leftrightarrow x(st^+u^+)^+y \in L \quad \text{as } a^+b^+ = b^+a^+ \\
&\Leftrightarrow x(st^+u)^+y \in L \quad \text{as } (ab)^+ = (ab^+)^+ \\
&\Leftrightarrow x(st^+u1)^+y \in L \\
&\Leftrightarrow x(st^+v1)^+y \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow x(st^+v)^+y \in L \\
&\Leftrightarrow x(st^+v^+)^+y \in L \quad \text{as } (ab)^+ = (ab^+)^+ \\
&\Leftrightarrow x(sv^+t^+)^+y \in L \quad \text{as } a^+b^+ = b^+a^+ \\
&\Leftrightarrow x(sv^+t)^+y \in L \quad \text{as } (ab)^+ = (ab^+)^+.
\end{aligned}$$

Therefore $u^+ \approx_L v^+$. □

We now show that $\approx_L$ is the largest congruence such that L is a union of congruence classes. Since $\approx_L$ says that for *certain* unary term functions $t(x)$ we have $t(u) \in L$ if and only if $t(v) \in L$ it follows from Proposition 2.1.6 that $\sim_L \subseteq \approx_L$. However, we demonstrate this directly below.

Proposition 2.2.3. *The relation $\approx_L$ is the largest $(2,1,0)$-congruence such that L is a union of congruence classes.*

Proof. First we need that L is indeed a union of $\approx_L$-classes. Let $a \in L$ and $a \approx_L b$.

Then $1a1 = a \in L$, so $1b1 = b \in L$. Hence L is a union of congruence classes.

Now suppose ρ is a $(2, 1, 0)$-congruence and L is a union of ρ-classes. Let $a\ \rho\ b$. Then for all $x, y, s, t \in M$, we have $xay\ \rho\ xby$, and since $sat\ \rho\ sbt$, we have $(sat)^+\ \rho\ (sbt)^+$, and hence $x(sat)^+y\ \rho\ x(sbt)^+y$. As L is a union of ρ-classes, we have $xay \in L$ if and only if $xby \in L$ and $x(sat)^+y \in L$ if and only if $x(sbt)^+y \in L$. Hence $a \approx_L b$. As $\rho \subseteq \approx_L$ for arbitrary (2,1,0)-congruence ρ, $\approx_L$ is the largest one of the kind. $\square$

As by Definition 2.1.4, the syntactic congruence $\sim_L$ is the largest congruence in an algebra such that L is a union of congruence classes, we have the following.

Theorem 2.2.4. *Let M be a left Ehresmann monoid and let L be a language over M. Then $\sim_L$ is the relation $\approx_L$.*

We have shown that for syntactic congruences over left Ehresmann monoids we need only two kinds of unary terms to determine them. Note that Theorem 2.2.4 does not appear to simplify for arbitrary left ample monoids. Unfortunately, the results for Ehresmann monoids will be more complicated. To further generalize with syntactic congruence to arbitrary unary or binary monoid, we see that without the axiom for left Ehresmann monoid, the proof of Proposition 2.2.2 does not work.

We show that Theorem 2.2.4 is indeed an extension of the characterisation for inverse monoids (in [34], for example). Of course we already know this in some sense since monoid congruences on an inverse monoid are inverse monoid congruences, but we now check directly. That is to say we show that the second kind of terms for $\sim_L$ are redundant in an inverse monoid.

Proposition 2.2.5. *In an inverse monoid M, if for all $x, y \in M$,*

$$xuy \in L \Leftrightarrow xvy \in L,$$

then for all $x, y, s, t \in M$,

$$x(sut)^+y \in L \Leftrightarrow x(svt)^+y \in L.$$

Proof. For clarity, since now we have yet to prove syntactic congruence in left Ehresmann monoid is an extension of the one in inverse monoid, we now denote them by $\sim_L^E$ and $\sim_L^I$ respectively. Note since an inverse monoid is regular, $\mathcal{R} = \widetilde{\mathcal{R}}$. As a^+ is the unique idempotent in $\widetilde{R}_a$,[1] it is the unique idempotent in R_a, and is equal to aa^{-1}. We would hope that $\sim_L^I$ also respects the $^+$ operation in an inverse monoid, and we show directly this is the case.

Suppose that $u, v \in M$ and for all $x, y \in M$,

$$xut \in L \Leftrightarrow xvy \in L.$$

[1] Here as usual we use non-script letters to denote the classes of relations defined by script letters

Then $u \sim_L^I v$. Consider the standard homomorphism from M to the quotient $M/\sim_L^I$ It is well known [21] and observed in Chapter 1 that the image $M/\sim_L^I$ is an inverse monoid with $[a]^{-1} = [a^{-1}]$. So

$$\begin{aligned} u \sim_L^I v &\Leftrightarrow [u] = [v] \\ &\Leftrightarrow [u^{-1}] = [u]^{-1} = [v]^{-1} = [v^{-1}] \\ &\Leftrightarrow u^{-1} \sim_L^I v^{-1}. \end{aligned}$$

As $\sim_L^I$ is a congruence, $u^+ = uu^{-1} \sim_L^I vv^{-1} = v^+$. Hence for any $x, y, s, t \in M$

$$\begin{aligned} u \sim_L^I v &\Rightarrow sut \sim_L^I svt \\ &\Rightarrow (sut)^+ \sim_L^I (svt)^+ \\ &\Rightarrow x(sut)^+y \sim_L^I x(svt)^+y. \end{aligned}$$

Thus

$$x(sut)^+y \in L \Leftrightarrow x(svt)^+y \in L,$$

as claimed. $\square$

From now on we will continue with $\sim_L$ rather than $\sim_L^E$ and $\sim_L^I$ without ambiguity.

We now give an example of an application of Theorem 2.2.4.

Lemma 2.2.6. *Let M be a left Ehresmann monoid, and let E be the semilattice of projections. Suppose that $uv \in E$ implies both $u, v \in E$. Then $\sim_E$ has classes, E and $M \setminus E$. Moreover, the syntactic congruence of E on the left Ehresmann monoid M coincides with that on the monoid M.*

Proof. Since E is a semilattice, if both $u, v \in E$, then $uv \in E$. So $uv \in E$ if and only if both $u, v \in E$.

Suppose that $u, v \in E$. Then for all $x, y \in M$, we have

$$xuy \in E \Leftrightarrow x, y \in E \Leftrightarrow xvy \in E.$$

Further, for any s, t we have

$$\begin{aligned} x(sut)^+y \in E &\Leftrightarrow x, y \in E \\ &\Leftrightarrow x(svt)^+y \in E. \end{aligned}$$

Thus $u \sim_E v$.

Further, if we are given that for all $x, y \in M$ we have $xuy \in E$ if and only if $xvy \in E$, then taking $x = y = 1$ we deduce that $u \in E$ if and only if $v \in E$ and then from the above that $u \sim_L v$ where M is regarded as left Ehresmann. $\square$

Below we demonstrate with an illustrative example.

Let M be a monoid acting on the left of a semilattice Y with identity by monoid morphisms. This means there is a map $M \times Y \to Y, (m, y) \mapsto m \cdot y$ such that

$$m \cdot 1_Y = 1_Y, 1_M \cdot y = y, m \cdot (n \cdot y) = mn \cdot y, m \cdot (yz) = (m \cdot y)(m \cdot z).$$

Then we can form the semidirect product $Y \rtimes M$ with operation

$$(y, m)(z, n) = (y(m \cdot z), mn)$$

and putting

$$(y, m)^+ = (y, 1)$$

we have that $Y \rtimes M$ is left ample [14], (so certainly left Ehresmann).

By taking certain M and certain Y, we describe some examples of languages and their syntactic congruences.

Let X be a set and let $M = X^*$. Let Y be the power set of X^* equipped with the operation of union. Then Y is a monoid semilattice with identity $\emptyset$. M acts on Y by

$$m \cdot y = \{mw : w \in y\}.$$

Let E be the language of idempotents $E = E(Y \rtimes M)$. By considering the second co-ordinates of idempotents, we see that if $(y, m)(z, n) = (y(m \cdot z), mn) \in E$ then $mn = 1$. Since $m, n \in M = X^*$, we get $m = n = 1$ and hence $(y, m), (z, n) \in E$. By Lemma 2.2.6, $u \sim_L v$ is equivalent to $u \in E$ if and only if $v \in E$, that is, the syntactic congruence of E has just two classes.

It is easy from the left-right dual that if M is a right Ehresmann monoid, and L is a M-language, then the syntactic congruence of L is given by:

for all $u, v \in M$ we have $u \sim_L v$ if and only if for all $x, y, s, t \in M$:

1. $$xuy \in L \quad \Leftrightarrow \quad xvy \in L$$

2. $$x(sut)^*y \in L \quad \Leftrightarrow \quad x(svt)^*y \in L.$$

The left-right dual of Proposition 2.2.2, and hence Theorem 2.2.3, clearly holds.

Both left-sided and right-sided cases hold with much simplified term functions as there are corresponding identities that simplify the behaviour of the unary operation. However, the 2-sided case is more complicated as $^+$ and * operators are interwined.

2.3 Syntactic congruences on two-sided Ehresmann monoids

To proceed with the case of two-sided Ehresmann monoids, we first define some specific biunary term functions.

For $i \in \mathbb{N}^0$, let $l_i, r_i \in M$. Define:

t_0 terms: $t_0(x) = l_0 x r_0$

t_i terms for $i \geq 1$ consist of two kinds of terms, t_i^+ and t_i^*

t_1 terms:

t_1^+ term: $t_1^+(x) = l_0(l_1 x r_1)^+ r_0$

t_1^* term: $t_1^*(x) = l_0(l_1 x r_1)^* r_0$

t_2 terms:

t_2^+ term: $t_2^+(x) = l_0(l_1(l_2 x r_2)^+ r_1)^* r_0$

t_2^* term: $t_2^*(x) = l_0(l_1(l_2 x r_2)^* r_1)^+ r_0$

t_3 terms:

t_3^+ term: $t_3^+(x) = l_0(l_1(l_2(l_3 x r_3)^+ r_2)^* r_1)^+ r_0$.

t_3^* term: $t_3^*(x) = l_0(l_1(l_2(l_3 x r_3)^* r_2)^+ r_1)^* r_0$.

$$\vdots$$

so that the $^+$ and * in the brackets alternate. Alternatively, we can define $t_0(x) = l_0 x r_0$, $t_1^+(x) = t_0((l_1 x r_1)^+)$, $t_1^*(x) = t_0((l_1 x r_1)^*)$, and recursively define $t_{i+1}^+(x) = t_i^*((l_{i+1} x r_{i+1})^+)$ and $t_{i+1}^*(x) = t_i^+((l_{i+1} x r_{i+1})^*)$ for $i \geq 1$.

Now we are going to use the above list of terms to determine the syntactic congruence of a language over a (two-sided) Ehresmann monoids.

Definition 2.3.1. Let M be an Ehresmann monoid. Given an M-language L, define the relation $\approx_L$ by the rule that for any $u, v \in M$ we have $u \approx_L v$ if and only if for all $l_0, l_1, \cdots \in M$ and for all $r_0, r_1, \cdots \in M$:

1. $$t_0(u) \in L \quad \Leftrightarrow \quad t_0(v) \in L$$

2. For all $n \in \mathbb{N}$, $$t_n^+(u) \in L \quad \Leftrightarrow \quad t_n^+(v) \in L$$ $$t_n^*(u) \in L \quad \Leftrightarrow \quad t_n^*(v) \in L.$$

First of all, we show:

Proposition 2.3.2. *The relation $\approx_L$ is a bi-unary monoid congruence.*

Proof. To show that a relation is a bi-unary monoid congruence, we need to show that it is an equivalence, it respects multiplication, and it respects the unary operations $^+$ and *. That is, if $u \approx_L v$ and $u' \approx_L v'$, then $uu' \approx_L vv'$, $u^+ \approx_L v^+$ and $u^* \approx_L v^*$.

It is easy to show that $\approx_L$ is an equivalence.

We now show $\approx_L$ is compatible with multiplication. Let $u \approx_L v$ and $u' \approx_L v'$. Then for a t_0 term $t_0(x) = l_0 x r_0$ we have

$$\begin{aligned}
l_0(uu')r_0 \in L &\Leftrightarrow l_0 u(u'r_0) \in L \\
&\Leftrightarrow l_0 v(u'r_0) \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow (l_0 v)u'r_0 \in L \\
&\Leftrightarrow (l_0 v)v'r_0 \in L \quad \text{as } u' \approx_L v' \\
&\Leftrightarrow l_0(vv')r_0 \in L.
\end{aligned}$$

For a t_n term, where we may take $t_n^+(x) = l_0 \dots (l_n x r_n)^+ \dots r_0$, we have

$$\begin{aligned}
l_0 \dots (l_n uu' r_n)^+ \dots r_0 \in L &\Leftrightarrow l_0 \dots (l_n u(u'r_n))^+ \dots r_0 \in L \\
&\Leftrightarrow l_0 \dots (l_n v(u'r_n))^+ \dots r_0 \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow l_0 \dots ((l_n v)u'r_n)^+ \dots r_0 \in L \\
&\Leftrightarrow l_0 \dots ((l_n v)v'r_n)^+ \dots r_0 \in L \quad \text{as } u' \approx_L v' \\
&\Leftrightarrow l_0 \dots (l_n vv' r_n)^+ \dots r_0 \in L.
\end{aligned}$$

and where we take a t_n^*-term, say $t_n^*(x) = l_0 \dots (l_n x r_n)^* \dots r_0$, we have dually that

$$\begin{aligned}
l_0 \dots (l_n uu' r_n)^* \dots r_0 \in L &\Leftrightarrow l_0 \dots (l_n u(u'r_n))^* \dots r_0 \in L \\
&\Leftrightarrow l_0 \dots (l_n v(u'r_n))^* \dots r_0 \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow l_0 \dots ((l_n v)u'r_n)^* \dots r_0 \in L \\
&\Leftrightarrow l_0 \dots ((l_n v)v'r_n)^* \dots r_0 \in L \quad \text{as } u' \approx_L v' \\
&\Leftrightarrow l_0 \dots (l_n vv' r_n)^* \dots r_0 \in L.
\end{aligned}$$

Hence $uu' \approx_L vv'$.

We now show $\approx_L$ is compatible with the operation $^+$. Let $u \approx_L v$. Then for a t_0-term $t_0(x) = l_0 x r_0$ we have

$$\begin{aligned}
l_0 u^+ r_0 \in L &\Leftrightarrow l_0(1u1)^+ r_0 \in L \\
&\Leftrightarrow l_0(1v1)^+ r_0 \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow l_0 v^+ r_0 \in L.
\end{aligned}$$

By Lemma 1.2.6 and the fact that idempotents commute, for a t_n^+-term $t_n^+(x) =$

$l_0 \dots (l_n x r_n)^+ \dots r_0$, we have

$$\begin{aligned}
l_0 \dots (l_n u^+ r_n)^+ \dots r_0 \in L \quad &\Leftrightarrow \quad l_0 \dots (l_n u^+ r_n^+)^+ \dots r_0 \in L \quad \text{as } (ab)^+ = (ab^+)^+ \\
&\Leftrightarrow \quad l_0 \dots (l_n r_n^+ u^+)^+ \dots r_0 \in L \quad \text{as } a^+b^+ = b^+a^+ \\
&\Leftrightarrow \quad l_0 \dots (l_n r_n^+ u)^+ \dots r_0 \in L \quad \text{as } (ab)^+ = (ab^+)^+ \\
&\Leftrightarrow \quad l_0 \dots (l_n r_n^+ u 1)^+ \dots r_0 \in L \\
&\Leftrightarrow \quad l_0 \dots (l_n r_n^+ v 1)^+ \dots r_0 \in L \quad \text{as } u \approx_L v \\
&\Leftrightarrow \quad l_0 \dots (l_n r_n^+ v)^+ \dots r_0 \in L \\
&\Leftrightarrow \quad l_0 \dots (l_n r_n^+ v^+)^+ \dots r_0 \in L \quad \text{as } (ab)^+ = (ab^+)^+ \\
&\Leftrightarrow \quad l_0 \dots (l_n v^+ r_n^+)^+ \dots r_0 \in L \quad \text{as } a^+b^+ = b^+a^+ \\
&\Leftrightarrow \quad l_0 \dots (l_n v^+ r_n)^+ \dots r_0 \in L \quad \text{as } (ab)^+ = (ab^+)^+
\end{aligned}$$

and for a t_n^*-term $t_n^*(x) = l_0 \dots (l_n x r_n)^* \dots r_0$, we have

$$\begin{aligned}
l_0 \dots (l_n u^+ r_n)^* \dots r_0 \in L \quad &\Leftrightarrow \quad l_0 \dots (l_n (1u1)^+ r_n)^* \dots r_0 \in L \\
&\Leftrightarrow \quad l_0 \dots (l_n (1v1)^+ r_n)^* \dots r_0 \in L \quad \text{using a } t_{n+1} \text{ term} \\
&\qquad \text{and as } u \approx_L v \\
&\Leftrightarrow \quad l_0 \dots (l_n v^+ r_n)^* \dots r_0 \in L.
\end{aligned}$$

It follows that $u^+ \approx_L v^+$.

To show $\approx_L$ respects the * operation is dual.

This completes the proof that $\approx_L$ is a biunary monoid congruence. □

Next, we need show that $\approx_L$ is the largest congruence such that L is a union of congruence classes.

Theorem 2.3.3. *The relation $\approx_L$ is the largest bi-unary monoid congruence such that L is a union of congruence classes. That is, $\approx_L$ is the syntactic congruence $\sim_L$.*

Proof. First we need that L is indeed a union of $\approx_L$-classes. Let $a \in L$ and suppose that $a \approx_L b$. Then consider the t_0 term $t_0(x) = l_0 x r_o$ where by letting $l_0 = r_0 = 1$. We have $1a1 = a \in L$, so $1b1 = b \in L$. Hence L is a union of congruence classes.

Now suppose ρ is a $(2,1,1,0)$-congruence and L is a union of ρ-classes. Let $a \; \rho \; b$. Then by Proposition 2.1.6 we have $t(a) \in L$ if and only if $t(b) \in L$ for any $(2,1,1,0)$-unary term function. Hence in particular this applies to the terms $t_i, i \geq 0$ that we have defined. Hence $a \approx_L b$. As $\rho \subseteq \approx_L$ for arbitrary $(2,1,1,0)$-congruence ρ, the relation $\approx_L$ is the largest one of the kind. Hence $\approx_L$ is the syntactic congruence $\sim_L$. □

Now we know that the congruence $\approx_L$ is indeed the syntactic congruence in L, we have proved:

Corollary 2.3.4. *The syntactic congruence $\sim_L$ of a language L inside a two-sided Ehresmann monoid M is given by:*

for all $u, v \in M$ we have that $u \sim_L v$ if and only if for all elements $l_0, l_1, \cdots$ and $r_0, r_1, \cdots$ in M:

1.

$$t_0(u) \in L \quad \Leftrightarrow \quad t_0(v) \in L$$

2. For all $n \in \mathbb{N}$,

$$t_n^+(u) \in L \quad \Leftrightarrow \quad t_n^+(v) \in L$$

$$t_n^*(u) \in L \quad \Leftrightarrow \quad t_n^*(v) \in L$$

We now formalise our approach in the following, the proof of which follows that of Theorem 2.3.3.

Theorem 2.3.5. *Let $\mathbf{A}$ be an algebra, let $\mathcal{T}$ be the set of all unary term operations and let $\mathcal{T}'$ be a subset of $\mathcal{T}$ such that $t(x) = x \in \mathcal{T}'$. Let $L \subseteq A$. Define the relation $\approx_L$ given by the rule that $u \approx_L v$ if for all $t(x) \in \mathcal{T}'$ we have*

$$t(u) \in L \Leftrightarrow t(v) \in L.$$

If $\approx_L$ is a congruence, then $\approx_L = \sim_L$.

Proof. We know that $u \sim_L v$ if and only if for all unary term functions $t(x)$ we have

$$t(u) \in L \Leftrightarrow t(v) \in L.$$

So if $u \sim_L v$ and $t(x) \in \mathcal{T}$, then $t(u) \in L$ if and only if $t(v) \in L$. Whereas $u \approx_L v$ if and only if for all $t(x) \in \mathcal{T}'$, we have $t(u) \in L$ if and only if $t(v) \in L$. This means that $\sim_L \subseteq \approx_L$. Now if $\approx_L$ is a congruence, and $u \approx_L v$, then as $t(x) = x \in \mathcal{T}'$, we have if $u \in L$, then $t(u) \in L$, so $t(v) \in L$, and so $v \in L$. This means L is a union of $\approx_L$ classes, so $\approx_L \subseteq \sim_L$. Hence $\approx_L = \sim_L$. $\square$

2.3.1 Syntactic congruences on two-sided Ehresmann monoids where idempotents are central

The list of unary term functions at the beginning of the Section 2.3 seems complicated. However, there are special cases where the list can be simplified. The first case is when the idempotents are central, that is, when $ea = ae$ for all $a \in M$ and $e \in E = E(M)$.

To see what we can get when idempotents are central, we first define $s_1^+(x) = px^+q$ and $s_1^*(x) = px^*q$.

