Bachelorarbeit

Reversible Automata: Characterizations and Construction

ausgeführt am

Institut für
Diskrete Mathematik und Geometrie
TU Wien

unter der Anleitung von

Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

durch

Fabian Wöhrer
Matrikelnummer: 11776792

Wien, am 8. April 2024

Contents

1 Introduction

Reversibility is a desired property in the study of computational machines. It means that every elementary computational step can be reverted without any loss of information. In particular, a finite automaton is called reversible, if every letter induces a partial injective map from the set of states into itself. The reversible languages, i.e., those languages that can be accepted by a reversible automaton, form a proper subclass of the class of regular languages. As it turns out, the minimal DFA of a reversible language is usually not reversible. This fact eliminates a supposedly trivial way to characterize reversible languages, which at the same time establishes them as an interesting class of languages. Indeed, their study requires several advanced concepts from the algebraic theory of automata and formal languages as well as a considerable amount of semigroup theory.

This work is roughly divided into two parts. After recapitulating some definitions and well-known results of automata theory, Chapter 3 is devoted to characterizing the class of reversible languages from a group-theoretic, algebraic and topological perspective. On the other hand, Chapter 4 covers the algorithmic side. In Section 4.1 we derive a decision algorithm, that determines whether a given regular language is reversible. Section 4.2 features a constructive algorithm, that assumes a reversible language L as input and builds a (quasi-)reversible automaton accepting L. Chapter 3 and Section 4.1 are mainly based on [10], whereas the construction in Section 4.2 is due to [5].

2 Preliminaries

We quickly recall the usual definitions and some well-known results about languages and automata, as well as some important notions from algebraic automata theory. For all the proofs, more detailed explanations and examples of the presented concepts – especially regarding algebraic automata theory – we refer to [6] and [11].

2.1 Languages and automata

Definition 2.1. Let $A = \{a_1, \cdots, a_n\}$ be an *alphabet* with *letters* $a_1, \ldots, a_n$. Then we denote by A^* the free monoid, i.e., the set of all finite *words* over A, including the empty word ε as unit. The operation * is known as *Kleene star.* A *language* over A^* is any subset $L \subseteq A^*$.

Definition 2.2. The *regular* (or *rational*) languages on A^* are defined as the smallest set of languages $\mathrm{Rat}(A^*)$ satisfying the following conditions:

(1) $\mathrm{Rat}(A^*)$ contains $\emptyset$ and every singleton $\{a\}$ for each letter $a \in A^*$,

(2) $\mathrm{Rat}(A^*)$ is closed under finite union, concatenation and Kleene star.

Consequently, regular languages are exactly those that can be represented as regular expressions, for example $(a + bb)^* + aa^*b$.

Definition 2.3. A (nondeterministic) finite *automaton* is a quintuple $\mathcal{A} = (Q, A, E, I, F)$, where Q is a finite set of *states*, A is an alphabet, $E \subseteq Q \times A \times Q$ is the set of *transitions*, $I \subseteq Q$ is the set of *initial states* and $F \subseteq Q$ is the set of *final states.* If $(q, a, p) \in E$ is a transition, we also write $q \xrightarrow{a} p$.

There is a natural extension of E to a subset of $Q \times A^* \times Q$, which we will also call E. It is also common to interpret E as a function $\delta : Q \times A^* \to 2^Q$. We will use both notations, depending on what is more convenient in the situation.

Definition 2.4. We say that a word $w \in A^*$ is *accepted* (or *recognized*) by a finite automaton $\mathcal{A} = (Q, A, E, I, F)$, if there are states $q_i \in I$ and $q_f \in F$ such that $(q_i, w, q_f) \in E$. The language accepted by $\mathcal{A}$ is thus defined as

$$|\mathcal{A}| = \{w \in A^* \mid \mathcal{A} \text{ accepts } w\}.$$

Definition 2.5. A finite automaton is *deterministic* (short a DFA) if there is only one initial state and the transition relation is actually a function $\cdot : Q \times A \to Q$. In particular, every DFA is a NFA.

Remark 2.6. According to this definition, DFAs are always *complete* – for each state and symbol a transition into some state is defined. Sometimes the above definition of a DFA is slightly altered, such that the transition relation is only required to be a partial function. We will sometimes – especially when talking about the *minimal DFA* – implicitly use this alternative notion. Such a DFA can then always be completed by adding a *trap* state, where all missing transitions are collected.