Proposition 2.3.6. *Let M be an Ehresmann monoid with central idempotents. Then $^+$ and * coincide, i.e., $a^+ = a^*$ for all $a \in M$.*

Proof. Let $a \in M$. We know that $a^+a = a$, so $aa^+ = a$ as idempotents are central. Then $(aa^+)^* = a^*$, so $(a^*a^+)^* = a^*$, which means $a^*a^+ = a^*$. Hence in E, we have $a^* \leq a^+$. Dually, we obtain $a^+ \leq a^*$ so that $a^* = a^+$. □

So $s_1^+(x) = px^+q = px^*q = s_1^*(x)$. We can define $s_1(x) = px^+q$. Next we see that the $^+$ and * operations "can be distributed" into the brackets.

Lemma 2.3.7. *If M is Ehresmann with elements of E being central, then for any $s, t \in M$ we have*

$$(st)^+ = s^+t^+ \text{ and dually } (st)^* = s^*t^*.$$

Proof. We have

$$(st)^+ = (st^+)^+ = (t^+s)^+ = (t^+s^+)^+ = t^+s^+ = s^+t^+.$$

and the case for * holds as $^+$ and * coincide. □

In fact we have:

Proposition 2.3.8. *Let M be an Ehresmann monoid with central idempotents. Then it is actually restriction monoid.*

Proof. All we need to do is to check the ample identities. In fact, as $^+$ and * coincide, it suffice in checking that the left ample identity holds.

$$(ab^+)^+a = (b^+a)^+a = (b^+a^+)^+a = b^+a^+a = b^+a = ab^+.$$

□

In the language of Theorem 2.3.5 the next result is saying that to determine syntactic congruences in Ehresmann monoids with central idempotents we can restrict our set of unary term operations to those of the form t_0 and s.

Proposition 2.3.9. *Let M be an Ehresemann monoid with central idempotents and let $L \subseteq M$. Then $\sim_L$ coincides with $\approx_L$, where for any $u, v \in M$ we have $u \approx_L v$ if and only if for all $p, q \in M$ we have*

$$puq \in L \text{ iff } pvq \in L,$$

$$pu^+q \in L \text{ iff } pv^+q \in L.$$

Proof. Let $u, v \in M$ be such that $u \approx_L v$. Then for any $k \in M$, and for all $p, q \in M$,

$$pukq \in L \text{ iff } pvkq \in L$$

and

$$\begin{aligned} p(uk)^+q \in L \quad &\text{iff} \quad pu^+k^+q \in L \\ &\text{iff} \quad pv^+k^+q \in L \\ &\text{iff} \quad p(vk)^+q \in L. \end{aligned}$$

We have shown that $uk \approx_L vk$ and dually, $ku \approx_L kv$. So if $h \approx k$ then we obtain

$$uh \approx vh \approx vk,$$

so that is a semigroup congruence.

Still with $u \approx_L v$, for all $p, q \in M$, first using the $s(x)$ term we have

$$pu^+q \in L \text{ iff } pv^+q \in L.$$

Further, using $s(x)$ terms again,

$$p(u^+)^+q \in L \text{ iff } pu^+q \in L \text{ iff } pv^+q \in L \text{ iff } p(v^+)^+q \in L,$$

so that $u^+ \approx_L v^+$. (Of course, $u^* \approx v^*$ as $^+$ and * coincide.) So $\approx_L$ is a $(2,1,1)$-congruence. As $p, q \in M$ is arbitrary, by setting $p = q = 1$, we have $u \in L$ iff $v \in L$, which means L is a union of congruence classes. It follows from Theorem 2.3.5 that $\sim_L$ coincides with $\approx_L$. □

2.3.2 When the language is finite

Another case where we hope for simplification is when the language L is finite, where we hope that we need terms t_i for only finitely many $i \in \mathbb{N}^0$.

To this end we define the relations $\sim_{L,i}$.

Definition 2.3.10. Let the relation $\sim_{L,i}$ be determined by $t_0, t_1, \ldots, t_i$. That is, $u \sim_{L,i} v$ means

$$t_j(u) \in L \text{ iff } t_j(v) \in L \text{ for all } 0 \leq j \leq i.$$

To simplify notation, we would usually refer to $\sim_{L,i}$ as $\sim_i$, where L is known.

Lemma 2.3.11. *With the above definitions we have*

$$\sim_0 \supseteq \sim_1 \supseteq \ \ldots \ \supseteq \sim_i \supseteq \ldots$$

Proof. It suffices to prove that $\sim_i \supseteq \sim_{i+1}$ for any $i \in \mathbb{N}^0$. Recall that $u \sim_i v$ means -

$$t_j(u) \in L \text{ iff } t_j(v) \in L \text{ for all } 0 \leq j \leq i.$$

So $u \sim_{i+1} v$ means

$$t_j(u) \in L \text{ iff } t_j(v) \in L \text{ for all } 0 \leq j \leq i+1,$$

so that

$$t_j(u) \in L \text{ iff } t_j(v) \in L \text{ for all } l\, 0 \leq j \leq i$$

certainly holds. Hence $u \sim_i v$. That is, $\sim_i \supseteq \sim_{i+1}$. □

Lemma 2.3.12. *We have*

$$\bigcap_{i \in \mathbb{N}^0} \sim_i = \sim_L .$$

Proof. We know that $u \sim_L v$ means

$$t_j(u) \in L \text{ iff } t_j(v) \in L \text{ for all } 0 \leq j,$$

so that certainly

$$t_j(u) \in L \text{ iff } t_j(v) \in L \text{ for all } 0 \leq j \leq i$$

holds. Hence $u \sim_i v$. That is, $\sim_i \supseteq \sim_L$ which gives us that $\bigcap_{i \in \mathbb{N}^0} \sim_i \supseteq \sim_L$.

Conversely, if $u \bigcap_{i \in \mathbb{N}^0} \sim_i v$, we have $u \sim_i v$ for all $i \in \mathbb{N}^0$, then by definition for any $i \in \mathbb{N}^0$ and for any term $t_i(x)$, we have $t_i(u) \in L$ if and only if $t_i(v) \in L$ (since $u \sim_i v$), and so we deduce $u \sim_L v$ as required. □

We hope that for any finite set L we can show $\sim_i = \sim_L$ for some i, which means that when we are expressing $\sim_L$ we need only check that for finitely many types of terms t_i we have $t_i(u) \in L$ if and only if $t_i(v) \in L$, in order to deduce that $u \sim_L v$. We can show this is true in the special case that M is the free ample monoid on X. The description of the free ample monoid $\mathrm{FA}(X)$ is given in Subsection 1.4.1.

First, let M be an Ehresmann monoid and let $L \subseteq M$. Let

$$H = H_L = \{x \in M \mid t_j(x) \in L \text{ for some } j\}$$

and $K = M \backslash H$. Then, given $u, v \in K$, for any $t_i(x)$, we have $t_i(u) \notin L$ and $t_i(v) \notin L$ so the statement:

$$t_i(u) \in L \text{ iff } t_i(v) \in L$$

for all $i \geq 0$ is true! If $u \in H$ and $w \in K$, then $\exists\, i$ with $t_i(u) \in L$ but $t_i(w) \notin L$. Then $u \not\sim_L w$. So K is a $\sim_L$-class. Note also that $u \not\sim_i w$, and because

$$\sim_0 \supseteq \sim_1 \supseteq \ \ldots \ \supseteq \sim_i \supseteq \ldots,$$

we have $u \not\sim_j w$ for all $j \geq i$.

We now focus on the case where $M = \mathrm{FA}(X)$ is free ample on X and let $L \subseteq \mathrm{FA}(X)$.

Lemma 2.3.13. *For a finite language L in $M = \mathrm{FA}(X)$, the set $H = H_L$ is finite.*

Proof. Before we prove the lemma, we first prove:

Lemma 2.3.14. *Let $(A, a), (B, b) \in M$. If $t((B, b)) = (A, a)$ for some term $t(x)$, then $|B| \leq |A|$ and the letters of the words in B have to be letters in the words of A.*

Proof. We first remark that $A \subseteq FG(X)$ is prefix closed, $a \in A$ and $a \in X^*$.

If $t(x) = x$, then we have $(A, a) = (B, b)$, and it is clear that $|B| = |A| \leq |A|$ and the letters of the words in B have to be letters in the words of A.

If $t(x) = s(x)u(x)$ and $t(B, b) = (T, t)$, $s(B, b) = (S, s)$ and $u(B, b) = (U, u)$, then $(T, t) = (S, s)(U, u)$. As a result $T = S \cup s \cdot U$. As $s \in S \subseteq T$ and $U \subseteq s^{-1} \cdot T$, we have $|S| \leq |T|$, $s \in T$ and also $|U| \leq |s^{-1} \cdot T| = |T|$.

If $t(x) = s^+(x)$, with $t(B, b) = (T, t)$ and $s(B, b) = (S, s)$, then $(T, t) = (S, s)^+ = (S, 1)$ and hence $|T| = |S|$.

If $t(x) = s^*(x)$, with $t(B, b) = (T, t)$ and $s(B, b) = (S, s)$, then $(T, t) = (S, s)^* = (s^{-1} \cdot S, 1)$ and hence $|T| = |S|$.

Also in the above 3 cases, the letters of the words in S and U have to be letters in the words of T. The result is clear if $S \subseteq T$. On the other hand, for any $g \in T$, $g^{-1} \cdot T = \{(g^{-1}t)^r | t \in T\}$. Thus the words in $g^{-1} \cdot T$ are made up of letters of words in T.

It follows by induction on the number of basic operations needed to construct the unary term $t(x)$ such that $t((B, b)) = (A, a)$ that $|B| \leq |A|$ and the letters of the words in B have to be letters in the words of A. $\square$

As a result, if $|A| = k$, then as $|B| \leq k$, and the words of B are made up from the letters of A, there are only finitely many choices for B and hence as $b \in B$, only finitely many choices for b and so only finitely many choices for (B, b). Hence if L is finite, there are only finitely many $(A, a) \in L$ and thus finitely many (B, b) have terms $t_i(x)$ such that $t_i((B, b)) \in L$. So $H = H_L$ is finite. $\square$

We now have the following situation. Let $L \subseteq \mathrm{FA}(X)$ be finite and let H, K be as given. Then we have $\mathrm{FA}(X) = H \cup K$, where H is finite, $H \cap K = \emptyset$ and K is contained in a single $\sim_L$-class. We know therefore that H is a union of $\sim_L$-classes. We have

$$\sim_0 \supseteq \sim_1 \supseteq \ldots \supseteq \sim_i \supseteq \ldots$$

Let $\sim_i^H$ be the equivalence relation on H given by

$$h \sim_i^H k \text{ iff } h \sim_i k.$$

We partition H into $\sim_0^H$-classes. We then partition H into $\sim_i^H$-classes; sooner or later we find an $i \geq 0$ such that the partition given by $\sim_i^H$ is the same as that given by $\sim_j^H$ for any $j \geq i$. This implies for $h, k \in H$, such that $h \sim_i k$, then for all $j \in \mathbb{N}$, $t_j(u) \in L$ iff $t_j(v) \in L$. This gives us $h \sim_L k$.

We now prove:

Theorem 2.3.15. *If L is a finite language over* $\mathrm{FA}(X)$*, then* $\sim_L = \sim_j$ *for some* $j \geq 0$.

Proof. Let $i \geq 0$ be as above. We know that $\sim_i \supseteq \sim_L$.

Suppose $h \sim_i k$. If $h, k \in H$ then from above, $h \sim_L k$. If $h, k \in K$ then we know $h \sim_L k$.

Suppose $h \in H$ and $k \in K$ and $h \sim_i k$. If also $h' \in H$ and $k' \in K$ and $h' \sim_i k'$, by transitivity of $\sim_i$, we have $h' \sim_i k' \sim_i k \sim_i h$, since $k \sim_L k'$ and $\sim_L \subseteq \sim_i$. Hence $h \sim_i h'$. So, if exists, there is at most one $\sim_L$-class in H is contained in the same $\sim_i$-class as K.

Suppose $h \in H$ and $h \sim_i k$ for some (equivalently, all) $k \in K$. Then $\exists\ i_h > i$ with $t_{i_h}(h) \in L$ but $t_{i_h}(k) \notin L$. Thus $h \not\sim_l k$ for all $l \geq i_h$. Let j be the maximum of $\{i_h \mid h \in H\}$. Together with the fact that $\sim_l^H = \sim_i^H$ for any $l \geq i$, and $h \sim_i k$ for all i and for all $k, h \in K$, we have $\sim_l = \sim_j$ for any $l \geq j$, thus $\sim_j = \sim_L$. $\square$

Note that Theorem 2.3.15 holds for any Ehresmann monoid M whenever H is finite.

2.3.3 An example where we need our full list of unary term functions

The aim of this subsection is to give an example of a language over an ample monoid such that $\sim_L \neq \sim_i$ for any $i \geq 0$. Again we take a free ample monoid $M = \mathrm{FA}(X)$, where here we choose X to be

$$X = \{a_i, b, u_i, v_i : i \geq 0\}.$$

Let L be the language consisting of the following elements:

$$\begin{gathered} u_0 a_0 v_0 \\ u_1(u_0 a_1 v_0)^+ v_1 \\ u_2(u_1(u_0 a_2 v_0)^+ v_1)^* v_2 \\ \vdots \end{gathered}$$

To see $\sim_L \neq \sim_i$ for any $i \geq 0$, first see for any term $t(x)$ (other than $t(x) = 1$) we have $t(b) \notin L$. Certainly then $t_0(b) \notin L$, $t_i^+(b) \notin L$ and $t_i^*(b) \notin L$ for any $i > 0$ and any choice of $l_0, l_1, \ldots, r_0, r_1, \ldots$. Consider the t_0 term $t_0(x) = u_0 x v_0$. We have $t_0(a_0) \in L$ but $t_0(b) \notin L$. So $a_0 \not\sim_0 b$.

We have $a_1 \sim_0 b$, since for any t_0 term, $t_0(a_1) = l_0 a_1 r_0 \notin L$ and we know $t_0(b) \notin L$. On the other hand, taking the t_1^+ term $t_1^+(x) = u_1(u_0 x v_0)^+ v_1$, we have $t_1^+(a_1) \in L$ but $t_1^+(b) \notin L$. So, $a_1 \not\sim_1 b$, and hence $\sim_1 \subset \sim_0$.

In general, for any $i \geq 0$, we have $a_{i+1} \sim_i b$ as for any choice of $t_0(x)$ or $t_j(x)$, $j \leq i$, we have $t_0(a_{i+1}), t_j(a_{i+1}), t_0(b), t_j(b) \notin L$. However, $a_{i+1} \not\sim_{i+1} b$, for if we take

$$t_{i+1}^+(x) = u_{i+1}(\ldots(u_0 a_{i+1} v_0)^+ v_1 \ldots) v_{i+1}$$

we have $t_{i+1}^+(a_{i+1}) \in L$, but $t_{i+1}^+(b) \notin L$. So, $\sim_{i+1} \subset \sim_i$ for all i, and we need all terms for $\sim_L$.

2.3.4 Syntactic congruences on two-sided Ehresmann monoids where the language is the set of idempotents

Yet another case where there is simplification is when the language is the set of idempotents of the free ample monoid. What follows is analogous to Lemma 2.2.6.

Lemma 2.3.16. *Let M be an Ehresmann monoid, and let E be the semilattice of projections. Suppose that $uv \in E$ implies both u and $v \in E$. Then $\sim_E$ has classes, E and $M \setminus E$. Moreover, the syntactic congruence of E on the Ehresmann monoid M coincides with that on the monoid M.*

Proof. Since E is a semilattice, if both u and $v \in E$, then $uv \in E$. So $uv \in E$ if and only if both u and $v \in E$.

Suppose that $u, v \in E$. Then for all $x, y \in M$, we have

$$xuy \in E \Leftrightarrow x, y \in E \Leftrightarrow xvy \in E.$$

Further, for any $t(x) = t_i^+(x)$ or $t(x) = t_i^*(x)$ and any $a \in FA(X)$ we have $t(a) = l_0 e r_0$ for some $e \in E$, so that

$$\begin{aligned} t(u) \in E &\Leftrightarrow l_0, r_0 \in E \\ &\Leftrightarrow t(v) \in E. \end{aligned}$$

Thus $u \sim_E v$.

Further, if we are given that for all $x, y \in M$ we have $xuy \in E$ if and only if $xvy \in E$, then taking $x = y = 1$ we deduce that $u \in E$ if and only if $v \in E$ and then from the above that $u \sim_L v$ where M is regarded as Ehresmann. □

Below we would demonstrate an illustrative examples:

Let M be the free ample monoid, $L = E = E(M)$. If $uv \in E$, by taking the homomorphism to X^* we end up with second co-ords being 1, so $u, v \in E$. By Lemma 2.3.16, $u \sim_L v$ is equivalent to $u \in E$ if and only if $v \in E$.

There are further examples of syntactic congruence of different languages in Chapter 5.

Chapter 3

Recognisability of languages using syntactic congruences

In the previous chapter we considered syntactic congruences on universal algebras, focussing on left and two-sided ample and Ehresmann monoids. Here we begin our consideration of recognisable languages in universal algebras, using the notion of the syntactic congruence. In a later chapter we will investigate connections with finite state automata.

The following definition is familiar for monoids [34].

Definition 3.0.1. Let $\mathbf{A}$ be a universal algebra and let $L \subseteq A$. We say that $L \in \operatorname{Rec} \mathbf{A}$ if and only if $\mathbf{A}/ \sim_L$ is finite.

If L is in $\operatorname{Rec} \mathbf{A}$, we say that L is *recognisable*.

Lemma 3.0.2. *Given the definition of recognisable language in Definition 3.0.1, $L \in \operatorname{Rec} \mathbf{A}$ if and only if there is a morphism from $\phi : A \to N$ where N is finite such that $L = L\phi\phi^{-1}$.*

Proof. If $L \in \operatorname{Rec} \mathbf{A}$, then $\mathbf{A}/ \sim_L$ is finite. Define $\phi : \mathbf{A} \to \mathbf{A}/ \sim_L$ by $a\phi = [a]$. Obviously, $L \subseteq L\phi\phi^{-1}$. To show that $L\phi\phi^{-1} \subseteq L$, let $a \in L\phi\phi^{-1}$. Then $a\phi = a'\phi$ for some $a' \in L$. Hence $[a] = [a']$ which means $a \sim_L a'$. As L is a union of $\sim_L$-classes. $a \in L$. As a result, $L\phi\phi^{-1} \subseteq L$, so that $L = L\phi\phi^{-1}$.

On the other hand, suppose there is a morphism from $\phi : A \to N$ where N is finite such that $L = L\phi\phi^{-1}$. Let $a \in L$ and $a' \in A$ be such that $a\phi = a'\phi$, in other words, $a \ker\phi\ a'$. Now $a' \in a\phi\phi^{-1} \subseteq L\phi\phi^{-1} = L$, hence L is a union of $\ker\phi$-classes. As $\sim_L$ is the largest congruence such that L is a union of congruence class, $\ker\phi \subseteq \sim_L$. As a result, we have $|\mathbf{A}/ \sim_L| \leq |\mathbf{A}/ \ker\phi| = |N| < \infty$, and thus $L \in \operatorname{Rec} \mathbf{A}$. $\square$

It is important to relate recognizable languages in similar algebras, that is, algebras with the same signature, because we can connect recognizable languages to algebras with better understood structures. The good news is that, we can show that a language is recognizable if and only if its pre-image is recognizable.

Suppose $\mathbf{A}$ and $\mathbf{B}$ are two similar algebras, that is, that they have the same signature. Also suppose that $\theta : \mathbf{A} \to \mathbf{B}$ is a surjective homomorphism from $\mathbf{A}$ onto $\mathbf{B}$. To relate the languages of the algebras, what we do is to relate their syntactic congruences. Let $L \subseteq B$ and $K = L\theta^{-1} \subseteq A$; we will relate the syntactic congruence $\sim_K$ of K and the syntactic congruence $\sim_L$ of L. In particular, we would like to show that $(a, b) \in \sim_K$ if and only if $(a\theta, b\theta) \in \sim_L$.

Define

$$\nu_{L\sim_K} = \{(a', b') : a' = a\theta \text{ and } b' = b\theta \text{ for some } a, b \in A \text{ s.t. } (a, b) \in \sim_K\} \subseteq \mathbf{B} \times \mathbf{B}.$$

Lemma 3.0.3. *The relation $\nu_{L\sim_K}$ is a congruence on $\mathbf{B}$ such that L is a union of congruence classes.*

Proof. First we need to prove that $\nu_{L\sim_K}$ is a congruence.

Let us prove that it is reflexive. Since θ is surjective, for all $a' \in B$, there exists $a \in A$ such that $a' = a\theta$. Since $\sim_K$ is a congruence, $(a, a) \in \sim_K$. Therefore $(a', a') \in \nu_{L\sim_K}$.

Let us prove that it is symmetric. If $a', b' \in B$ is such that $(a', b') \in \nu_{L\sim_K}$, then there exists $a, b \in A$ s.t. $a' = a\theta, b' = b\theta$ and $(a, b) \in \sim_K$. Since $\sim_K$ is a congruence, $(b, a) \in \sim_K$, and hence $(b', a') \in \nu_{L\sim_K}$.