Definition 2.7. A finite automaton is called *trim*, if every state $q \in Q$ is visited in some path from an initial to a final state, i.e., there are words $u, v \in A^*$ and states $q_i \in I$, $q_f \in F$ such that $(q_i, u, q) \in E$ and $(q, v, q_f) \in E$.

The following theorem, named after Stephen Cole Kleene, one of the founders of theoretical computer science, connects regular languages to finite automata.

Theorem 2.8 (Kleene's theorem)**.** *Let $L \subseteq A^*$ be a language. The following statements are equivalent:*

(1) *L is a regular language,*

(2) *L is accepted by a NFA,*

(3) *L is accepted by a DFA.*

2.2 Algebraic automata theory

Every regular language L is accepted by (infinitely) many finite automata. However, especially from an algebraic perspective, it is often advantageous to consider a DFA accepting L with a minimal number of states. Such a DFA always exists and is unique (up to isomorphism).

Definition 2.9. Let $L \subseteq A^*$ and $u \in A^*$. Then we call $u^{-1}L = \{w \in A^* \mid uw \in L\}$ the *left quotient* of L by the word u.

Definition 2.10. Let $L \subseteq A^*$ be a regular language. The *minimal DFA* of L is given by $\mathcal{D}_L = (Q, A, \cdot, \{q_0\}, F)$, where

$$\begin{aligned} Q &= \{u^{-1}L \mid u \in A^*\}, \\ q_0 &= \varepsilon^{-1}L = L, \\ F &= \{u^{-1}L \mid u \in L\} = \{u^{-1}L \mid \varepsilon \in u^{-1}L\}, \end{aligned}$$

and $u^{-1}L \cdot a = (ua)^{-1}L$ for every $a \in A$.

Finite automata and regular languages are deeply connected to finite monoids. Recall that a monoid is just a set together with an associative binary operation and a unit element.

Definition 2.11. Let M be a monoid and $\varphi : A^* \to M$ be a monoid homomorphism. We say that a language $L \subseteq A^*$ is *recognized* by M (or by φ) if there is a subset $P \subseteq M$ such that $L = \varphi^{-1}(P)$.

The following simple result will turn out to be very useful for the proof of the algebraic characterization in Section 3.2.

Lemma 2.12. *Let M be a monoid and $\varphi : A^* \to M$ be a monoid homomorphism. A language $L \subseteq A^*$ is recognized by φ if and only if $\varphi^{-1}(\varphi(L)) = L$.*

Definition 2.13. Let $\mathcal{A} = (Q, A, \cdot, \{q_0\}, F)$ be a DFA. Every word $w \in A^*$ induces a map

$$\tau_w : Q \to Q,\ q \mapsto q \cdot w.$$

We define the *transition monoid* $M(\mathcal{A})$ of $\mathcal{A}$ as the set

$$M(\mathcal{A}) = \{\tau_w \in Q^Q \mid w \in A^*\},$$

with unit τ_ε and the monoid operation $\tau_u \cdot \tau_v = \tau_{uv}$.

Lemma 2.14. *Let $\mathcal{A}$ be a DFA recognizing a language $L \subseteq A^*$. Then $M(\mathcal{A})$ recognizes L.*

In particular, every regular language is recognized by a finite monoid. We even have the converse, yielding another characterization of regular languages, in addition to Kleene's theorem.

Theorem 2.15. *A language $L \subseteq A^*$ is regular if and only if it is recognized by a finite monoid.*

Although the transition monoid already provides a concrete example of a finite monoid recognizing a regular language, it has the disadvantage of being dependent on a corresponding automaton. The solution to this issue is the so-called *syntactic monoid*, which plays a crucial role in this entire work.

Definition 2.16. Let $L \subseteq A^*$. We define the *syntactic congruence* $\approx_L$ on A^* by

$$w_1 \approx_L w_2 \iff (\forall u, v \in A^* : uw_1v \in L \iff uw_2v \in L),$$

and call $M(L) = A^*/_{\approx_L}$ the *syntactic monoid* of L. Furthermore, the natural homomorphism $\eta : A^* \to M(L)$, $w \mapsto [w]_{\approx_L}$ is called the *syntactic homomorphism*.

A priori, the actual construction of the syntactic monoid of a language seems to be not as obvious as the construction of the transition monoid of a DFA. However, we have:

Theorem 2.17. *Let $L \subseteq A^*$ be a regular language. Then $M(L) \simeq M(\mathcal{D}_L)$.*

Remark 2.18. The above result states that we can obtain $M(L)$ by first constructing $\mathcal{D}_L$ and then its transition monoid $M(\mathcal{D}_L)$. Afterwards we just perform the identification $\tau_w \mapsto [w]_{\approx_L}$.