Let us prove that it is transitive. If $a', b', c' \in B$ such that $(a', b'), (b', c') \in \nu_{L\sim_K}$, then there exists $a, b_1, b_2, c \in A$ such that $a' = a\theta$, $b_1\theta = b' = b_2\theta$, $c' = c\theta$ and $(a, b_1), (b_2, c) \in \sim_K$. As $b_1\theta = b' = b_2\theta$, $b_1 \ker\theta\ b_2$. Note since $K = L\theta^{-1}$, $\ker\theta$ is a congruence such that K is a union of $\ker\theta$-classes. Therefore, $\ker\theta \subseteq \sim_K$ as $\sim_K$ is the largest congruence with K as a union of congruence classes. So $b_1 \ker\theta\ b_2$ implies $b_1 \sim_K b_2$. By the transitivity of $\sim_K$ we have $(a, c) \in \sim_K$, so $(a', c') \in \nu_{L\sim_K}$.

Let us prove that it is compatible with basic operations. Let F be any basic operation of rank n. For each $i = 1, \ldots, n$, let $a'_i, b'_i \in B$, be such that $(a'_i, b'_i) \in \nu_{L\sim_K}$. Then there exists $a_i, b_i \in A$ such that $a'_i = a_i\theta, b'_i = b_i\theta$ and $(a_i, b_i) \in\sim_K$. As $(a_i, b_i) \in\sim_K$ and $\sim_K$ is a congruence,

$$\begin{aligned}
(F(a_1, \ldots, a_n), F(b_1, \ldots, b_n)) \in \sim_K \ &\Rightarrow\ ((F(a_1, \ldots, a_n))\theta, (F(b_1, \ldots, b_n))\theta) \in \nu_{L\sim_K} \\
&\Rightarrow\ (F(a_1\theta, \ldots, a_n\theta), F(b_1\theta, \ldots, b_n\theta)) \in \nu_{L\sim_K} \\
&\Rightarrow\ (F(a'_1, \ldots, a'_n), F(b'_1, \ldots, b'_n)) \in \nu_{L\sim_K}
\end{aligned}$$

Then we need to prove that L is a union of $\nu_{L\sim_K}$-classes. Suppose $a' \in L$, and $(a', b') \in \nu_{L\sim_K}$. Then $a' = a\theta$ for some $a \in K$, $b' = b\theta$ for some $b \in A$ such that $(a, b) \in \sim_K$. Therefore, as K is a union of $\sim_K$-classes, $b \in K$, and $b' = b\theta \in K\theta = L$. So L is a union of $\nu_{L\sim_K}$-classes. $\square$

On the other hand, we define

$$\nu_{K_{\sim_L}} = \{(a,b) : (a\theta, b\theta) \in \sim_L\} \subseteq \mathbf{A} \times \mathbf{A}.$$

Lemma 3.0.4. *The relation $\nu_{K_{\sim_L}}$ is a congruence such that K is a union of congruence classes.*

Proof. As before, we need to prove that $\nu_{K_{\sim_L}}$ is a congruence. First we prove it is reflexive. This follows since for all $a \in A$, we have $(a\theta, a\theta) \in \sim_L$, since $\sim_L$ is a congruence, and so $(a,a) \in \nu_{K_{\sim_L}}$.

Then let us prove it is symmetric. We have

$$\begin{aligned}
(a,b) \in \nu_{K_{\sim_L}} &\Rightarrow (a\theta, b\theta) \in \sim_L, && (3.1)\\
&\Rightarrow (b\theta, a\theta) \in \sim_L \qquad \text{as } \sim_L \text{ is a congruence,} && (3.2)\\
&\Rightarrow (b,a) \in \nu_{K_{\sim_L}}. && (3.3)
\end{aligned}$$

Next, we prove it is transitive.

$$\begin{aligned}
(a,b),(b,c) \in \nu_{K_{\sim_L}} &\Rightarrow (a\theta, b\theta),(b\theta, c\theta) \in \sim_L, && (3.4)\\
&\Rightarrow (a\theta, c\theta) \in \sim_L \qquad \text{as } \sim_L \text{ is a congruence,} && (3.5)\\
&\Rightarrow (a,c) \in \nu_{K_{\sim_L}}. && (3.6)
\end{aligned}$$

We also need to prove it is compatible with basic operations. Let F be a basic operation of rank n, and suppose $(a_i, b_i) \in \nu_{K_{\sim_L}}$ for all $i = 1, \ldots, n$. Then

$$\begin{aligned}
&(a_i\theta, b_i\theta) \in \sim_L \ (\forall i = 1, \ldots, n),\\
&\Rightarrow (F(a_1\theta, \ldots, a_n\theta), F(b_1\theta, \ldots, b_n\theta)) \in \sim_L, \quad \text{as } \sim_L \text{ is a congruence,}\\
&\Rightarrow ((F(a_1, \ldots, a_n))\theta, (F(b_1, \ldots, b_n))\theta) \in \sim_L, \quad \text{as } \theta \text{ is a homomorphism,}\\
&\Rightarrow (F(a_1, \ldots, a_n), F(b_1, \ldots, b_n)) \in \nu_{K_{\sim_L}}.
\end{aligned}$$

Finally, we need to prove that K is a union of $\nu_{K_{\sim_L}}$-classes. Suppose $a \in K$, and $(a,b) \in \nu_{K_{\sim_L}}$. Then $(a\theta, b\theta) \in \sim_L$. Because $a \in K = L\theta^{-1}$, $a\theta \in L$. Also since L is a union of $\sim_L$-classes, we have $b\theta \in L$, therefore $b \in L\theta^{-1} = K$. □

The above lemmas have proved half of the following:

Theorem 3.0.5. *Let $\mathbf{A}, \mathbf{B}$ be similar algebras, $\theta : \mathbf{A} \to \mathbf{B}$ be a surjective homomorphism. Let $L \subseteq B$ and $K = L\theta^{-1} \subseteq A$, and $\sim_L, \sim_K, \nu_{L_{\sim_K}}, \nu_{K_{\sim_L}}$ be defined as above. Then $\sim_L = \nu_{L_{\sim_K}}$ and $\sim_K = \nu_{K_{\sim_L}}$.*

Proof. As $\nu_{L_{\sim_K}}$ is a congruence such that L is a union of congruence classes, we know that $\nu_{L_{\sim_K}} \subseteq \sim_L$. Similarly, as $\nu_{K_{\sim_L}}$ is a congruence such that K is a union of congruence classes, we know that $\nu_{K_{\sim_L}} \subseteq \sim_K$. To prove that $\sim_L \subseteq \nu_{L_{\sim_K}}$, suppose $(a', b') \in \sim_L$, and let $a, b \in A$ be such that $a' = a\theta, b' = b\theta$. Then $(a,b) \in \nu_{K_{\sim_L}} \subseteq \sim_K$.

By the definition of $\nu_{L\sim_K}$, $(a',b') \in \nu_{L\sim_K}$. Hence $\nu_{L\sim_K} = \nu_L$. On the other hand, to prove that $\sim_K \subseteq \nu_{K\sim_L}$, suppose $(a,b) \in \sim_K$. Then $(a\theta, b\theta) \in \nu_{L\sim_K} = \sim_L$, hence by the definition of $\nu_{K\sim_L}$, $(a,b) \in \nu_{K\sim_L}$. Hence $\nu_{K\sim_L} = \sim_K$. □

One can see from the above proof that:

Corollary 3.0.6. *For any $a, b \in A$, we have $(a,b) \in \sim_K$ if and only if $(a\theta, b\theta) \in \sim_L$.*

Finally we have:

Theorem 3.0.7. *Let $\mathbf{A}, \mathbf{B}$ be similar algebras, $\theta : \mathbf{A} \to \mathbf{B}$ be a surjective homomorphism. Let $L \subseteq B$. Then*

$$L \in \operatorname{Rec} \mathbf{B} \Leftrightarrow L\theta^{-1} \in \operatorname{Rec} \mathbf{A}.$$

Proof. Let $K = L\theta^{-1}$, Corollary 3.0.6 implies that $(a,b) \in \sim_K$ if and only if $(a\theta, b\theta) \in \sim_L$. Hence there is a one-one correspondence between $\mathbf{A}/\sim_{L\theta^{-1}}$ and $\mathbf{B}/\sim_L$, which takes $[u]_{\sim_K}$ to $[u\theta]_{\sim_L}$, thus $|\mathbf{A}/\sim_{L\theta^{-1}}|$ is finite if and only if $|\mathbf{B}/\sim_L|$ is finite. □

Now given $K \subseteq A$, K is said to be $\ker\theta$-*closed* if K is a union of $\ker\theta$-classes.

Theorem 3.0.8. *Let $\mathbf{A}, \mathbf{B}$ be similar algebras, $\theta : \mathbf{A} \to \mathbf{B}$ be a surjective homomorphism. Let $K \subseteq A$. The following are equivalent:*

1. *K is $\ker\theta$-closed;*

2. *$K = K\theta\theta^{-1}$;*

3. *$K = L\theta^{-1}$ for some $L \subseteq B$;*

4. *$\ker\theta \subseteq \sim_K$.*

Moreover, if K satisfies any one of the above condition, $K \in \operatorname{Rec} \mathbf{A} \Leftrightarrow K\theta \in \operatorname{Rec} \mathbf{B}$.

Proof. (1)⇒(2) Suppose K is $\ker\theta$-closed. We always have $K \subseteq K\theta\theta^{-1}$. To show that $K\theta\theta^{-1} \subseteq K$, let $a \in K\theta\theta^{-1}$. Then $a\theta \in K\theta$, and hence $a\theta = b\theta$ for some $b \in K$. By the definition of $\ker\theta$, $a \ker\theta\, b$. Hence a is also in K.

(2)⇒(3) Suppose $K = K\theta\theta^{-1}$. Let $L = K\theta$. Then $L\theta^{-1} = K\theta\theta^{-1} = K$.

(3)⇒(4) Suppose $K = L\theta^{-1}$ for some $L \subseteq B$. Let $a \in K$ and $a \ker\theta\, b$. Then $a\theta \in L$ and $b\theta = a\theta \in L$, hence $b \in L\theta^{-1} = K$. Hence $\ker\theta$ is a congruence such that K is a union of congruence class. By the definition of $\sim_K$, $\ker\theta \subseteq \sim_K$.

(4)⇒(1) Suppose $\ker\theta \subseteq \sim_K$. Let $a \in K$ and $a \ker\theta\, b$. Then $a \sim_K b$. By the definition of $\sim_K$, K is a union of $\sim_K$, hence $b \in K$. Therefore K is $\ker\theta$-closed.

The final remark follows from Theorem 3.0.7 by letting $L = K\theta$. □

Here we require $\mathbf{A}, \mathbf{B}$ to be similar algebras. The thing we build on is the free term algebra, and other similar algebras can be considered as factors of this via a congruence. Let us take the signature of Ehresmann monoids (2,1,1,0) as an example. Let X be a countable set, which can be finite or infinite. We define the elements of the free term algebra $FT_{\mathcal{S}}(X)$ on X of the signature $\mathcal{S} = (2,1,1,0)$ inductively as follows:

We first include the elements in X. That is, $x \in FT_{\mathcal{S}}(X)$ for all $x \in X$. We then add in an extra symbol for each nullary operation, that is, $1 \in FT_{\mathcal{S}}(X)$. Then we define the rest of the algebra inductively using the unary and binary operations. If $s, t \in FT_{\mathcal{S}}(X)$, then $s \cdot t \in FT_{\mathcal{S}}(X), s^+ \in FT_{\mathcal{S}}(X)$ and $s^* \in FT_{\mathcal{S}}(X)$. Here $\cdot$ is a symbol for the binary operation, and $^+$ and * are symbols for the two unary operations of the signature (2,1,1,0). Then we can make $FT_{\mathcal{S}}(X)$ into an algebra by defining the operations as above for any $s, t \in FT_{\mathcal{S}}(X)$.

Taking as an example, for $x, y \in FT_{\mathcal{S}}(X)$, we have the following elements of $FT_{\mathcal{S}}(X)$:

$$1,\, x\,,\, y\,,\, y^+,\, x^+ \cdot (x \cdot y)^* \cdot y\,,\, (y^+)^+,\, x \cdot y^+,\, x \cdot (y \cdot y),\, (x \cdot y) \cdot y\,,\, (x \cdot x) \cdot x.$$

The object we built is the free term algebra with signature $(2,1,1,0)$.

If A is any algebra in the same signature as $FT_{\mathcal{S}}(X)$, and $\theta : X \to A$ is a map, then θ can be extended uniquely to a morphism ϕ from $FT_{\mathcal{S}}(X)$ to A by inductively putting

$$1_{FT_{\mathcal{S}}(X)}\phi = 1_A$$

and for all $x \in X$,

$$x\phi = x\theta.$$

Let $s, t \in FT_{\mathcal{S}}(X)$ be defined inductively as above. If $s\phi$ and $t\phi$ are defined, then we can define $(s \cdot t)\phi = (s\phi)(t\phi)$, $(s^+)\phi = s\phi^+$ and $(s^*)\phi = s\phi^*$. Then ϕ is well defined and a morphism. Note that if $w \in FT_{\mathcal{S}}(X)$, then w has a unique expression as a sequence of symbols (from x, the set of basic operational symbols, and brackets.)

From the free term algebra, we obtain other algebras that can be defined by identities. We can define congruence relations induced by these identities, and the quotient set defined in the natural way is then isomorphic to our target algebra. Formally we have:

Proposition 3.0.9. *Let $T = FT_{\mathcal{S}}(X)$ be a free term algebra with signature $\mathcal{S}$. Let $FA_{\mathcal{S}}(X)$ be a free algebra of the same signature $\mathcal{S}$, determined by a set of identities $\{l_i = r_i : i \in I\}$ for some index set I. Let $H = \{(l_i, r_i) : i \in I\}$ be the relation on T determined by the identities. Then $FA_{\mathcal{S}}(X) \cong T/\langle H \rangle$.*

Proof. As T itself is a free algebra on X, there is a map $\alpha : X \to T$ where $n\alpha = n$ for all $n \in X$. Suppose $\theta : X \to S$, where S is an algebra of signature $\mathcal{S}$ and S

satisfies the identities. Then there is a morphism $\phi : T \to S$ such that $\alpha\phi = \theta$.

Now for any $(l_i, r_i) \in H$, $l_i\phi = r_i\phi$ as S satisfies the identities. So $H \subseteq \ker\phi$, and so as $\langle H\rangle$ is the smallest congruence containing H, $\langle H\rangle \subseteq \ker\phi$. So by Proposition 1.7.12 we can define $\bar{\phi} : T/\langle H\rangle \to S$ by $[u]\bar{\phi} = u\phi$. We now have $\bar{\alpha}\bar{\phi} = \theta$, where $\bar{\alpha} : X \to T/\langle H\rangle$ is given by $n\bar{\alpha} = [n]$. Hence $T/\langle H\rangle$ is a free algebra determined by the identities. Since such free algebra is unique up to isomorphism, $FA_{\mathcal{S}}(X) \cong T/\langle H\rangle$. Notice also that $T/\langle H\rangle$ satisfies all the identities $l_i = r_i, i \in I$. $\square$

The above is a general result for varieties, below there are a few observations, which are special cases.

For example, as we have seen, you can consider a unary monoid as a monoid with an additional unary operation $^+$. It has a signature $\mathcal{S} = (2, 1, 0)$. The free unary monoid on X is a unary monoid $\mathrm{FU}(X)$ together with a map $\alpha : X \to \mathrm{FU}(X)$ with the property that, for every unary monoid U and every map $\theta : X \to U$, there is a unique morphism $\phi : \mathrm{FU}(X) \to U$ such that $\alpha\phi = \theta$. We will get the free unary monoid by taking the free term algebra $FT_{\mathcal{S}}(X)$ and factoring by the congruence generated by

$$\{((s \cdot t) \cdot u, s \cdot (t \cdot u)), (1 \cdot s, s), (s \cdot 1, s) : s, t, u \in FT_{\mathcal{S}}(X)\}.$$

According to [16], a semigroup is left restriction if and only if it satisfies

$$x^+x = x, x^+y^+ = y^+x^+, (x^+y)^+ = x^+y^+, xy^+ = (xy)^+x.$$

On the other hand, for any set X, the free left restriction monoid and the free left ample monoid coincide. Thus we can get the free left ample monoid $\mathrm{FLA}(X)$ by factoring $FT_{\mathcal{S}}(X)$ by the congruence generated by

$$\{((s \cdot t) \cdot u, s \cdot (t \cdot u)), (1 \cdot s, s), (s \cdot 1, s),$$

$$(s^+s, s), (s^+t^+, t^+s^+), ((s^+t)^+, s^+t^+), (st^+, (st)^+s) : s, t, u \in FT_{\mathcal{S}}(X)\}.$$

We give a structure theorem for $\mathrm{FLA}(X)$ in Chapter 1.

Further, factoring $FT_{\mathcal{S}}(X)$ by the congruence generated by

$$\{((s \cdot t) \cdot u, s \cdot (t \cdot u)), (1 \cdot s, s), (s \cdot 1, s), (s^+, 1) : s, t, u \in FT_{\mathcal{S}}(X)\}$$

will yield a monoid with an additional unary operation that is constant with its image at the monoid identity. That is, the free monoid X^*, but in an augmented signature.

Given a set X, let $\mathrm{FU}(X)$, $\mathrm{FLE}(X)$, and $\mathrm{FLA}(X)$ be the free unary monoid, free left Ehresmann monoid, and free left ample monoid on X respectively. Also now we assume M be a left ample monoid generated by X. If we regard X as a subset of

FU(X), FLE(X), FLA(X) and M, then we naturally obtain unary monoid morphism $\theta : \mathrm{FU}(X) \to \mathrm{FLE}(X)$, $\varphi : \mathrm{FLE}(X) \to \mathrm{FLA}(X)$, and $\psi : \mathrm{FLA}(X) \to M$. Moreover, each of these morphisms is onto. If both **A** and **B** are left Ehresmann monoid, take **A** to be FLE(X), and **B** to be FLA(X) as an example, we can show, as an illustration of Theorem 3.0.7:

EXAMPLE 3.0.10. Let $L \subseteq \mathrm{FLA}(X)$. Then

$$L \in \mathrm{Rec}\,\mathrm{FLA}(X) \Leftrightarrow L\varphi^{-1} \in \mathrm{Rec}\,\mathrm{FLE}(X).$$

Proof. We use the description of $\sim_L$ given in Section 2.2. Suppose $u, v \in \mathrm{FLE}(X)$ are such that $u \sim_{L\varphi^{-1}} v$. As φ is surjective, for all $a', b', c', d' \in \mathrm{FLA}(X)$, there exist $a, b, c, d \in \mathrm{FLE}(X)$, such that $a' = a\varphi, b' = b\varphi, c' = c\varphi, d' = d\varphi$. We have

$$\begin{aligned} a'(u\varphi)b' \in L &\Leftrightarrow a\varphi u\varphi b\varphi \in L \\ &\Leftrightarrow aub \in L\varphi^{-1} \\ &\Leftrightarrow avb \in L\varphi^{-1} \\ &\Leftrightarrow a\varphi v\varphi b\varphi \in L \\ &\Leftrightarrow a'(v\varphi)b' \in L. \end{aligned}$$

Furthermore,

$$\begin{aligned} a'(c'u\varphi d')^+b' \in L &\Leftrightarrow a\varphi(c\varphi u\varphi d\varphi)^+b\varphi \in L \\ &\Leftrightarrow a(cud)^+b \in L\varphi^{-1} \\ &\Leftrightarrow a(cvd)^+b \in L\varphi^{-1} \\ &\Leftrightarrow a\varphi(c\varphi v\varphi d\varphi)^+b\varphi \in L \\ &\Leftrightarrow a'(c'v\varphi d')^+b' \in L. \end{aligned}$$

So, $u\varphi \sim_L v\varphi$.

Similarly, if $u\varphi \sim_L v\varphi$, then for all $a, b, c, d \in \mathrm{FLE}(X)$,

$$\begin{aligned} aub \in L\varphi^{-1} &\Leftrightarrow a\varphi u\varphi b\varphi \in L \\ &\Leftrightarrow a\varphi v\varphi b\varphi \in L \\ &\Leftrightarrow avb \in L\varphi^{-1}, \end{aligned}$$

and also

$$\begin{aligned} a(cud)^+b \in L\varphi^{-1} &\Leftrightarrow a\varphi(c\varphi u\varphi d\varphi)^+b\varphi \in L \\ &\Leftrightarrow a\varphi(c\varphi v\varphi d\varphi)^+b\varphi \in L \\ &\Leftrightarrow a(cvd)^+b \in L\varphi^{-1}. \end{aligned}$$

This implies $u \sim_{L\varphi^{-1}} v$.

So we have established a one-one correspondence between $\mathrm{FLE}(X)/\sim_{L\varphi^{-1}}$ and $\mathrm{FLA}(X)/\sim_L$, thus $|\mathrm{FLE}(X)/\sim_{L\varphi^{-1}}|$ is finite if and only if $|\mathrm{FLA}(X)/\sim_L|$ is finite. □

The case for right Ehresmann monoid can be treated dually.

The previous theorems rely on the language in $\mathbf{A}$ to be the pre-image of a homomorphism. However, this is not always the case. Next we consider examples of $\mathbf{A}, \mathbf{B}$ and $\theta : \mathbf{A} \to \mathbf{B}$ and $K \subseteq A$ such that K is not a union of $\ker\theta$-classes.

Let $\mathrm{FLA}(X)$ be the free left ample monoid on X, and let X^* be the free monoid on X in the augmented signature. Let $\theta : \mathrm{FLA}(X) \to X^*$ be given by $(A, a)\theta = a$. Then θ is an onto morphism. If $L \subseteq X^*$, then $L\theta^{-1} \subseteq \mathrm{FLA}(X)$. If $(A, a) \in L\theta^{-1}$, we have $(A, a)\theta = a \in L$ and so $(B, a) \in L\theta^{-1}$ for any $(B, a) \in \mathrm{FLA}(X)$. Thus, for example, taking any $x \in X$ where we have the singleton $K = \{(\{1, x\}, x)\}$ would be such that $K \neq L\theta^{-1}$ for any subset L of X^*, since if $K = L\theta^{-1}$ we would have $\{(\{1, x, x^2\}, x)\} \in K$.

3.1 Example

Recall in Chapter 1.4 that every element $\underline{a} \in \mathrm{FIM}(X)$ can be written in the form of $\underline{a} = (A, a)$. In this form, $\mathrm{FLA}(X) = \{(A, a) \in \mathrm{FIM}(X) \mid a \in X^*, A \subseteq X^*\} = \{(A, a) \in \mathrm{FIM}(X) \mid A \subseteq X^*\}$ as $a \in A$ and $\mathrm{FA}(X) = \{(A, a) \in \mathrm{FIM}(X) \mid a \in X^*\}$.

EXAMPLE 3.1.1. If $\mathbf{A} = \mathrm{FU}(X), \mathrm{FLA}(X)$ or $\mathrm{FA}(X)$ and L is finite, then $L \in \mathrm{Rec}\,\mathbf{A}$.

Proof. By Theorem 2.1.7, for any $u, v \in \mathbf{A}$ we have $u \sim_L v$ if and only if for any unary term function $t(x)$

$$t(u) \in L \Leftrightarrow t(v) \in L.$$

If $\mathbf{A} = \mathrm{FU}(X)$, for each $w \in L$, there can only be finitely many $u \in \mathbf{A}$ such that $t(u) = w$, where $t(x)$ is a unary term function. This follows since the expression of an element in $\mathrm{FU}(X)$ is unique except for the position of brackets. Since L is finite, there can only be finitely many $u \in A$ such that for some unary term function $t(x)$, we have $t(u) \in L$.

From the proof of Lemma 2.3.13, we have that if L is finite, then

$$K_L = \{w \in \mathrm{FA}(X) : t(w) \in L \text{ for some unary term function } t(x)\}$$

is finite. Clearly this will also hold for $\mathrm{FLA}(X)$.

So in all cases, there are finitely many $u \in A$ such that $t(u) \in L$. All others $u \in A$ with $t(u) \notin L$ for any term t must lie in a single $\sim_L$-class. As a result, there can only be a finite number of $\sim_L$-classes and thus $L \in \mathrm{Rec}\,\mathbf{A}$. $\square$

3.2 Closure properties of recognizable languages

In this section we consider closure properties of $\mathrm{Rec}\,\mathbf{A}$. We begin with Boolean operations.

Proposition 3.2.1. *Let* $\mathbf{A}$ *be a universal algebra and* $L \subseteq A$ *be a language in* $\mathbf{A}$. *Then* $L \in \operatorname{Rec}\mathbf{A}$ *implies that* $L^c = A \setminus L \in \operatorname{Rec}\mathbf{A}$.

Proof. If $L \in \operatorname{Rec}\mathbf{A}$, then $\mathbf{A}/\sim_L$ is finite. Let $\phi : \mathbf{A} \to \mathbf{A}/\sim_L$ be the quotient map from $\mathbf{A}$ onto $\mathbf{A}/\sim_L$, defined by $w\phi = [w]$ where $[w]$ is the $\sim_L$ congruence class of w.

Note that by the definition of syntactic congruence, L is a union of $\sim_L$-classes. Hence $L^c = A \setminus L$ is also a union of $\sim_L$-classes.

As $\sim_{L^c}$ is the largest congruence such that L^c is a union of congruence classes, we have $\sim_L \subseteq \sim_{L^c}$. However, as $L = (L^c)^c$, by substituting L by L^c, we see that $\sim_{L^c} \subseteq \sim_{(L^c)^c} = \sim_L$. Hence $\sim_L = \sim_{L^c}$ and therefore $\mathbf{A}/\sim_{L^c}$ is finite. □

EXAMPLE 3.2.2. Let $\mathbf{A}$ be an algebra.

1. $A \in \operatorname{Rec}\mathbf{A}$ as $A \times A$ is the largest congruence in $\mathbf{A}$ with A as the only congruence class. Then $\sim_A = A \times A$ and $\mathbf{A}/\sim_A$ is singleton.

2. $\phi \in \operatorname{Rec}\mathbf{A}$ as $\phi = A^c$.

Lemma 3.2.3. *If* ρ *and* σ *are two congruences on* $\mathbf{A}$, *then* $|\mathbf{A}/(\rho \cap \sigma)| \leq |\mathbf{A}/\rho| \cdot |\mathbf{A}/\sigma|$.

Proof. Note that the intersection of two congruence is a congruence. Define a mapping $g : \mathbf{A}/(\rho \cap \sigma) \to \mathbf{A}/\rho \times \mathbf{A}/\sigma$ by $a(\rho \cap \sigma) \mapsto (a\rho, a\sigma)$ for all $a \in A$.
Then g is well-defined and one-one as

$$\begin{aligned} a(\rho \cap \sigma) = b(\rho \cap \sigma) &\Leftrightarrow a\ (\rho \cap \sigma)\ b \\ &\Leftrightarrow a\ \rho\ b \quad \text{and} \quad a\ \sigma\ b \\ &\Leftrightarrow (a\rho, a\sigma) = (b\rho, b\sigma). \end{aligned}$$

To show that g is a morphism, we have

$$\begin{aligned} &(a(\rho \cap \sigma) b(\rho \cap \sigma))g \\ &= (ab(\rho \cap \sigma))g \\ &= ((ab)\rho, (ab)\sigma) \\ &= (a\rho, a\sigma)(b\rho, b\sigma) \\ &= (a(\rho \cap \sigma))g(b(\rho \cap \sigma))g. \end{aligned}$$

To show that g is a morphism, let F be an arbitary basic operation in $\mathbf{A}$ with rank n. Then F induces operations of the same rank in $\mathbf{A}/(\rho \cap \sigma)$, $\mathbf{A}/\rho$ and $\mathbf{A}/\sigma$.

Now let $a_1, \dots, a_n \in A$. We have

$$\begin{aligned}
&(F(a_1(\rho \cap \sigma), \dots, a_n(\rho \cap \sigma)))g \\
&= ((F(a_1, \dots, a_n))(\rho \cap \sigma))g \\
&= ((F(a_1, \dots, a_n))\rho, (F(a_1, \dots, a_n))\sigma) \\
&= (F(a_1\rho, \dots, a_n\rho), F(a_1\sigma, \dots, a_n\sigma)) \\
&= F((a_1\rho, a_1\sigma), \dots, (a_n\rho, a_n\sigma)) \\
&= F((a_1(\rho \cap \sigma))g, \dots, (a_n(\rho \cap \sigma))g).
\end{aligned}$$

Then $|\mathbf{A}/(\rho \cap \sigma)| \leq |\mathbf{A}/\rho \times \mathbf{A}/\sigma| = |\mathbf{A}/\rho| \cdot |\mathbf{A}/\sigma|$, with equality if g is onto. □

Proposition 3.2.4. *If $L, K \in \operatorname{Rec} \mathbf{A}$ then $L \cap K \in \operatorname{Rec} \mathbf{A}$.*

Proof. As $\sim_L$ and $\sim_K$ are congruences, so is $\sim_L \cap \sim_K$. If $a\ (\sim_L \cap \sim_K)\ b$, then $a \sim_L b$ and $a \sim_K b$. If $a \in L \cap K$, then $a \in L$ and $a \in K$. As L and K are unions of their respective syntactic congruence classes, $b \in L$ and $b \in K$, and hence $b \in L \cap K$. This means that $L \cap K$ is a union of congruence classes of $\sim_L \cap \sim_K$, in other words, $\sim_L \cap \sim_K \in \mathcal{C}_{L \cap K}$. So $\sim_L \cap \sim_K \subseteq \sim_{L \cap K}$.

Now if $L, K \in \operatorname{Rec} \mathbf{A}$, then both $\sim_L$ and $\sim_K$ have finite index. By Lemma 3.2.3, $\sim_L \cap \sim_K$ has finite index. Therefore $\sim_{L \cap K}$ has finite index, and $L \cap K \in \operatorname{Rec} \mathbf{A}$. □

Corollary 3.2.5. *If $L_1, L_2, \dots L_m \in \operatorname{Rec} \mathbf{A}$, then $L_1 \cap L_2 \cap \dots \cap L_m \in \operatorname{Rec} \mathbf{A}$.*

Proof. Proposition 3.2.4 and induction. □

Corollary 3.2.6. *If $L, K \in \operatorname{Rec} \mathbf{A}$, then $L \cup K \in \operatorname{Rec} \mathbf{A}$.*

Proof. We have $L \cup K = (L^c \cap K^c)^c$; hence result by Propositions 3.2.1 and 3.2.4. □

Corollary 3.2.7. *If $L_1, L_2, \dots L_m \in \operatorname{Rec} \mathbf{A}$ then $L_1 \cup L_2 \cup \dots \cup L_m \in \operatorname{Rec} \mathbf{A}$.*

Proof. Proposition 3.2.6 and induction. □

Corollary 3.2.8. *If $L, K \in \operatorname{Rec} \mathbf{A}$ then $L \setminus K \in \operatorname{Rec} \mathbf{A}$.*

Proof. We have $L \setminus K = L \cap K^c$; hence result by Proposition 3.2.1 and 3.2.4. □

The final result in this section is more special, and deals with languages over $\mathrm{FU}(\Sigma)$ for some alphabet Σ.

Proposition 3.2.9. *Let $L, K \in \operatorname{Rec} \mathrm{FU}(\Sigma)$. Then $LK \in \operatorname{Rec} \mathrm{FU}(\Sigma)$*

Proof. Recall the Schützenberger Product in Chapter 1.6. If M, N are unary monoids, define a unary operation $^+$ in $M \diamond N$ by

$$\begin{pmatrix} m & P \\ 0 & n \end{pmatrix}^+ = \begin{pmatrix} m^+ & \{(m^+, 1), (1, n^+)\} \\ 0 & n^+ \end{pmatrix},$$

which turns $M \diamond N$ into a unary monoid. On the other hand, if $\varphi_1 : \mathrm{FU}(\Sigma) \to M$ is a morphism such that $L = (L\varphi_1)\varphi_1^{-1}$, and $\varphi_2 : \mathrm{FU}(\Sigma) \to N$ is a morphism such that $K = (K\varphi_2)\varphi_2^{-1}$, we define

$$\Omega(w) = \{(w_1\varphi_1, w_2\varphi_2) \mid (w_1, w_2) \in \mathrm{FU}(\Sigma), w_1w_2 = w\}.$$

Since $v^+ \in \mathrm{FU}(\Sigma)$ can only be written as a product v^+1 or $1v^+$, we have then $\Omega(v^+) = \{(v^+\varphi_1, 1), (1, v^+\varphi_2)\}$ for any $v \in \mathrm{FU}(\Sigma)$. So

$$(v^+)\varphi = \begin{pmatrix} v^+\varphi_1 & \Omega(v^+) \\ 0 & v^+\varphi_2 \end{pmatrix} = \begin{pmatrix} v^+\varphi_1 & \{(v^+\varphi_1, 1), (1, v^+\varphi_2)\} \\ 0 & v^+\varphi_2 \end{pmatrix} = (v\varphi)^+.$$

Together with Lemma 1.6.3, φ is a unary monoid homomorphism. The rest of the proof is just an analogy of Theorem 1.6.4. $\square$

3.3 Recognizable languages in $\mathrm{FLA}(X)$ and $\mathrm{FIM}(X)$

We begin this section by noting that although $\mathrm{FLA}(X)$ and $\mathrm{FIM}(X)$ are algebras of the same signature, their unary operations are different. The underlying universes as sets which have the relation that $\mathrm{FLA}(X) \subseteq \mathrm{FIM}(X)$, and thus it makes sense to consider languages as a subset of both $\mathrm{FLA}(X)$ and $\mathrm{FIM}(X)$ and study their properties as languages sitting inside both structures.

Theorem 3.3.1. *Let $L \subseteq \mathrm{FLA}(X) \subseteq \mathrm{FIM}(X)$. Then $L \in \mathrm{Rec}\,\mathrm{FIM}(X)$ implies that $L \in \mathrm{Rec}\,\mathrm{FLA}(X)$*

Proof. Suppose we have $\sim_L \subseteq \mathrm{FLA}(X) \times \mathrm{FLA}(X)$ and $\sim'_L \subseteq \mathrm{FIM}(X)^2$ ($\mathrm{FIM}(X)^2$ means $\mathrm{FIM}(X) \times \mathrm{FIM}(X)$) as the syntactic congruence of L in $\mathrm{FLA}(X)$ and $\mathrm{FIM}(X)$ respectively. We now consider $\sim'_L \cap \mathrm{FLA}(X)^2$. Suppose $u, v \in \mathrm{FLA}(X)$ are such that $u \sim'_L v$. By Theorem 2.2.5, the syntactic congruence $\sim'_L$ on $\mathrm{FIM}(X)$ can be treated as a special case of left Ehresmann monoid syntactic congruence. As $\mathrm{FLA}(X)^2$ is a congruence in $\mathrm{FLA}(X)$, $\sim'_L \cap \mathrm{FLA}(X)^2$ is also a congruence in $\mathrm{FLA}(X)$. Also as $u \sim'_L v$, we have for all $x, y, s, t \in \mathrm{FIM}(X)$,

$$xuy \in L \quad \Leftrightarrow \quad xvy \in L \tag{3.7}$$

$$x(sut)^+y \in L \quad \Leftrightarrow \quad x(svt)^+y \in L. \tag{3.8}$$

As $\mathrm{FLA}(X) \subseteq \mathrm{FIM}(X)$, we have Equation (3.7) and (3.8) holds for all x, y, s, t in $\mathrm{FLA}(X)$. As a result, $u \sim_L v$. Therefore, $\sim'_L \cap \mathrm{FLA}(X)^2 \subseteq \sim_L$.

Now if $L \in \mathrm{Rec}\,\mathrm{FIM}(X)$, then $\sim'_L$ has finite index. On the other hand, $\sim'_L \cap\ \mathrm{FLA}(X)^2$ is the restriction of $\sim'_L$ in $\mathrm{FLA}(X)$, so the number of congruence class of $\sim'_L$ $\cap\ \mathrm{FLA}(X)^2$ is less than or equal to that of $\sim'_L$, and hence finite. Finally, since

$\sim'_L \cap \mathrm{FLA}(X)^2 \subseteq \sim_L$, it follows that $\sim_L$ also has finite index and thus L is in $\mathrm{Rec}\,\mathrm{FLA}(X)$. $\square$

In the proof of the above theorem, we have established that $\sim'_L \cap \mathrm{FLA}(X)^2 \subseteq \sim_L$, where $\sim_L$ and $\sim'_L$ are the syntactic congruence of L in $\mathrm{FLA}(X)$ and $\mathrm{FIM}(X)$ respectively. In general we do not have equality. In particular, Chapter 5 show us what $\sim_L$ and $\sim'_L$ like when $L = \mathrm{FLA}(X)$.

Chapter 4

Finite state automata accepting languages in free unary monoids

In this chapter, we focus our attention on languages over unary monoids. We investigate the relationship between recognizable languages in the sense of Chapter 3 and languages recognised by finite state automata. We need to first develop a notion of a finite state automata reading elements of the free unary monoid.

Recall in Chapter 3 that the free unary monoid can be obtained from the free term algebra with signature (2,1,0) by factoring it with the congruence generated by relations according to the associative law and the fact 1 is a multiplicative identity.

4.1 +-automata

Let L be a language over a free unary monoid or a free left ample monoid or a finite set. We wish to relate recognisability of L in terms of syntactic congruences to recognisability using a version of a finite state automaton. We now introduce a new class of finite state automata that will provide this connection.

Let Σ be a finite set and let us define a +-automaton $\mathcal{A}^+$ to be a 6-tuple

$$\mathcal{A}^+ = (\Sigma, Q, \delta, q_0, F, P)$$

where

$$(\Sigma, Q, \delta, q_0, F)$$

is a DFA over Σ and $P : Q \times Q \to Q$. Please be reminded that all ingredients are finite.

Let $\mathrm{FT}_{\mathcal{S}}(\Sigma)$ be the free term algebra on Σ with signature $\mathcal{S} = (2, 1, 0)$. We know how the domain of δ is extended from $Q \times \Sigma$ to $Q \times \Sigma^*$. We now extend the domain of δ to $Q \times \mathrm{FT}_{\mathcal{S}}(\Sigma)$ inductively as follows:

1. $\delta(q, \epsilon) = q$;

2. $\delta(q, uv) = \delta(\delta(q, u), v)$;

3. $\delta(q, u^+) = P(q, \delta(q_0, u))$,

where $u, v \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$.

In other words, let $t_m = t_m(x_1, \ldots, x_n)$ be a term in $\mathrm{FT}_{\mathcal{S}}(\Sigma)$ formed by using m operations from $x_1, \ldots, x_n \in \Sigma$. If the m-th operation is multiplication, i.e. $t_m = uv$, we have $\delta(q, t_m) = \delta(q, uv) = \delta(\delta(q, u), v)$. If the m-th operation is the unary operation, i.e. $t_m = u^+$, we have $\delta(q, t_m) = \delta(q, u^+) = P(q, \delta(q_0, u))$. Thus by induction, and the note in Chapter 3 concerning uniqueness of expressions of elements in $\mathrm{FT}_{\mathcal{S}}(X)$, we have uniquely defined $\delta(q, t)$ for any term $t \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$.

It is important to note that in the above definition, we actually want to use $\mathrm{FU}(\Sigma)$ in replacement of $\mathrm{FT}_{\mathcal{S}}(\Sigma)$. In $\mathrm{FU}(\Sigma)$, any multiplication of any element u with the identity ϵ give rise to itself, that is, $u\epsilon = \epsilon u = u$. Also we have the associative law. These are not present in $\mathrm{FT}_{\mathcal{S}}(\Sigma)$. So we have to show that these are preserved in the above definition.

Lemma 4.1.1. *According to the above definition, for all $q \in Q$ and $u, v, w \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$:*

1. $\delta(q, u\epsilon) = \delta(q, \epsilon u) = \delta(q, u)$;

2. $\delta(q, (uv)w) = \delta(q, u(vw)) = \delta(\delta(\delta(q, u), v), w)$.

Proof. 1. According to the definition,

$$\delta(q, u\epsilon) = \delta(\delta(q, u), \epsilon) = \delta(q, u).$$

Similarly,

$$\delta(q, \epsilon u) = \delta(\delta(q, \epsilon), u) = \delta(q, u).$$

2. According to the definition,

$$\delta(q, (uv)w) = \delta(\delta(q, uv), w) = \delta(\delta(\delta(q, u), v), w).$$

Similarly,

$$\delta(q, u(vw)) = \delta(\delta(q, u), vw) = \delta(\delta(\delta(q, u), v), w).$$

□

On $\mathcal{T}_Q$, the full transformation monoid on Q, we now define a unary operation. For any $\alpha \in \mathcal{T}_Q$, we define α^+ by

$$q\alpha^+ = P(q, q_0\alpha).$$

For each $u \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$, we define σ_u by

$$q\sigma_u = \delta(q, u),$$

so that $\sigma_u \in \mathcal{T}_Q$.

Now $\delta : Q \times \mathrm{FT}_{\mathcal{S}}(\Sigma) \to Q$ gives us a map $\theta : \mathrm{FT}_{\mathcal{S}}(\Sigma) \to \mathcal{T}_Q$ given by $w\theta = \sigma_w$. So for all $q \in Q$, $q(w\theta) = q\sigma_w = \delta(q, w)$.

Lemma 4.1.2. *The above defined θ is a morphism.*

Proof. For any $q \in Q, u, v \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$,

$$q((uv)\theta) = q\sigma_{uv} = \delta(q, uv) = \delta(\delta(q, u), v) = \delta(q\sigma_u, v) = (q\sigma_u)\sigma_v = q(\sigma_u\sigma_v) = u\theta v\theta.$$

Also,

$$q(u^+\theta) = q\sigma_{u^+} = \delta(q, u^+) = P(q, \delta(q_0, u)) = P(q, q_0\sigma_u) = q\sigma_u^+ = q(u\theta)^+.$$

□

Proposition 4.1.3. *For all $u, v, w \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$, $((uv)w)\theta = (u(vw))\theta$.*

Proof. On the L.H.S.,

$$((uv)w)\theta = \delta(q, (uv)w) = \delta(\delta(q, uv), w) = \delta(\delta(\delta(q, u), v), w).$$

On the R.H.S.,

$$(u(vw))\theta = \delta(q, u(vw)) = \delta(\delta(q, u), vw) = \delta(\delta(\delta(q, u), v), w).$$

□

Proposition 4.1.4. *For all $u \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$, $(u\epsilon)\theta = (\epsilon u)\theta = u\theta$.*

Proof. We have

$$(u\epsilon)\theta = \delta(q, u\epsilon) = \delta(\delta(q, u), \epsilon) = \delta(q, u).$$

Similarly,

$$(\epsilon u)\theta = \delta(q, \epsilon u) = \delta(\delta(q, \epsilon), u) = \delta(q, u).$$

Also,

$$u\theta = \delta(q, u).$$

□

From Propositions 4.1.3 and 4.1.4, we know that $H = \{((uv)w, u(vw)), (u\epsilon, u), (\epsilon u, u)\}$ is contained in $\ker\theta$. As a result, by Proposition 1.7.12 we have a well-defined morphism

$$\bar{\theta} : \mathrm{FT}_{\mathcal{S}}(\Sigma)/\left< H \right> = \mathrm{FU}(\Sigma) \to \mathcal{T}_Q$$

by $[w]\bar{\theta} = w\theta$. We can also define

$$\delta(q,[w]) = q([w]\bar{\theta}) = q(w\theta).$$

In other words, as the free unary monoid can be obtained from the free term algebra with signature (2,1,0) by factoring it with the congruence generated according to the associative law and identity multiplication, we have:

Corollary 4.1.5. *If $w, w' \in \mathrm{FT}_{\mathcal{S}}(\Sigma)$ are such that $[w] = [w']$ in $\mathrm{FU}(\Sigma)$, then $\delta(q,w) = \delta(q,w')$ for all $q \in Q$.*

Usually in $\mathrm{FU}(\Sigma)$, we write θ instead of $\bar{\theta}$ and w instead of $[w]$.

So, summarising, we can define δ with domain of $Q \times \mathrm{FU}(\Sigma)$ as follows:

1. $\delta(q,\epsilon) = q$;
2. $\delta(q,uv) = \delta(\delta(q,u),v)$;
3. $\delta(q,u^+) = P(q,\delta(q_0,u))$,

where $u, v \in \mathrm{FU}(\Sigma)$.

We can also defined $\theta : \mathrm{FU}(\Sigma) \to \mathcal{T}_Q$ as: for all $q \in Q$, $q(w\theta) = q\sigma_w = \delta(q,w)$.

We remind the reader that the unary operation $+$ in $\mathcal{T}_Q$ is not the standard one. You need to define $L(\mathcal{A}^+)$ as

$$L(\mathcal{A}^+) = \{w \in \mathrm{FU}(\Sigma) : \delta(q_0,w) \in F\}.$$

Theorem 4.1.6. *Let $L \subseteq \mathrm{FU}(\Sigma)$. Then L is recognised by a finite unary monoid if and only if $L = L(\mathcal{A}^+)$ for a $+$-automaton $\mathcal{A}^+$.*

Proof. Suppose that $L = L(\mathcal{A}^+)$.

We have $L \subseteq L\theta\theta^{-1}$, and for any $w \in L\theta\theta^{-1}$ we have $w\theta = v\theta$ for some $v \in L = L(\mathcal{A}^+)$. We have

$$\delta(q_0,w) = q_0(w\theta) = q_0(v\theta) = \delta(q_0,v) \in F$$

so that $w \in L(\mathcal{A}^+) = L$. Thus $L = L\theta\theta^{-1}$. Since $\mathcal{T}_Q$ is finite we have that $L \in \mathrm{Rec}\,\mathrm{FU}(\Sigma)$.

Conversely, suppose that N is a finite unary monoid and $\phi : \mathrm{FU}(\Sigma) \to N$ is a unary monoid morphism such that $L = L\phi\phi^{-1}$. Let

$$\mathcal{A}^+ = (\Sigma, N, \delta, 1, L\phi, P)$$

where for any $x \in \Sigma$ we have

$$\delta(q,x) = q(x\phi), \text{ and } P(q,p) = qp^+.$$

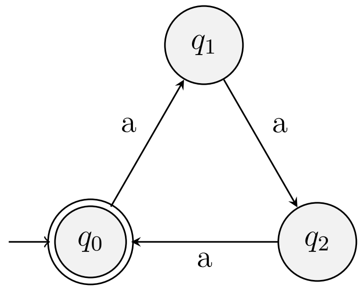

Figure 4.1: +-automata example

We show by induction that $\delta(q, w) = q(w\phi)$ for all $w \in \mathrm{FU}(\Sigma)$. This is true for $w = x \in \Sigma$. Proceeding by induction for $t = uv \in \mathrm{FU}(\Sigma)$,

$$\delta(q, t) = \delta(\delta(q, u), v) = \delta(q(u\phi), v) = (q(u\phi))v\phi = q(t\phi),$$

and for $t = u^+ \in \mathrm{FU}(\Sigma)$,

$$\delta(q, t) = \delta(q, u^+) = P(q, \delta(1, u)) = P(q, 1(u\phi)) = q(u\phi)^+ = q(t\phi).$$

So by induction on the complexity of t, we have $\delta(q, t) = q(t\phi)$.

We then have that

$$w \in L(\mathcal{A}^+) \Leftrightarrow \delta(q_0, w) \in L\phi \Leftrightarrow 1(w\phi) \in L\phi \Leftrightarrow w \in L\phi\phi^{-1} = L.$$

$\square$

Figures 4.1 4.2 give us the information to define a +-automaton.

Here $\Sigma = \{a\}$. Note that the multiplication table is left zero. That is, for any $q, p \in \mathrm{FU}(\Sigma)$, $P(q, p) = q$. So for any $u \in \mathrm{FU}(\Sigma)$, $\delta(q, u^+) = P(q, \delta(q_0, u)) = q$. As a result, for any term such that the last operation is the unary operation, $+$, does not change the node inside the automata. For example, if $u, v, w, x, y \in \mathrm{FU}(\Sigma)$, $\delta(q, u(vw^+)^+xy^+) = \delta(\delta(\delta(\delta(q, u), (vw^+)^+), x), y^+) = \delta(\delta(q, u), x) = \delta(q, ux)$. Thus the expression can be reduced so that all the terms with unary operation are eliminated and it can be treated as an ordinary automaton. From the figure, we see that starting from q_0, the automaton would return to the accepting state whenever 3 a's have been inputted into it. As a result, the automaton accepts

$$(t_0(a))^+a^{p_1}(t_1(a))^+a^{p_2}(t_2(a))^+ \cdots a^{p_n}(t_n(a))^+,$$

where for $0 \leq i \leq n$, $t_i(a)$ is a term function, and $\Sigma_{i=0}^{n} p_i = 3k$, where $k \in \mathbb{N}^0$.

	P	p: q_0	q_1	q_2
	q_0	q_0	q_0	q_0
q	q_1	q_1	q_1	q_1
	q_2	q_2	q_2	q_2

Figure 4.2: multiplication table for P

4.2 Automata - NDAs

In the theory of automata over free monoids, it is well known that deterministic automata may be replaced by non-deterministic ones. Here we show the same is true for +-automata.

Definition 4.2.1. An *NDA* +-automaton $\mathcal{A}^+$ is a 6-tuple (Σ, Q, E, I, F, S) where

- Σ is a finite non-empty set, the alphabet;
- Q is a finite set of states;
- $E \subseteq Q \times \Sigma \times Q$;
- $I \subseteq Q$ is a set of initial states;
- $F \subseteq Q$ is a set of final states;
- $S \subseteq Q \times Q \times Q$.

From E we can define a function $\delta : Q \times \Sigma \to \mathcal{P}(Q)$, where $\mathcal{P}(Q)$ is the power set of Q and

$$\delta(q, x) = \{p \mid (q, x, p) \in E\},$$

and from S we can define a function $P : Q \times Q \to \mathcal{P}(Q)$, where

$$P(q, p) = \{r \mid (q, p, r) \in S\}.$$

Now we can extend the domain of the function δ from $Q \times \Sigma$ to $Q \times \mathrm{FU}(\Sigma)$ by induction on the term complexity. To start with, we define $\delta(q, \epsilon) = \{q\}$. Suppose we know $\delta(q, u)$ for all $q \in Q$ and u that are terms formed using $n-1$ or less operations. Now consider $\delta(q, w)$ where w is terms formed using n operations. If $w = uv$,

$$\delta(q, w) = \bigcup_{p \in \delta(q,u)} \delta(p, v);$$

whereas if $w = u^+$,

$$\delta(q, w) = \bigcup_{q_0 \in I,\, p \in \delta(q_0, u),\, q_0 \in I} P(q, p)$$

Definition 4.2.2. A word $w \in \mathrm{FU}(\Sigma)$ is *accepted* by an NDA $\mathcal{A}$ if

$$\delta(q_0, w) \cap F \neq \emptyset \text{ for some } q_0 \in I.$$

Definition 4.2.3. The *language recognised* by the NDA $\mathcal{A}$ is

$$L(\mathcal{A}) = \{w \in \mathrm{FU}(\Sigma) \mid w \text{ is accepted by } \mathcal{A}\}.$$

Proposition 4.2.4. *Let $L \subseteq \mathrm{FU}(\Sigma)$. Then L is recognised by a $+$-automaton implies that L is recognised by a NDA $+$-automaton.*

Proof. Let $L = L(\mathcal{A})$ where $\mathcal{A} = (\Sigma, Q, \delta, q_0, F, P)$ is a $+$-automaton. Put

$$E = \{(q, a, \delta(q, a)) \mid q \in Q, a \in \Sigma\} \subseteq Q \times \Sigma \times Q,$$

$I = \{q_0\}$ and

$$S = \{(q, p, P(q, p)) \mid q, p \in Q\} \subseteq Q \times Q \times Q.$$

Now we have an NDA $+$-automaton

$$\mathcal{A}' = (\Sigma, Q, E, I, F, S).$$

Notice that the associated function δ' of this NDA has $\delta'(q_0, w)$ as a singleton for any $w \in \mathrm{FU}(\Sigma)$, corresponding to $\delta(q_0, w)$. Hence

$$\begin{aligned} w \in L(\mathcal{A}) &\Leftrightarrow \delta(q_0, w) \in F \\ &\Leftrightarrow \delta'(q_0, w) \cap F \neq \emptyset \\ &\Leftrightarrow w \in L(\mathcal{A}'). \end{aligned}$$

As a result, $L(\mathcal{A}) = L(\mathcal{A}')$. □

Notation. Let $\mathcal{A} = (\Sigma, Q, E, I, F, S)$ be an NDA. For $T \subseteq Q, w \in \mathrm{FU}(\Sigma)$, we define

$$\delta(T, w) = \{q \in Q \mid q \in \delta(p, w) \text{ for some } p \in T\},$$

also denoted by Tw. Note that $Tw \subseteq Q$, so there exists only finitely many sets of the form Tw. On the other hand, for $T_1, T_2 \subseteq Q$, we define

$$P(T_1, T_2) = \{q \in Q \mid q \in P(q_1, q_2) \text{ for some } q_1 \in T_1, q_2 \in T_2\}.$$

Note that $q \in P(T_1, T_2)$ if and only if $(q_1, q_2, q) \in S$ for some $q_1 \in T_1$, $q_2 \in T_2$.

Comments. For $T, T_1, T_2 \subseteq Q, a, a_1, \ldots, a_n \in \Sigma, w, u, v \in \mathrm{FU}(\Sigma)$ we have that

$$\begin{array}{rcl} Tw & = & \bigcup_{p \in T} \{p\} w \\ P(T_1, T_2) & = & \bigcup_{q_1 \in T_1, q_2 \in T_2} P(q_1, q_2) \\ T\varepsilon & = & T \\ Ta_1 a_2 \ldots a_n & = & (\ldots((Ta_1)a_2) \ldots a_n) \\ (Tw)v & = & Twv \\ (Tw)u^+ & = & P(Tw, \delta(I, u)) \\ \emptyset w & = & \emptyset. \end{array}$$

Proposition 4.2.5. *If $L = L(\mathcal{A})$ for an NDA +-automaton $\mathcal{A}$, then $L = L(\mathcal{A}')$ for a +-automaton $\mathcal{A}'$.*

Proof. Let $L = L(\mathcal{A})$ where

$$\mathcal{A} = (\Sigma, Q, E, I, F, S)$$

is a NDA +-automaton. Construct a +-automaton

$$\mathcal{A}' = (\Sigma, Q', \delta, q_0, F', P')$$

where

$$\begin{array}{rcl} Q' & = & \{Iw : w \in \mathrm{FU}(\Sigma)\} \\ \delta(T, a) & = & Ta \quad \text{for all } T \in Q', a \in \Sigma \\ q_0 & = & I \\ F' & = & \{T \in Q' : T \cap F \neq \emptyset\} \\ P'(T_1, T_2) & = & P(T_1, T_2) \quad \text{for all } T_1, T_2 \in Q'. \end{array}$$

Note that we have $Q' \subseteq \mathcal{P}(Q)$, the power set of Q, so $|Q'| < \infty$.
Also, for $T_1, T_2 \in Q'$, we have $T_1 = Iw_1$, $T_2 = Iw_2$ for some $w_1, w_2 \in \mathrm{FU}(\Sigma)$, so

$$P'(T_1, T_2) = P(Iw_1, Iw_2) = P(Iw_1, \delta(I, w_2)) = (Iw_1)w_2^+ = Iw_1 w_2^+ \in Q'.$$

For $T \in Q'$, $a \in \Sigma$ we have $T = Iw$ for some $w \in \mathrm{FU}(\Sigma)$, so

$$\delta(T, a) = \delta(Iw, a) = (Iw)a = Iwa \in Q'.$$

Furthermore, $q_0 = I = I\varepsilon \in Q'$. Finally we have that

$$\begin{array}{rcl} w \in L(\mathcal{A}') & \Leftrightarrow & \delta(q_0, w) \in F' \\ & \Leftrightarrow & \delta(I, w) \in F' \\ & \Leftrightarrow & Iw \in F' \\ & \Leftrightarrow & Iw \cap F \neq \emptyset \\ & \Leftrightarrow & w \in L(\mathcal{A}). \end{array}$$

$\square$

In conclusion, we have

Theorem 4.2.6. *Let $L \subseteq \mathrm{FU}(\Sigma)$ where Σ is finite. Then L is recognised by a $+$-automaton if and only if L is recognised by a NDA $+$-automaton.*

4.3 Example

This material comes from an analogy of [34, Section 2, P.350-352], in the setting of ample monoids.

From an algorithmic standpoint, recognisable languages are defined in terms of automata, and inverse automata are naturally related to $\mathrm{FIM}(X)$ through Munn trees and hence are a very handy tool for the study of inverse semigroup [29],[36].

The class of languages accepted by inverse automata is described as that of i-languages [34]. It is natural to ask if there is any analogy of inverse automata for unary monoids and what kind of languages they accept.

We refer the reader to [34] for the definition of inverse automata and i-languages. For the purposes of this section we will consider a third kind of $+$-automaton. Namely, we allow the functions δ and P in the definition of a $+$-automaton to be partial. We call such $+$-automata *partial* $+$-automata. By associating such a $+$-automaton with a NDA $+$-automaton, as in Proposition 4.2.4, we easily see that we have not changed the class of recognisable languages.

Suppose $\theta : \mathrm{FU}(X) \to \mathrm{FLA}(X)$ is the natural unary monoid morphism from $\mathrm{FU}(X)$ onto $\mathrm{FLA}(X)$, where we take X to be finite.

Definition 4.3.1. We say that a partial $+$-automaton $\mathcal{A}$ is *returning* if for all $u \in \mathrm{FU}(X)$, if $\delta(q, u)$ exists, then $\delta(q, u^+)$ exists and equals to q.

Given a language $L \subseteq \mathrm{FLA}(X)$, we say that L is *closed* if

$$\forall u \in L, \quad \forall v \in \mathrm{FLA}(X), \quad v \geq u \quad \Rightarrow \quad v \in L,$$

and we say that L is *elastic* if

$$\forall a, b \in L, \quad a^+b \in L.$$

In the following, we use the fact that θ is onto.

Theorem 4.3.2. *Suppose $L \subseteq \mathrm{FLA}(X)$ is a language whose $L\theta^{-1}$ is accepted by a returning $+$-automaton $\mathcal{A}$, i.e. $L\theta^{-1} = L(\mathcal{A})$, then L is closed and elastic.*

Proof. Let $u \in L$, $v \in \mathrm{FLA}(X)$ be such that $v \geq u$, so that $u = u^+v$ by definition of $\leq$. Now let $v' \in v\theta^{-1}$, and $u' \in u\theta^{-1}$. Then $(u'^+v')\theta = (u'\theta)^+v'\theta = u^+v = u \in$

L. Therefore, $u'^+v' \in L\theta^{-1}$, in other words, $\delta(q_0, u'^+v') \in F$. Now $u' \in u\theta^{-1} \subseteq L\theta^{-1} = L(\mathcal{A})$, so $\delta(q_0, u') \in F$ exists, thus $\delta(q_0, u'^+) = q_0$ also exists. Therefore $\delta(q_0, v') = \delta(\delta(q_0, u'^+), v') = \delta(q_0, u'^+v') \in F$ and hence $v' \in L(\mathcal{A}) = L\theta^{-1}$, thus $v \in L$. Therefore, L is closed.

On the other hand, suppose $a, b \in L$. Let $a' \in a\theta^{-1}$, and $b' \in b\theta^{-1}$. Then $a', b' \in L\theta^{-1} = L(\mathcal{A})$. So $\delta(q_0, a') \in F$ exists, and thus $\delta(q_0, a'^+) = q_0$. Therefore $\delta(q_0, b') = \delta(\delta(q_0, a'^+), b') = \delta(q_0, a'^+b')$, so $\delta(q_0, a'^+b')$ exists and is in F. So $a'^+b' \in L\theta^{-1}$ and $a^+b = (a'^+b')\theta \in L$. Therefore, L is elastic. $\square$

We believe the reverse of Theorem 4.3.2 is true, which we leave as a conjecture at this moment, but sketch how it may be proved.

To try to prove the reverse of Theorem 4.3.2, it seems that we need a minimal +-automaton. Starting with a partial +-automaton, we can replace it with a standard +-automaton by using a sink state, as follows.

Definition 4.3.3. Let $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ be a +-automaton. A *sink* state of $\mathcal{A}$ is a state s such that $s \notin F$ and for all $q \in Q, x \in \Sigma$ we have

$$\delta(s, x) = s = P(q, s) = P(s, q).$$

Sink state is unique in a +-automaton as we can see in the following:

Lemma 4.3.4. *Let s be a sink state of a +-automaton $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$. Then s is the only sink state, and for all $w \in \mathrm{FU}(\Sigma)$ we have $\delta(s, w) = s$.*

Proof. (Sketch) If s, s' are both sink states, then $s = P(s, s') = s'$. For the second statement, use induction on the complexity of w. $\square$

Then we may make a partial +-automaton into a total +-automaton with a sink state that accepts the same language:

Lemma 4.3.5. *Let $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ be a partial +-automaton. We make $\mathcal{A}$ into a +-automaton $\mathcal{A}'$ with set of states $Q' = Q \cup \{s\}$ a sink state s by extending the domain of δ to $\delta : Q' \times \Sigma \to Q'$ and P to $P' : Q' \to Q'$ by defining*

$$\delta'(q, x) = s = P'(r, p)$$

whenever $\delta(q, x)$ or $P(r, p)$ is not defined, and

$$\delta'(s, x) = s = P'(s, p) = P'(p, s) = P'(s, s)$$

for all $x \in \Sigma$ and $p \in Q$. Then $L(\mathcal{A}) = L(\mathcal{A}')$.

Lemma 4.3.6. *Let $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ be a +-automaton with sink state s. Then putting $Q' = Q \setminus \{s\}$ and restricting δ and P so that*

$$\delta' : Q' \to Q', P : Q' \times Q' \to Q',$$

so that δ' and P' are partial functions, we have that $\mathcal{A}' + (\Sigma, Q', \delta', P', q_0, F)$ is a +-automaton such that $L(\mathcal{A}) = L(\mathcal{A}')$.

The next task we need is to make a +-automaton trim.

Definition 4.3.7. Let $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ be a +-automaton. We define $R(q,p) \subseteq Q$ inductively as follows. We have $q, p \in R(q,p)$. If there is a word $w = uv \in \mathrm{FU}(\Sigma)$ such that $\delta(q,w) = p$ then $R(q, \delta(q,u)) \subseteq R(q,p)$ and $R(\delta(q,u), p) \subseteq R(q,p)$. If there is a word $w = u^+ \in \mathrm{FU}(\Sigma)$ such that $\delta(q,w) = p$ then $R(q, \delta(q,u)) \subseteq R(q,p)$.

Definition 4.3.8. Let $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ be a +-automaton with sink state s. We say that $\mathcal{A}$ is *tight* if $Q = \bigcup_{p \in F} R(q_0, p) \cup \{s\}$.

Conjecture 4.3.9. Let $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ be a +-automaton. Let $Q' = Q \setminus Z$ where Z is the set of states not occurring in $\bigcup_{p \in F} R(q_0, p)$. We then restrict δ to δ' and P to P' where

$$\delta' : Q' \times \mathrm{FU}(\Sigma) \to Q' \text{ and } P' : Q' \times Q' \to Q'$$

The resulting $\mathcal{A}'$ is then a partial +-automaton, and $L(\mathcal{A}') = L(\mathcal{A})$.

We then make $\mathcal{A}'$ into a total +-automaton $\mathcal{A}''$ with sink state s as above. Then $\mathcal{A}''$ is tight.

Definition 4.3.10. We say that a tight +-automaton $\mathcal{A} = (\Sigma, Q, \delta, P, q_0, F)$ with sink state s is *returning* if, whenever $\delta(q,w) \neq s$ we have $\delta(q, w^+) = q$.

Note in the above, if $\delta(q,w) \neq s$ then q must lie in some $R(q_0, p)$ for some $p \in F$.

We now need to find a notion of minimal automaton, that involves an equivalence on the set of states that is compatible with both δ and P. We put forward the following as a solution.

We define a relation $\sim$ on Q by the rule that

$$\sim = \cap_{i \geq 0} \sim_i$$

where

$$q \sim_0 q' \Leftrightarrow [q \in F \text{ iff } q' \in F]$$

and if $\sim_i$ has been defined then

$$q \sim_{i+1} q' \Leftrightarrow q \sim_i q' \text{ and}$$

$$\delta(q,w) \sim_i \delta(q',w),\ P(q,p) \sim_i P(q',p) \text{ and } P(p,q) \sim_i P(p,q')$$

for any $w \in \mathrm{FU}(\Sigma)$ and $p \in Q$.

It is clear that $\sim$ is an equivalence relation on Q, and denoting

$$\bar{Q} = \{[q] : q \in Q\}, \bar{F} = \{[q] : q \in F\}$$

and

$$\bar{\delta}([q], x) = [\delta(q, x)],\ \bar{P}([q], [p]) = [P(q, p)]$$

we have that $\bar{\delta}, \bar{P}$ are well defined and

$$\overline{\mathcal{A}} = (\Sigma, \bar{Q}, \bar{\delta}, \bar{P}, [q_0], \bar{F})$$

is a +-automaton such that $\sim$ is equality on $\bar{Q}$ and $L(\overline{\mathcal{A}}) = L(\mathcal{A})$. Moreover, if $\mathcal{A}$ is tight then so is $\overline{\mathcal{A}}$.

The proof that a closed elastic $L \subseteq FLA(\Sigma)$ is accepted by a returning automaton should now mirror that in the inverse case, but with many extra steps.

Conjecture 4.3.11. If $L \subseteq \mathrm{FLA}(X)$ is closed and elastic, then $L\theta^{-1} = L(\mathcal{A})$ for some returning +-automaton.

EXAMPLE 4.3.12. For example, $L = \{\epsilon, x, x^+\}$ for some $x \in X$.

$$\begin{aligned} u = \epsilon, \quad v \geq u \quad &\Rightarrow \quad v = \epsilon \in L, \\ u = x, \quad v \geq u \quad &\Rightarrow \quad v = x \in L, \\ u = x^+, \quad v \geq u \quad &\Rightarrow \quad v \in \{\epsilon, x^+\} \subseteq L, \end{aligned}$$

So L is closed. It is also easy to check L is elastic.

EXAMPLE 4.3.13. For example, $L = \{x, x^+\}$ for some $x \in X$. We see that

$$u = x^+, \quad v \geq u \quad \Rightarrow \quad v \in \{\epsilon, x^+\},$$

But $\epsilon \notin L$. So L is not closed. But it is still elastic.

If $L \subseteq \mathrm{FLA}(X)$, we would like to know what does $L\theta^{-1}$ looks like. For example:

EXAMPLE 4.3.14. Let $L = \{x^+\} \subseteq \mathrm{FLA}(X)$ for some $x \in X$. Then $L\theta^{-1}$ is a unary subsemigroup of $\mathrm{FU}(X)$, containing $\{x^+, (x^+)^+, x^+x^+, \ldots\}$.

This then gives us that:

EXAMPLE 4.3.15. Let $K = \{x^+\} \subseteq \mathrm{FU}(X)$, then $K \neq L\theta^{-1}$ for any $L \subseteq \mathrm{FLA}(X)$.

Chapter 5

Syntactic congruences of different languages

In this chapter, we discuss some examples of syntactic congruences of different languages inside $\mathrm{FIM}(X)$.

Recall that every element $\underline{a} \in \mathrm{FIM}(X)$ can be written as $\underline{a} = (A, a)$, where A is a finite, prefix closed subset of $\mathrm{FG}(X)$ and $a \in A$. We have

$$\mathrm{FLA}(X) = \{(A, a) \in \mathrm{FIM}(X) \mid a \in X^*, A \subseteq X^*\},$$

so as $a \in A$ we have

$$\mathrm{FLA}(X) = \{(A, a) \in \mathrm{FIM}(X) \mid A \subseteq X^*\}.$$

Further,

$$\mathrm{FA}(X) = \{(A, a) \in \mathrm{FIM}(X) \mid a \in X^*\}.$$

For example we have

$$\begin{aligned} \underline{a}^+ &= \underline{a}\,\underline{a}^{-1} \\ &= (A, a)(A, a)^{-1} \\ &= (A, a)(a^{-1}A, a^{-1}) \\ &= (A \cup aa^{-1}A, aa^{-1}) \\ &= (A, 1). \end{aligned}$$

Note that X^* can be embedded as a subset of $\mathrm{FIM}(X)$:

Proposition 5.0.1. *Let X^* be the free monoid of X. We have*

$$X^* \cong \{(a^{\downarrow}, a) \in \mathrm{FIM}(X) | a \in X^*\}.$$

Proof. Define a mapping $x \mapsto (x^{\downarrow}, x)$ for all $x \in X^*$. Then it is easy to check that the map is a monoid homomorphism.

For $x, y \in X^*$, $xy \mapsto ((xy)^{\downarrow}, xy) = (x^{\downarrow} \cup xy^{\downarrow}, xy) = (x^{\downarrow}, x)(y^{\downarrow}, y)$.

Further, $\epsilon \mapsto (\{\epsilon\}, \epsilon)$.

If $(x_1^{\downarrow}, x_1) = (x_2^{\downarrow}, x_2)$, then their 2nd co-ordinates, i.e., x_1 and x_2, are equal. Hence the map is an injection, which is clearly onto.

□

Identifying X^* with its image in $\mathrm{FLA}(X)$, as sets,

$$X^* \subseteq \mathrm{FLA}(X) \subseteq \mathrm{FA}(X) \subseteq \mathrm{FIM}(X),$$

but they are of algebras of different signatures. We have $\mathrm{FLA}(X)$ and $\mathrm{FIM}(X)$ are algebras of type (2,1,0), although their unary operations are different; $\mathrm{FA}(X)$ is an algebra of type (2,1,1,0); X^* is an algebra of type (2,0). Here we investigate the syntactic congruence of languages such as these that are themselves sitting inside a larger algebra. To make the things clearer, from now on we use $\sim_{L,A}$ instead of $\sim_L$ for the syntactic congruence of a language L in an algebra A.

First, if the language L is equal to A, the underlying universe of the algebra, then the universal relation, $A \times A$ is the certainly largest congruence, in which A is the only (and hence a union of) congruence class. So $\sim_{A,A} = A \times A = A^2$.

From Definition 2.2.1 we know that the syntactic congruence $\sim_{L,\mathrm{FLA}(X)}$ has to satisfy the condition that for all $u, v \in M, u \sim_L v$ if and only if for all $x, y, s, t \in M$:

1. $$xuy \in L \quad \Leftrightarrow \quad xvy \in L$$

   and

2. $$x(sut)^+y \in L \quad \Leftrightarrow \quad x(svt)^+y \in L$$

However, Theorem 2.2.5 implies that we need only 1. to determine the congruence $\sim_{L,\mathrm{FIM}(X)}$.

From Corollary 2.3.4 we know that $\sim_{L,\mathrm{FA}(X)}$ has to satisfy the condition that

for all $u, v \in M, u \sim_L v$ if and only if for all $l_0, l_1, \ldots, r_0, r_1, \cdots \in M$ and for all $n \in \mathbb{N}$:

1. $$t_0(u) \in L \quad \Leftrightarrow \quad t_0(v) \in L$$

   and

2. $$t_n^+(u) \in L \quad \Leftrightarrow \quad t_n^+(v) \in L$$

   $$t_n^*(u) \in L \quad \Leftrightarrow \quad t_n^*(v) \in L.$$

5.1 Syntactic Congruence of $\mathrm{FA}(X)$ in $\mathrm{FIM}(X)$

We first state the following lemma without proof.

Lemma 5.1.1. *If $a \in FG(X)$ such that $a, a^{-1} \in X^*$, then $a = \epsilon$.*

Now consider $\sim_{\mathrm{FA}(X),\mathrm{FIM}(X)}$.

Proposition 5.1.2. *For all $\underline{u}, \underline{v} \in \mathrm{FIM}(X)$, if $\underline{u} \sim_{\mathrm{FA}(X),\mathrm{FIM}(X)} \underline{v}$, then $\underline{v}\,\underline{u}^{-1}, \underline{u}\,\underline{v}^{-1} \in \mathrm{FA}(X)$.*

Proof. For all $\underline{u}, \underline{v} \in \mathrm{FIM}(X), \underline{u} \sim_{\mathrm{FA}(X),\mathrm{FIM}(X)} \underline{v}$ if and only if for all $\underline{x}, \underline{y} \in \mathrm{FIM}(X)$,

$$\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FA}(X) \quad \Leftrightarrow \quad \underline{x}\,\underline{v}\,\underline{y} \in \mathrm{FA}(X).$$

Now let $\underline{x} = 1$, and $\underline{y} = \underline{u}^{-1}$. We have

$$1\underline{u}\,\underline{u}^{-1} = \underline{u}^{+} \in \mathrm{FA}(X) \quad \Leftrightarrow \quad 1\underline{v}\,\underline{u}^{-1} = \underline{v}\,\underline{u}^{-1} \in \mathrm{FA}(X).$$

Since $1\underline{u}\,\underline{u}^{-1} = \underline{u}^{+} \in \mathrm{FA}(X)$ is true for all $\underline{u} \in \mathrm{FIM}(X)$, we must have $\underline{v}\,\underline{u}^{-1} \in \mathrm{FA}(X)$. Dually, $\underline{u}\,\underline{v}^{-1} \in \mathrm{FA}(X)$.

□

Theorem 5.1.3. *For all $\underline{u}, \underline{v} \in \mathrm{FIM}(X)$, $\underline{u} \sim_{\mathrm{FA}(X),\mathrm{FIM}(X)} \underline{v}$ if and only if $u = v$.*

Proof. Recall that $\mathrm{FA}(X) = \{(A, a) \in \mathrm{FIM}(X) \mid a \in X^*\}$. So, if $\underline{\mathrm{u}} \sim_{\mathrm{FA}(X),\mathrm{FIM}(X)} \underline{\mathrm{v}}$, we now have vu^{-1} and uv^{-1} in X^*. As $vu^{-1} = (uv^{-1})^{-1}$, by Lemma 5.1.1, $vu^{-1} = \epsilon$. This implies $u = v$. On the other hand, one can easily verify that if $u = v$, for all $\underline{x}, \underline{y} \in M$, $\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FA}(X) \quad \Leftrightarrow \quad xuy \in X^* \quad \Leftrightarrow \quad xvy \in X^* \quad \Leftrightarrow \quad \underline{x}\,\underline{v}\,\underline{y} \in \mathrm{FA}(X)$. □

In other words, $\underline{u} \sim_{\mathrm{FA}(X),\mathrm{FIM}(X)} \underline{v}$ if and only if their corresponding reduced word is the same. So,

Corollary 5.1.4. *For any alphabet X, we have $\mathrm{FIM}(X)/\sim_{\mathrm{FA}(X),\mathrm{FIM}(X)} \cong FG(X)$, and hence $\sim_{\mathrm{FA}(X),\mathrm{FIM}(X)}$ is the least group congruence on $\mathrm{FIM}(X)$.*

Proof. It is clear that $\sim_{\mathrm{FA}(X),\mathrm{FIM}(X)}$ is a group congruence. The fact it is the least group congruence σ follows from the description of σ in [21]. □

5.2 Syntactic Congruence of $\mathrm{FLA}(X)$ in $\mathrm{FIM}(X)$

Now consider $\sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)}$. Similar to the case where $L = \mathrm{FA}(X)$, we have

$$1\underline{u}\,\underline{u}^{-1} = \underline{u}^{+} \in \mathrm{FLA}(X) \quad \Leftrightarrow \quad 1\underline{v}\,\underline{u}^{-1} = \underline{v}\,\underline{u}^{-1} \in \mathrm{FLA}(X).$$

However, not all $\underline{u} \in \mathrm{FIM}(X)$ are such that $\underline{u}^{+} \in \mathrm{FLA}(X)$.

Recall that $\mathrm{FLA}(X) = \{(A, a) \in \mathrm{FIM}(X) | A \subseteq X^*\}$. As a result,

$$\underline{a}^+ \in \mathrm{FLA}(X) \Leftrightarrow A \subseteq X^* \Leftrightarrow \underline{a} \in \mathrm{FLA}(X).$$

Lemma 5.2.1. *If $\underline{u} \in \mathrm{FLA}(X)$, and $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$, then $u = v$.*

Proof. From the above, if $\underline{u} \in \mathrm{FLA}(X)$, then $\underline{u}^+ \in \mathrm{FLA}(X)$, and so if $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$, then $\underline{v}\,\underline{u}^{-1} \in \mathrm{FLA}(X)$. Since $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$ and $\mathrm{FLA}(X)$ is a union of $\sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)}$ classes, $\underline{v} \in \mathrm{FLA}(X)$. Dually we have $\underline{u}\,\underline{v}^{-1} \in \mathrm{FLA}(X)$. In this case vu^{-1} and uv^{-1} are both in X^* and this again implies $u = v$. $\square$

Define

$$H = \{\underline{u} \mid \text{there exists } \underline{x}, \underline{y} \in \mathrm{FIM}(X) \text{ s.t. } \underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FLA}(X)\} \subseteq \mathrm{FIM}(X).$$

It is the set of $\underline{u}$ in $\mathrm{FIM}(X)$ that has non-empty context with respect to $\mathrm{FLA}(X)$. Clearly,

Lemma 5.2.2. *For all $\underline{u}, \underline{v} \notin H$, $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$.*

Proof. For any $T \subseteq \mathrm{FIM}(X)$, and $\underline{u} \in \mathrm{FIM}(X)$,

$$C_T(\underline{u}) = \{(\underline{x}, \underline{y}) \in \mathrm{FIM}(X) \times \mathrm{FIM}(X) : \underline{x}\,\underline{u}\,\underline{y} \in T\}.$$

Then by our description of $\sim_{T,\mathrm{FIM}(X)}$, which we now denote as $\sim$,

$$\underline{u} \sim \underline{v} \quad \Leftrightarrow \quad C_T(\underline{u}) = C_T(\underline{v}).$$

So if $\underline{u}, \underline{v} \notin H$, $C_{FLA(X)}(\underline{u}) = C_{FLA(X)}(\underline{v}) = \emptyset$ and so $\underline{u} \sim \underline{v}$. $\square$

If $\underline{u} \in H$, then there exists $\underline{x}, \underline{y} \in \mathrm{FIM}(X)$ such that $\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FLA}(X)$.

Note that if we let $\underline{x} = (T, x)$, $\underline{u} = (U, u)$, $\underline{y} = (Y, y)$,

$$\begin{aligned} \underline{x}\,\underline{u}\,\underline{y} &= (T, x)(U, u)(Y, y) \\ &= (T \cup xU, xu)(Y, y) \\ &= (T \cup xU \cup xuY, xuy). \end{aligned}$$

Notice that $\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FLA}(X)$ if and only if $T \cup xU \cup xuY \subseteq X^*$. So if $\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FLA}(X)$, $T \cup xU \subseteq X^*$ which is equivalent to $\underline{x}\,\underline{u} \in \mathrm{FLA}(X)$. Hence

Lemma 5.2.3. *We have,*

$$H = \{\underline{u} \mid \exists \underline{x} \in \mathrm{FIM}(X) \text{ s.t. } \underline{x}\,\underline{u} \in \mathrm{FLA}(X)\}.$$

If $\underline{u} \in H$, and $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$, then $\underline{v} \in H$, and $u = v$.

Proof. From above, we have $H \subseteq \{\underline{u} \mid \exists \underline{x} \in \mathrm{FIM}(X)$ such that $\underline{x}\,\underline{u} \in \mathrm{FLA}(X)\}$. As we can let $\underline{y} = 1$, we actually have $\{\underline{u} \mid \exists \underline{x} \in \mathrm{FIM}(X)$ such that $\underline{x}\,\underline{u} \in \mathrm{FLA}(X)\} \subseteq H$ and hence the equality.

On the other hand, if $\underline{u} \in H$, and $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$, then there exists $\underline{x}, \underline{y} \in \mathrm{FIM}(X)$ such that $\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FLA}(X)$. So $\underline{x}\,\underline{v}\,\underline{y}$ is also in $\mathrm{FLA}(X)$ and hence $\underline{v} \in H$. In this case, as $\sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)}$ is a congruence, we know $\underline{x}\,\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{x}\,\underline{v}$. As both are in $\mathrm{FLA}(X)$, from the result before we can deduce that $xu = xv$, and thus $u = v$. □

On the other hand,

Proposition 5.2.4. *If $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$, then for all $g \in X^*$,*

$$U \subseteq g^{-1}X^* \Leftrightarrow V \subseteq g^{-1}X^*.$$

Proof. Let $\sim = \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)}$. If $\underline{u} \sim \underline{v}$, then for any $g \in X^*$,

$$\underline{g}\,\underline{u} \in \mathrm{FLA}(X) \quad \Leftrightarrow \quad \underline{g}\,\underline{v} \in \mathrm{FLA}(X)$$

Hence,

$$gU \subseteq X^* \quad \Leftrightarrow \quad gV \in X^*$$

and the result follows.

□

In summary, we have shown the first part of the following:

Theorem 5.2.5. *Let $H = \{\underline{u} \mid \exists \underline{x} \in \mathrm{FIM}(X)$ s.t. $\underline{x}\,\underline{u} \in \mathrm{FLA}(X)\}$. Then $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$ if and only if either*

1. $\underline{u}, \underline{v} \in \mathrm{FIM}(X) \setminus H$;

2. $\underline{u}, \underline{v} \in H$, $u = v$ *and for all* $g \in X^*$,

$$U \subseteq g^{-1}X^* \Leftrightarrow V \subseteq g^{-1}X^*.$$

Proof. We have proved the forward part, and the backward part for $\underline{u}, \underline{v} \in \mathrm{FIM}(X) \setminus H$.

Now let $\underline{u}$, $\underline{v} \in H$ such that $u = v$ and for all $g \in X^*$, $U \subseteq g^{-1}X^*$ if and only if $V \subseteq g^{-1}X^*$. Then $gU \subseteq X^*$ if and only if $gV \subseteq X^*$.

Now for all $\underline{x} = (T, x)$, $\underline{u} = (U, u)$, $\underline{v} = (V, v)$, and $\underline{y} = (Y, y) \in \mathrm{FIM}(X)$

$$
\begin{array}{rll}
& T \cup xU \cup xuY \subseteq X^* & \\
\Leftrightarrow & T \subseteq X^* \text{ and } xU \subseteq X^* \text{ and } xuY \subseteq X^* & \\
\Leftrightarrow & T \subseteq X^* \text{ and } xU \subseteq X^* \text{ and } xuY \subseteq X^* \text{ and } x \in X^* & \text{as } x \in T \\
\Leftrightarrow & T \subseteq X^* \text{ and } xV \subseteq X^* \text{ and } xuY \subseteq X^* \text{ and } x \in X^* & \\
\Leftrightarrow & T \subseteq X^* \text{ and } xV \subseteq X^* \text{ and } xvY \subseteq X^* \text{ and } x \in X^* & \text{as } u = v \\
\Leftrightarrow & T \subseteq X^* \text{ and } xV \subseteq X^* \text{ and } xvY \subseteq X^* & \text{as } x \in T \\
\Leftrightarrow & T \cup xV \cup xvY \subseteq X^*. &
\end{array}
$$

So $\underline{x}\,\underline{u}\,\underline{y} \in \mathrm{FLA}(X)$ if and only if $\underline{x}\,\underline{v}\,\underline{y} \in \mathrm{FLA}(X)$, i.e., $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$. ☐

Corollary 5.2.6. *Let $\underline{u}, \underline{v} \in \mathrm{FLA}(X)$. Then the following are equivalent:*

1. $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$;
2. $u = v$;
3. $\underline{u}\,\sigma\,\underline{v}$, *where σ is the minimum group congruence of* $\mathrm{FIM}(X)$.

Proof. (1)⇒(2) Direct implication of Theorem 5.2.5, as $\mathrm{FLA}(X) \subseteq H$.

(1)⇐(2) As both $\underline{u}$ and $\underline{v}$ are in $\mathrm{FLA}(X)$, $U, V \subseteq X^* = g^{-1}gX^* \subseteq g^{-1}X^*$ for all $g \in X^*$. So $U \subseteq g^{-1}X^*$ if and only if $V \subseteq g^{-1}X^*$ holds true, and by Theorem 5.2.5, we have $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$.

(2)⇔(3) Finally, it is well known [21, P.197] that $u = v$, if and only if $\underline{u}\,\sigma\,\underline{v}$. ☐

Now we would like to further investigate what H looks like and give a more explicit description of the relation $\underline{u} \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} \underline{v}$.

Lemma 5.2.7. *Let $H = \{\underline{u} \mid \exists \underline{x} \in \mathrm{FIM}(X)$ s.t. $\underline{x}\underline{u} \in \mathrm{FLA}(X)\}$. Then*

$$
\begin{array}{rcl}
H & = & \{\underline{u} = (U, u) \mid \exists x \in X^* \textit{ s.t. } (x^{\downarrow}, x)(U, u) \in \mathrm{FLA}(X)\} \\
& = & \{(U, u) \mid \exists x \in X^* \textit{ s.t. } U \subseteq x^{-1}X^*\}.
\end{array}
$$

Proof. From the above, we know that $H = \{\underline{u} \mid \exists \underline{x} \in \mathrm{FIM}(X) \text{ s.t. } \underline{x}\,\underline{u} \in \mathrm{FLA}(X)\}$ and $\underline{x}\,\underline{u} \in \mathrm{FLA}(X) \quad\Leftrightarrow\quad T \cup xU \subseteq X^*$. The latter implies $x \in X^*$ and $xU \subseteq X^*$. So we have shown that if there exists (T, x) such that $(T, x)(U, u) \in \mathrm{FLA}(X)$, then there exists x such that $xU \subseteq X^*$ and thus $U \subseteq x^{-1}X^*$.

Conversely, note that if $\exists\, x$ s.t. $xU \subseteq X^*$, then $x \in X^*$. Hence $x^{\downarrow} \cup xU \subseteq X^*$ and thus $(x^{\downarrow}, x)(U, u) \in \mathrm{FLA}(X)$. So $H = \{\underline{u} = (U, u) \mid \exists\, x \in X^* \text{ s.t. } (x^{\downarrow}, x)(U, u) \in \mathrm{FLA}(X)\} = \{(U, u) \mid \exists\, x \in X^* \text{ s.t. } U \subseteq x^{-1}X^*\}$, as desired. ☐

Let $x = x_1 \cdots x_n$, where $x_i \in X$, $i = 1, \ldots, n$. Then the elements of $x^{-1}X^*$ have the form $x_n^{-1} \cdots x_1^{-1}w$, where $w \in X^*$. So all reduced words in $x^{-1}X^*$ look like $x_n^{-1} \cdots x_i^{-1}v$, where $v \in X^*$, $1 \le i \le n$. As $U \subseteq x^{-1}X^*$, all the reduced words in U have the same form.

There is a good reason for it–we define an order on $(X^{-1})^*$ by the rule that for $x_1, x_2 \in X^*$,

$$x_1^{-1} \leq x_2^{-1} \text{ if and only if } (x_1^{-1})^{\downarrow} \supseteq (x_2^{-1})^{\downarrow}.$$

Theorem 5.2.8. *Let $H = \{(U, u) \mid \exists x \in X^* \text{ s.t. } U \subseteq x^{-1}X^*\}$. Then for any $(U, u) \in H$, there is a unique $x_u \in X^*$ such that $x_u^{-1} \in U$, and $U \subseteq x_u^{-1}X^*$, that is, all the reduced words in U have the form $x_n^{-1} \cdots x_i^{-1}v$, where $x_i \in X$, $i = 1, \ldots, n$, $x_u = x_1 \cdots x_n$, and $v \in X^*$.*

Proof. Let $(U, u) \in H$, and $x \in X^*$ be such that $U \subseteq x^{-1}X^*$. If $x = x'_1 \cdots x'_m$, then we know all the reduced words in U have the form $(x'_m)^{-1} \cdots (x'_j)^{-1}v$ for some $1 \leq j \leq m$, $v \in X^*$. Among all such reduced words there is a smallest j, say j_0, such that $(x'_m)^{-1} \cdots (x'_{j_0})^{-1}v \in U$ for some $v \in X^*$. Define x_u to be $x'_{j_0} \cdots x'_m$ and simply rename $x'_{j_0}, \ldots, x'_m$ to $x_1, \ldots, x_n$.

Since all $x'_1, \ldots, x'_m \in X$, so do $x_1, \ldots, x_n$, and hence $x_u \in X^*$. Now by construction, $x_u^{-1}v = x_n^{-1} \cdots x_1^{-1}v = (x'_m)^{-1} \cdots (x'_{j_0})^{-1}v \in U$ for some $v \in X^*$. Since U is prefix-closed, x_u^{-1} is also in U. Also, all reduced words in U have the form $(x'_m)^{-1} \cdots (x'_j)^{-1}w = x_n^{-1} \cdots x_i^{-1}w$ where $i = j - j_0 + 1$.

Finally, the x_u defined in this way is unique, and is independent of the choice of $x \in X^*$ in the beginning. For if we choose another $\bar{x} \in X^*$ and result in another $\bar{x_u}$, then $\bar{x_u} \in X^*$ and $\bar{x_u}^{-1} \in U \subseteq x_u^{-1}X^*$. Hence $\bar{x_u}^{-1}$ has the form of $x_n^{-1} \cdots x_i^{-1}$, which means $x_u^{-1} \leq \bar{x_u}^{-1}$. In duality we have $\bar{x_u}^{-1} \leq x_u^{-1}$ and thus $x_u^{-1} = \bar{x_u}^{-1}$, or $x_u = \bar{x_u}$. □

Corollary 5.2.9. *Let x_u be constructed as in Theorem 5.2.8, then $(x_u^{\downarrow}, x_u)(U, u) \in$ FLA(X).*

Definition 5.2.10. The unique x_u in Theorem 5.2.8 is called the *tail* of $\underline{u} = (U, u)$.

In conclusion, we have

Theorem 5.2.11. *Given $(U, u), (V, v) \in H$, let $x_u, z_v \in X^*$ be the tails of (U, u) and (V, v) respectively. If $(U, u) \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} (V, v)$, then $x_u = z_v$.*

Proof. As $(x_u^{\downarrow}, x_u)(U, u) \in \mathrm{FLA}(X)$, we have $(x_u^{\downarrow}, x_u)(V, v)$ is also in $\mathrm{FLA}(X)$. Therefore, $x_u z_v^{-1} \in x_u V \subseteq X^*$. Dually $z_v x_u^{-1} \in z_v U \subseteq X^*$, and hence $x_u = z_v$. □

Theorem 5.2.12. *Given $(U, u), (V, v)$. We have $(U, u) \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} (V, v)$ if and only if either*

1. *$(U, u), (V, v) \in \mathrm{FIM}(X) \setminus H$;*
2. *$(U, u), (V, v) \in H$, $u = v$ and $x_u = z_v$, where $x_u, z_v \in X^*$ are the tails of (U, u) and (V, v) respectively.*

Proof. After Theorem 5.2.5 and the previous Theorem, all we left to prove is that $(U,u),(V,v) \in H$, $u = v$ and $x_u = z_v$ implies $(U,u) \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} (V,v)$.

Now we will be using Theorem 5.2.5. For all $g \in X^*$, if $U \subseteq g^{-1}X^*$, then as from Theorem 5.2.8 we have $x_u^{-1} \in U$, so $x_u^{-1} \in g^{-1}X^*$. As $x_u = z_v$, we have $z_v^{-1} \in g^{-1}X^*$, so that, using Theorem 5.2.8, we have $V \subseteq z_v^{-1}X^* \subseteq g^{-1}X^*X^* \subseteq g^{-1}X^*$. The reverse is also true. So by Theorem 5.2.5, we have $(U,u) \sim_{\mathrm{FLA}(X),\mathrm{FIM}(X)} (V,v)$. □

5.3 Syntactic Congruence of X^* in $\mathrm{FIM}(X)$

Next we consider $\sim_{X^*,\mathrm{FIM}(X)}$. Let

$$C_{X^*}(\underline{u}) = \{(\underline{w},\underline{z}) \in \mathrm{FIM}(X) \times \mathrm{FIM}(X) \mid \underline{w}\,\underline{u}\,\underline{z} \in X^*\},$$

the context of $\underline{u}$, with respect to X^*, and

$$H = \{\underline{u} \in \mathrm{FIM}(X) \mid C_{X^*}(\underline{u}) \neq \emptyset\},$$

the set in $\mathrm{FIM}(X)$ that has non-empty context with respect to X^*.

As in the previous section, we have an analogous result for X^* instead of $\mathrm{FLA}(X)$,

Lemma 5.3.1. *For all $\underline{u},\underline{v} \notin H$, $\underline{u} \sim_{X^*,\mathrm{FIM}(X)} \underline{v}$.*

Proof. Same as Lemma 5.2.2. □

To understand the set of elements with non-empty context, we first introduce the following terminology.

Definition 5.3.2. We say that $\underline{u}$ is *linear* if there exists $w, v \in X^*$ such that $U = (w^{-1})^{\downarrow} \cup v^{\downarrow}$.

Note that if $v \in X^*$, v would be in the form $v_1 \cdots v_n$, where $v_j \in X$. If $y \in v^{\downarrow}$, then $y = v_1 \cdots v_i$ for some $i \leq n$. On the other hand, if $y \in (v^{-1})^{\downarrow}$, $y = v_n^{-1} \cdots v_k^{-1}$, for some $k \in \{1, \ldots, n\}$. Now we have the following technical result:

Proposition 5.3.3. *If $\underline{u} = (U,u) = ((w^{-1})^{\downarrow} \cup v^{\downarrow}, u)$ is linear and $y \in U$, then $(y^{\downarrow}, y)^{-1}\underline{u} = ((y^{-1} \cdot w^{-1})^{\downarrow} \cup (y^{-1} \cdot v)^{\downarrow}, y^{-1} \cdot u)$.*

Proof. For any reduced words $p, q \in \mathrm{FG}(X)$ we have

$$(p \cdot q)^{\downarrow} \subseteq p^{\downarrow} \cup p \cdot q^{\downarrow}.$$

First we know that $(y^{\downarrow}, y)^{-1} = (y^{-1} \cdot y^{\downarrow}, y^{-1}) = ((y^{-1})^{\downarrow}, y^{-1})$. Hence

$$\begin{aligned}
(y^{\downarrow}, y)^{-1}\underline{u} &= ((y^{-1})^{\downarrow}, y^{-1})(U,u) \\
&= ((y^{-1})^{\downarrow}, y^{-1})((w^{-1})^{\downarrow} \cup v^{\downarrow}, u) \\
&= ((y^{-1})^{\downarrow} \cup y^{-1} \cdot (w^{-1})^{\downarrow} \cup y^{-1} \cdot v^{\downarrow}, y^{-1} \cdot u).
\end{aligned}$$

Therefore, what we need to prove is

$$(y^{-1}\cdot w^{-1})^{\downarrow}\cup(y^{-1}\cdot v)^{\downarrow}=(y^{-1})^{\downarrow}\cup y^{-1}\cdot(w^{-1})^{\downarrow}\cup y^{-1}\cdot v^{\downarrow}.$$

Recall that $v,w\in X^*$. Let $v=v_1\cdots v_n$, and $w=w_1\cdots w_m$, we have two cases for routine checking:

1. $y\in v^{\downarrow}$. In this case $y=v_1\cdots v_i$, for some $i\leq n$.

$$\begin{array}{rcl} y^{-1}\cdot w^{-1} & = & v_i^{-1}\cdots v_1^{-1}w_m^{-1}\cdots w_1^{-1}; \\ (y^{-1}\cdot w^{-1})^{\downarrow} & = & \{1,v_i^{-1},v_i^{-1}v_{i-1}^{-1},\cdots,v_i^{-1}\cdots v_1^{-1},v_i^{-1}\cdots v_1^{-1}w_m^{-1},\cdots,v_i^{-1}\cdots v_1^{-1}w_m^{-1}\cdots w_1^{-1}\} \\ & = & (y^{-1})^{\downarrow}\cup y^{-1}\cdot(w^{-1})^{\downarrow}; \\ y^{-1}\cdot v & = & v_{i+1}\cdots v_n; \\ (y^{-1}\cdot v)^{\downarrow} & = & \{1,v_{i+1},v_{i+1}v_{i+2},\cdots,v_{i+1}\cdots v_n\}; \\ y^{-1}\cdot v^{\downarrow} & = & y^{-1}\cdot\{1,v_1,v_1v_2,\cdots,v_1\cdots v_n\} \\ & = & \{v_i^{-1}\cdots v_1^{-1},v_i^{-1}\cdots v_2^{-1},\cdots,v_i^{-1},1,v_{i+1},v_{i+1}v_{i+2},\cdots,v_{i+1}\cdots v_n\} \\ & = & (y^{-1})^{\downarrow}\cup(y^{-1}\cdot v)^{\downarrow}. \end{array}$$

   Hence

$$\begin{array}{rcl} (y^{-1}\cdot w^{-1})^{\downarrow}\cup(y^{-1}\cdot v)^{\downarrow} & = & (y^{-1})^{\downarrow}\cup y^{-1}\cdot(w^{-1})^{\downarrow}\cup(y^{-1}\cdot v)^{\downarrow} \\ & = & (y^{-1})^{\downarrow}\cup y^{-1}\cdot(w^{-1})^{\downarrow}\cup y^{-1}\cdot v^{\downarrow}. \end{array}$$

2. $y\in(w^{-1})^{\downarrow}$. In this case $y=w_m^{-1}\cdots w_k^{-1}$, for some $k\in\{1,\ldots,m\}$, and $y^{-1}=w_k\cdots w_m$.

$$\begin{array}{rcl} y^{-1}\cdot w^{-1} & = & w_{k-1}^{-1}\cdots w_1^{-1}; \\ (y^{-1}\cdot w^{-1})^{\downarrow} & = & \{1,w_{k-1}^{-1},w_{k-1}^{-1}w_{k-2}^{-1},\cdots,w_{k-1}^{-1}\cdots w_1^{-1}\}; \\ y^{-1}\cdot(w^{-1})^{\downarrow} & = & y^{-1}\cdot\{1,w_m^{-1},w_m^{-1}w_{m-1}^{-1},\cdots,w_m^{-1}\cdots w_1^{-1}\} \\ & = & \{w_k\cdots w_m,w_k\cdots w_{m-1},\cdots,w_k,1,w_{k-1}^{-1},\cdots,w_{k-1}^{-1}\cdots w_1^{-1}\} \\ & = & (y^{-1})^{\downarrow}\cup(y^{-1}\cdot w^{-1})^{\downarrow}; \\ y^{-1}\cdot v & = & w_k\cdots w_m v_1\cdots v_n; \\ (y^{-1}\cdot v)^{\downarrow} & = & \{1,w_k,w_kw_{k+1},\cdots,w_k\cdots w_m,w_k\cdots w_m v_1,w_k\cdots w_m v_1\cdots v_n\} \\ & = & (y^{-1})^{\downarrow}\cup y^{-1}\cdot v^{\downarrow}. \end{array}$$

   Hence

$$\begin{array}{rcl} (y^{-1}\cdot w^{-1})^{\downarrow}\cup(y^{-1}\cdot v)^{\downarrow} & = & (y^{-1}\cdot w^{-1})^{\downarrow}\cup(y^{-1})^{\downarrow}\cup y^{-1}\cdot v^{\downarrow} \\ & = & (y^{-1})^{\downarrow}\cup y^{-1}\cdot(w^{-1})^{\downarrow}\cup y^{-1}\cdot v^{\downarrow}. \end{array}$$

In conclusion, we have $(y^{-1}\cdot w^{-1})^{\downarrow}\cup(y^{-1}\cdot v)^{\downarrow}=(y^{-1})^{\downarrow}\cup y^{-1}\cdot(w^{-1})^{\downarrow}\cup y^{-1}\cdot v^{\downarrow}$, and thus the proposition is true. $\square$

Corollary 5.3.4. *If $\underline{u}=(U,u)$ is linear, then $(y^{\downarrow},y)^{-1}\underline{u}$ is also linear for all $y\in U$.*

Proof. We can see in Proposition 5.3.3 that $(y^{-1} \cdot w^{-1})^{\downarrow}$ in $(X^{-1})^*$ and $(y^{-1} \cdot v)^{\downarrow}$ in X^* in both cases. Therefore, $(y^{\downarrow}, y)^{-1}\underline{u} = ((y^{-1} \cdot w^{-1})^{\downarrow} \cup (y^{-1} \cdot v)^{\downarrow}, y^{-1} \cdot u)$ is linear. $\square$

Proposition 5.3.5. *Let $\underline{y}, \underline{z} \in \mathrm{FIM}(X)$. If $\underline{y}\,\underline{z}$ is linear, then both $\underline{y}$ and $\underline{z}$ are linear.*

Proof. Let $\underline{y} = (Y, y)$, and $\underline{z} = (Z, z)$. Then $\underline{y}\,\underline{z} = (Y \cup y \cdot Z, y \cdot z)$. For any $v \in X^*$, since $v^{\downarrow} \cap Y$ is finite, there is no problem over the existence of maximal elements, that is, elements of largest length. Say v_y is a maximal element. So, as the intersection of prefix closed sets is still prefix closed, so $(v_y)^{\downarrow} \subseteq v^{\downarrow} \cap Y$. As $v_y \in v^{\downarrow}$, $v_y = v_1 \cdots v_i$ for some $i \leq n$, where $v = v_1 \cdots v_n$. If $(v^{\downarrow} \cap Y) \setminus (v_y)^{\downarrow} \neq \emptyset$, say $v'_y \in (v^{\downarrow} \cap Y) \setminus (v_y)^{\downarrow}$, then as $v'_y \in (v^{\downarrow} \cap Y) \subseteq v^{\downarrow}$, $v'_y = v_1 \cdots v_j$ for some $j \leq n$. Now j must be greater than i, for otherwise v'_y would be in $(v_y)^{\downarrow}$. But then as $v'_y \in v^{\downarrow} \cap Y$ it would contradict v_y being a maximal element in $v^{\downarrow} \cap Y$. So $(v^{\downarrow} \cap Y) \setminus (v_y)^{\downarrow} = \emptyset$, and hence $v^{\downarrow} \cap Y = (v_y)^{\downarrow}$.

Similarly, $(v^{-1})^{\downarrow} \cap Y = (v''_y)^{\downarrow}$, where $v''_y = v_n^{-1} \cdots v_k^{-1}$, for some $k \in \{1, \ldots, n\}$.

If $\underline{y}\,\underline{z}$ is linear, then $Y \cup y \cdot Z = (w^{-1})^{\downarrow} \cup v^{\downarrow}$, where $v, w \in X^*$. In this case, $Y = (Y \cap v^{\downarrow}) \cup (Y \cap (w^{-1})^{\downarrow}) = (v_y)^{\downarrow} \cup (w''_y)^{\downarrow}$, so $\underline{y}$ is linear.

Now since $y \in Y \subseteq Y \cup y \cdot Z$, by Corollary 5.3.4, since $\underline{y}\,\underline{z}$ is linear, $(y^{\downarrow}, y)^{-1}\underline{y}\,\underline{z}$ is also linear. Now $(y^{\downarrow}, y)^{-1}\underline{y}\,\underline{z} = (y^{-1} \cdot y^{\downarrow}, y^{-1})(Y \cup y \cdot Z, y \cdot z) = (y^{-1} \cdot Y \cup Z, z)$. With an argument similar to above, we can see that $\underline{z}$ is linear. $\square$

Proposition 5.3.6. *Let $H = \{u \in \mathrm{FIM}(X) \mid C_{X^*}(u) \neq \emptyset\}$. Then $\underline{u} \in H$ if and only if $\underline{u}$ is linear.*

Proof. We see that H is the set in $\mathrm{FIM}(X)$ that has non-empty context with respect to X^*. In other words, $\underline{u} \in H$ if and only if there is $\underline{w}, \underline{z} \in \mathrm{FIM}(X)$ such that $\underline{w}\,\underline{u}\,\underline{z} \in X^*$. Now it is obvious that every element in X^* is linear, so by Proposition 5.3.5, we see that $\underline{u}$ must also be linear.

On the other hand, suppose that $\underline{u}$ is linear. Let $\underline{u} = ((x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}, x_2)$, where $x_2 \in (x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}$.

Claim. $x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow} \subseteq x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow} = (x_1 \cdot x_3)^{\downarrow}$.

We then have that

$$\begin{aligned} & (x_1^{\downarrow}, x_1)((x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}, x_2)((x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \; & (x_1^{\downarrow} \cup x_1 \cdot (x_1^{-1})^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}, x_1 x_2)((x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \; & (x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow} \cup x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1 \cdot x_3) \\ = \; & (x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}, x_1 x_3) \in X^* \quad \text{as } x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow} \subseteq x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}. \end{aligned}$$

Hence $u \in H$.

Proof of Claim. Since $x_2 \in (x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}$, we have two cases:

1. $x_2 \in (x_1^{-1})^{\downarrow}$. Let $x_1 = x_{1,1} \cdots x_{1,h}$, and $x_3 = x_{3,1} \cdots x_{3,i}$, then $x_2 = x_{1,h}^{-1} \cdots x_{1,k+1}^{-1}$

for some $k < h$. Hence

$$\begin{aligned}
& x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow} \\
= \; & x_{1,1} \cdots x_{1,k}\{1, x_{1,k+1}, x_{1,k+1}x_{1,k+2}, \cdots, x_{1,k+1} \cdots x_{1,h}x_{3,1} \cdots x_{3,i}\} \\
= \; & \{x_{1,1} \cdots x_{1,k}, \cdots, x_{1,1} \cdots x_{1,h}, x_{1,1} \cdots x_{1,h}x_{3,1}, \cdots, x_{1,1} \cdots x_{1,h}x_{3,1} \cdots x_{3,i}\} \\
\subseteq \; & \{1, \cdots, x_{1,1} \cdots x_{1,h}\} \cup x_{1,1} \cdots x_{1,h}\{1, \cdots, x_{3,1} \cdots x_{3,i}\} \\
= \; & x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}.
\end{aligned}$$

2. $x_2 \in x_3^{\downarrow}$. Let $x_1 = x_{1,1} \cdots x_{1,h}$, and $x_3 = x_{3,1} \cdots x_{3,i}$, then $x_2 = x_{3,1} \cdots x_{3,k}$ for some $k \leq i$. Hence

$$\begin{aligned}
& x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow} \\
= \; & x_{1,1} \cdots x_{1,h}x_{3,1} \cdots x_{3,k}\{1, x_{3,k+1}, \cdots, x_{3,k+1} \cdots x_{3,i}\} \\
\subseteq \; & x_{1,1} \cdots x_{1,h}\{1, x_{3,1}, \cdots, x_{3,1} \cdots x_{3,i}\} \\
= \; & x_1 \cdot x_3^{\downarrow} \\
\subseteq \; & x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}.
\end{aligned}$$

$\square$

Here is the main result of this section:

Theorem 5.3.7. *For $\underline{u}, \underline{v} \in H$, $\underline{u} \sim_{X^*,\mathrm{FIM}(X)} \underline{v}$ if and only if $\underline{u} = \underline{v}$.*

Proof. ($\Leftarrow$) Trivial.

($\Rightarrow$) Since $\underline{u}, \underline{v} \in H$, both $\underline{u}$ and $\underline{v}$ are linear. Let $\underline{u} = ((x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}, x_2)$, and $\underline{v} = ((y_1^{-1})^{\downarrow} \cup y_3^{\downarrow}, y_2)$. We know that $x_2 \in (x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}$ and $y_2 \in (y_1^{-1})^{\downarrow} \cup y_3^{\downarrow}$. Now since

$$(x_1^{\downarrow}, x_1)((x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}, x_2)((x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) = (x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}, x_1x_3)$$

We have as $\underline{u} = (U, x_2)$ that $(x_1^{\downarrow}, x_1)(U, u) = (x_1^{\downarrow} \cup x_1 \cdot U, x_1x_2) = (T, x_1x_2)$ say, so that we must have $(x_1x_2)^{\downarrow} \subseteq T$. Since $x_1x_2 \cdot ((x_1x_2)^{-1})^{\downarrow} = (x_1x_2)^{\downarrow}$, it follows that for any (K, k) we have $(x_1^{\downarrow}, x_1)(U, u)(K, k) = (x_1^{\downarrow}, x_1)(U, u)(((x_1x_2)^{-1})^{\downarrow} \cup K, k)$. As a result,

$$\begin{aligned}
& (x_1^{\downarrow}, x_1)\underline{u}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1}x_3) \\
= \; & (x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}, x_1x_3) \in X^*
\end{aligned}$$

That is, we have

$$(x_1^{\downarrow}, x_1)\underline{v}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1}x_3) \in X^*.$$

This gives

$$(x_1^{\downarrow} \cup x_1 \cdot (y_1^{-1})^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \cup x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1y_2x_2^{-1}x_3) \in X^*.$$

$$\begin{cases} x_1^{\downarrow} \subseteq X^* \\ x_1 \cdot (y_1^{-1})^{\downarrow} \subseteq X^* \\ x_1 \cdot y_3^{\downarrow} \subseteq X^* \\ x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \subseteq X^* \\ x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow} \subseteq X^*. \end{cases}$$

Since $x_1 \cdot (y_1^{-1})^{\downarrow} \subseteq X^*$, in particular $x_1 \cdot y_1^{-1}$ is equal to some $w \in X^*$. This means $x_1 = wy_1 \leq y_1$. Dually we have $y_1 \leq x_1$. and hence they are equal. Similarly,

$$x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \subseteq X^*$$

implies

$$x_1 \cdot y_2 \cdot (x_1 \cdot x_2)^{-1} = w \in X^*$$

or

$$x_1 \cdot y_2 = w(x_1 \cdot x_2)$$

So $x_1 \cdot x_2$ is a suffix of $x_1 \cdot y_2$. Dually we have $y_1 \cdot y_2$ is a suffix of $y_1 \cdot x_2$. But we know that $y_1 = x_1$. The statement becomes $x_1 \cdot y_2$ is a suffix of $x_1 \cdot x_2$. Hence we know that $x_1 \cdot y_2 = x_1 \cdot x_2$, thus $y_2 = x_2$.

Now the expression

$$(x_1^{\downarrow} \cup x_1 \cdot (y_1^{-1})^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \cup x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1 y_2 x_2^{-1} x_3) \in X^*,$$

simplifies to

$$(x_1^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup (x_1 \cdot x_2)^{\downarrow} \cup x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1 x_3) \in X^*.$$

But, for the whole expression to be in X^*, we require the first coordinate to be $(x_1 \cdot x_3)^{\downarrow}$. In particular, $x_1 \cdot y_3^{\downarrow} \subseteq (x_1 \cdot x_3)^{\downarrow}$, which mean $x_1 \cdot y_3$ is a prefix of $x_1 \cdot x_3$, or that y_3 is a prefix of x_3. Dually we have x_3 is a prefix of y_3. Hence they are equal and thus $\underline{u} = \underline{v}$. □

5.4 Syntactic Congruence of linear elements in FIM(X)

An interesting set arises from Definition 5.3.2, namely

$$L = \{\underline{u} \in \mathrm{FIM}(X) \mid \underline{u} \text{ is linear}\}.$$

What we would like is to investigate what is $\sim_{L,\mathrm{FIM}(X)}$. To begin with, let $C_L(\underline{u}) = \{(\underline{w}, \underline{z}) \in \mathrm{FIM}(X) \times \mathrm{FIM}(X) | \underline{w}\, \underline{u}\, \underline{z} \in L\}$, the context of $\underline{u}$, with respect to L, and

$H = \{\underline{u} \in \mathrm{FIM}(X) | C_L(\underline{u}) \neq \emptyset\}$, the set in $\mathrm{FIM}(X)$ that has non-empty context with respect to L.

As in the previous sections, we have an analogous result for L.

Lemma 5.4.1. *For all $\underline{u}, \underline{v} \notin H$, $\underline{u} \sim_{X^*,\mathrm{FIM}(X)} \underline{v}$.*

Proof. Same as Lemma 5.2.2. $\square$

Lemma 5.4.2. *The set of $\underline{u}$ in* $\mathrm{FIM}(X)$ *that has non-empty context with respect to L is actually L itself. In other words, $H = L$.*

Proof. We proof by showing that $\underline{u} \in H$ if and only if $\underline{u}$ is linear. Suppose that $\underline{u} \in H$ then there exist $\underline{w}, \underline{z}$ such that $\underline{w}\,\underline{u}\,\underline{z} \in L$. So $\underline{w}\,\underline{u}\,\underline{z}$ is linear. By Proposition 5.3.5, we know that $\underline{u}$ itself is linear.

Now suppose $\underline{u}$ is linear. Then $1\underline{u}1 = \underline{u} \in L$. Hence $(1,1) \in C_L(u)$ and thus $\underline{u} \in H$. $\square$

Similar to the result of previous section:

Theorem 5.4.3. *For $\underline{u}, \underline{v} \in H$, $\underline{u} \sim_{L,\mathrm{FIM}(X)} \underline{v}$ if and only if $\underline{u} = \underline{v}$.*

Proof. ($\Leftarrow$) Trivial.

($\Rightarrow$) Since $\underline{u}, \underline{v} \in H$, both $\underline{u}$ and $\underline{v}$ are linear. Let $\underline{u} = ((x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}, x_2)$, and $\underline{v} = ((y_1^{-1})^{\downarrow} \cup y_3^{\downarrow}, y_2)$. We know that $x_2 \in (x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}$ and $y_2 \in (y_1^{-1})^{\downarrow} \cup y_3^{\downarrow}$. Now as in the proof of Theorem 5.3.7, we know that

$$\begin{aligned}
& (x_1^{\downarrow}, x_1)\underline{u}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\
= \ & (x_1^{\downarrow}, x_1)((x_1^{-1})^{\downarrow} \cup x_3^{\downarrow}, x_2)(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\
= \ & (x_1^{\downarrow} \cup x_1 \cdot x_3^{\downarrow}, x_1 x_3) \\
= \ & ((x_1 \cdot x_3)^{\downarrow}, x_1 x_3) \in X^*, \text{ and hence linear.}
\end{aligned}$$

That is, we have

$$(x_1^{\downarrow}, x_1)\underline{v}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} x_3) \text{ is linear.}$$

This gives

$(x_1^{\downarrow} \cup x_1 \cdot (y_1^{-1})^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \cup x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1 y_2 x_2^{-1} x_3)$ is linear, hence

$$\left\{ \begin{array}{l}
x_1^{\downarrow} \\
x_1 \cdot (y_1^{-1})^{\downarrow} \\
x_1 \cdot y_3^{\downarrow} \\
x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \\
x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}
\end{array} \right.$$

are all subsets of $X^* \cup (X^{-1})^*$.

Since $x_1 \cdot (y_1^{-1})^{\downarrow} \subseteq X^* \cup (X^{-1})^*$, we have $x_1 \cdot y_1^{-1} \in X^* \cup (X^{-1})^*$. This means $x_1 = wy_1$, or we have $y_1 = wx_1$ for some $w \in X^*$.

Without loss of generality, let $y_1 = wx_1$. Now if $w \neq \epsilon$, consider the last element of w, say w_l, and pick an element in X that is different from w_l, say t. Then $t \cdot x_1 \cdot y_1^{-1} = t \cdot x_1 \cdot (wx_1)^{-1} = t \cdot w^{-1} \notin X^* \cup (X^{-1})^*$. Now we consider

$$\begin{aligned} & ((t \cdot x_1)^{\downarrow}, tx_1)\underline{u}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \; & ((t \cdot x_1 \cdot x_3)^{\downarrow}, tx_1x_3) \in X^*, \text{ and hence linear.} \end{aligned}$$

However,

$$\begin{aligned} & ((t \cdot x_1)^{\downarrow}, tx_1)\underline{v}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \; & ((t \cdot x_1)^{\downarrow} \cup t \cdot x_1 \cdot (y_1^{-1})^{\downarrow} \cup t \cdot x_1 \cdot y_3^{\downarrow} \cup t \cdot x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \cup t \cdot x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, t \cdot x_1 \end{aligned}$$

cannot be linear as $t \cdot x_1 \cdot y_1^{-1} \notin X^* \cup (X^{-1})^*$. This contradicts $\underline{u} \sim_{L,\mathrm{FIM}(X)} \underline{v}$. Hence it is only possible that $w = \epsilon$, and $y_1 = x_1$.

Similarly, $x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \subseteq X^* \cup (X^{-1})^*$ implies $x_1 \cdot y_2 \cdot (x_1 \cdot x_2)^{-1} \in X^* \cup (X^{-1})^*$. This means $x_1 \cdot y_2 = w(x_1 \cdot x_2)$ or $x_1 \cdot x_2 = w(x_1 \cdot y_2)$ for some $w \in X^*$.

Similar as before, without loss of generality, let $x_1 \cdot y_2 = w(x_1 \cdot x_2)$. Now if $w \neq \epsilon$, consider the last element of w, say w_l, and pick an element in X that is different from w_l, say t. Then $x_1 \cdot y_2 \cdot (t \cdot x_1 \cdot x_2)^{-1} = w(x_1 \cdot x_2) \cdot (t \cdot x_1 \cdot x_2)^{-1} = w \cdot t^{-1} \notin X^* \cup (X^{-1})^*$. Now we consider

$$\begin{aligned} & (x_1^{\downarrow}, x_1)\underline{u}(((t \cdot x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \; & ((t^{-1})^{\downarrow} \cup (x_1 \cdot x_3)^{\downarrow}, x_1x_3), \text{ which is linear.} \end{aligned}$$

However,

$$\begin{aligned} & (x_1^{\downarrow}, x_1)\underline{v}(((t \cdot x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \; & (x_1^{\downarrow} \cup x_1 \cdot (y_1^{-1})^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup x_1 \cdot y_2 \cdot ((t \cdot x_1 \cdot x_2)^{-1})^{\downarrow} \cup x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1y_2x_2^{-1}x_3) \end{aligned}$$

cannot be linear as $x_1 \cdot y_2 \cdot (t \cdot x_1 \cdot x_2)^{-1} \notin X^* \cup (X^{-1})^*$. This contradicting $\underline{u} \sim_{L,\mathrm{FIM}(X)} \underline{v}$. Hence it is only possible that $w = \epsilon$, and $x_1 \cdot y_2 = x_1 \cdot x_2$. This implies $y_2 = x_2$.

As in Theorem 5.3.7, the expression

$$(x_1^{\downarrow} \cup x_1 \cdot (y_1^{-1})^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \cup x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1y_2x_2^{-1}x_3)$$

simplifies to

$$(x_1^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup (x_1 \cdot x_2)^{\downarrow} \cup x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}, x_1x_3).$$

In the last step, we can note that both $x_1 \cdot y_3$ and $x_1 \cdot x_3$ are in both X^* and $x_1^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup (x_1 \cdot x_2)^{\downarrow} \cup x_1 \cdot x_2 \cdot (x_2^{-1} \cdot x_3)^{\downarrow}$. For the whole expression to be linear, we require that one has to be a prefix of another, i.e., $x_1 \cdot y_3 = (x_1 \cdot x_3)w$ or $x_1 \cdot x_3 = (x_1 \cdot y_3)w$ for some $w \in X^*$.

Without loss of generality, let $x_1 \cdot y_3 = (x_1 \cdot x_3)w$, so $y_3 = x_3 \cdot w$. Now if $w \neq \epsilon$, consider the first element of w, say w_1, and pick an element in X that is different from w_1, say t. Then $(x_1 \cdot x_3) \cdot t$ is not a prefix of $x_1 \cdot y_3$, nor is $x_1 \cdot y_3$ a prefix of $(x_1 \cdot x_3) \cdot t$. Now we consider

$$\begin{aligned} & (x_1^{\downarrow}, x_1)\underline{u}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3 \cdot t)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \;& ((x_1 \cdot x_3 \cdot t)^{\downarrow}, x_1 x_3), \text{ which is linear.} \end{aligned}$$

However,

$$\begin{aligned} & (x_1^{\downarrow}, x_1)\underline{v}(((x_1 \cdot x_2)^{-1})^{\downarrow} \cup (x_2^{-1} \cdot x_3 \cdot t)^{\downarrow}, x_2^{-1} \cdot x_3) \\ = \;& (x_1^{\downarrow} \cup x_1 \cdot (y_1^{-1})^{\downarrow} \cup x_1 \cdot y_3^{\downarrow} \cup x_1 \cdot y_2 \cdot ((x_1 \cdot x_2)^{-1})^{\downarrow} \cup x_1 \cdot y_2 \cdot (x_2^{-1} \cdot x_3 \cdot t)^{\downarrow}, x_1 y_2 x_2^{-1} x_3) \end{aligned}$$

cannot be linear as $(x_1 \cdot x_3) \cdot t$ is not a prefix of $x_1 \cdot y_3$, nor $x_1 \cdot y_3$ is a prefix of $(x_1 \cdot x_3) \cdot t$. This contradicts $\underline{u} \sim_{L,\mathrm{FIM}(X)} \underline{v}$. Hence it is only possible that $w = \epsilon$, and hence $x_1 \cdot y_3 = (x_1 \cdot x_3)$. This implies $y_3 = x_3$ and thus $\underline{u} = \underline{v}$.

□

Bibliography

[1] A. Blumensath and D. Janin. A syntactic congruence for languages of birooted trees. In *Semigroup Forum*, volume 91, pages 675–698. Springer, 2015.

[2] M. J. Branco, G. M. Gomes, and V. Gould. Left adequate and left ehresmann monoids. *International Journal of Algebra and Computation*, 21(07):1259–1284, 2011.

[3] N. Chomsky. Three models for the description of language. *IRE Transactions on information theory*, 2(3):113–124, 1956.

[4] D. M. Clark, B. A. Davey, R. S. Freese, and M. Jackson. Standard topological algebras: syntactic and principal congruences and profiniteness. *Algebra Universalis*, 52(2):343–376, 2005.

[5] A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups, Volume II*, volume 2. American Mathematical Soc., 1967.

[6] H. Comon, M. Dauchet, R. Gilleron, F. Jacquemard, D. Lugiez, S. Tison, and M. Tommasi. Tree automata techniques and applications, 2007.

[7] C. Cornock. *Restriction semigroups: structure, varieties and presentations.* PhD thesis, University of York, 2011.

[8] B. A. Davey, M. Jackson, M. Maróti, and R. N. McKenzie. Principal and syntactic congruences in congruence-distributive and congruence-permutable varieties. *Journal of the Australian Mathematical Society*, 85(1):59–74, 2008.

[9] M. Droste, D. Götze, S. Märcker, and I. Meinecke. Weighted tree automata over valuation monoids and their characterization by weighted logics. In *Algebraic Foundations in Computer Science*, pages 30–55. Springer, 2011.

[10] S. Eilenberg. *Automata, languages, and machines*, volume A. Academic press, 1974.

[11] J. Fountain. A class of right PP monoids. *The Quarterly Journal of Mathematics*, 28(3):285–300, 09 1977.

[12] J. Fountain. Adequate semigroups. *Proceedings of the Edinburgh Mathematical Society*, 22(2):113–125, 1979.

[13] J. Fountain. Free right type A semigroups. *Glasgow Mathematical Journal*, 33(2):135–148, 1991.

[14] J. Fountain, G. M. Gomes, and V. Gould. The free ample monoid. *International Journal of Algebra and Computation*, 19(04):527–554, 2009.

[15] G. M. Gomes and V. Gould. Left adequate and left ehresmann monoids ii. *Journal of Algebra*, 348(1):171–195, 2011.

[16] V. Gould. Notes on restriction semigroups and related structures. *preprint at http://www-users.york.ac.uk/∼varg1/restriction.pdf.*

[17] V. Gould and M. Kambites. Faithful functors from cancellative categories to cancellative monoids with an application to abundant semigroups. *International Journal of Algebra and Computation*, 15(04):683–698, 2005.

[18] R. Hirsch, M. Jackson, et al. Undecidability of representability as binary relations. *Journal of Symbolic Logic*, 77(4):1211–1244, 2012.

[19] C. Hollings. From right PP monoids to restriction semigroups: a survey. *European Journal of Pure and Applied Mathematics*, 2(1):21–57, 2009.

[20] J. M. Howie. *Automata and languages.* Oxford University Press, Inc., 1992.

[21] J. M. Howie. *Fundamentals of semigroup theory.* Clarendon Oxford, 1995.

[22] D. Janin. Walking automata in free inverse monoids. In *International Conference on Current Trends in Theory and Practice of Informatics*, pages 314–328. Springer, 2016.

[23] M. Kambites. Free adequate semigroups. *Journal of the Australian Mathematical Society*, 91(3):365–390, 2011.

[24] M. Kambites. Retracts of trees and free left adequate semigroups. *Edinburgh Mathematical Society. Proceedings of the Edinburgh Mathematical Society*, 54(3):731, 2011.

[25] M. V. Lawson. Semigroups and ordered categories. i. the reduced case. *Journal of Algebra*, 141(2):422–462, 1991.

[26] M. V. Lawson. *Finite automata.* CRC Press, 2003.

[27] S. W. Margolis and J. C. Meakin. Inverse monoids, trees and context-free languages. *Transactions of the American Mathematical Society*, 335(1):259–276, 1993.

[28] R. McKenzie, G. F. McNulty, and W. Taylor. *Algebras, lattices, varieties, Volume I.* Wadsworth & Brooks/Cole Advanced Books & Software Monterey, California, 1987.

[29] W. D. Munn. Free inverse semigroups. *Proceedings of the London Mathematical Society*, 3(3):385–404, 1974.

[30] J.-E. Pin. *Varieties of formal languages.* Plenum Publishing Co., 1986.

[31] H. E. Scheiblich. Free inverse semigroups. *Proceedings of the American Mathematical Society*, 38(1):1–7, 1973.

[32] B. M. Schein. Relation algebras and function semigroups. In *Semigroup forum*, volume 1, pages 1–62. Springer, 1970.

[33] M. P. Schützenberger. On finite monoids having only trivial subgroups. *Information and control*, 8(2):190–194, 1965.

[34] P. Silva. On free inverse monoid languages. *Informatique théorique et applications*, 1996.

[35] J. B. Stephen. Presentations of inverse monoids. *Journal of Pure and Applied Algebra*, 63(1):81–112, 1990.

[36] J. B. Stephen. Presentations of inverse monoids. *Journal of Pure and Applied Algebra*, 63(1):81–112, 1990.

[37] H. Straubing. A generalization of the Schützenberger product of finite monoids. *Theoretical Computer Science*, 13(2):137–150, 1981.