Corollary 2.19. *Let $L \subseteq A^*$ be a regular language. Then $M(L)$ recognizes L.*

The syntactic monoid $M(L)$ does not only recognize L, it is also – in a certain sense – the "smallest" monoid with this property.

Definition 2.20. Let M, N be monoids. We say that N is a *quotient* of M if there is a surjective homomorphism $\varphi : M \to N$. If N is a quotient of a submonoid of M, then we call N a *divisor* of M. We then also say that N *divides* M and write $N \preccurlyeq M$.

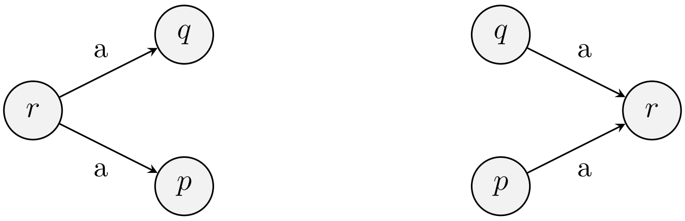
Theorem 2.21. *Let $L \subseteq A^*$ and M be a monoid. Then M recognizes L if and only if $M(L) \preccurlyeq M$.*

3 Characterization of reversible languages

The current chapter is mostly based on the work by J.-É. Pin [10]. Before we proceed with the actual characterizations of reversible languages, we first differentiate them from another class of regular languages, which seems similar, but is much simpler to describe.

Definition 3.1. A finite automaton $\mathcal{A} = (Q, A, E, I, F)$ is *reversible* if every letter $a \in A$ induces a partial injective (one-to-one) map from Q into itself. A *reversible language* is a regular language $L \subseteq A^*$ that is accepted by some reversible automaton.

This definition can also be phrased in terms of forbidden configurations. An automaton is deterministic if and only if it has a unique initial state and does not contain any configuration of type `FC1`. On the other hand, an automaton is *codeterministic* if and only if it has a unique final state and does not contain any configuration of type `FC2`.



(a) `FC1` (b) `FC2`

Figure 3.1: The two types of forbidden configurations

Proposition 3.2. *A finite automaton is reversible if and only if no configurations of type `FC1` or `FC2` occur.*

Proof. Clearly, `FC1` corresponds to the transition relation being a partial function, and `FC2` corresponds to injectivity. □

Definition 3.3. A finite automaton is called *bideterministic* if it is both deterministic and codeterministic.

By definition, every bideterministic automaton is also reversible. The converse is not true, as reversible automata may have several initial and/or final states. It is surprisingly easy to characterize the languages accepted by a bideterministic automaton.

Lemma 3.4. *Every trim bideterministic automaton is already minimal.*

Proof. Let $\mathcal{A} = (Q, A, \cdot, \{q_0\}, \{q_f\})$ be a trim bideterministic automaton and assume that $\mathcal{A}$ is not minimal. Furthermore, let $L = |\mathcal{A}|$. Then there are at least two distinct words $u, v \in A^*$ satisfying $u^{-1}L = v^{-1}L$ and $q_0 \cdot u \neq q_0 \cdot v$. Let $p = q_0 \cdot u$ and $r = q_0 \cdot v$. Since $\mathcal{A}$ is trim, there is a word $w \in A^*$ with $p \cdot w = q_f$, which implies $uw \in L$ and therefore $w \in u^{-1}L = v^{-1}L$. This in turn implies $vw \in L$ and thus

$$r \cdot w = (q_0 \cdot v) \cdot w = q_0 \cdot vw = q_f = p \cdot w.$$

Since $p \neq r$, this is a contradiction to $\mathcal{A}$ being codeterministic. □

Theorem 3.5. *A regular language $L \subseteq A^*$ is accepted by a bideterministic automaton if and only if its minimal DFA $\mathcal{D}_L$ is reversible and has a unique final state.*

Proof. We show both implications.

$\boxed{\Leftarrow}$ If $\mathcal{D}_L$ is reversible and has a unique final state, then it is already bideterministic, since the initial state of $\mathcal{D}_L$ is always unique.

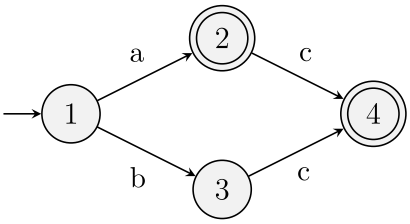
$\boxed{\Rightarrow}$ Conversely, let $\mathcal{A}$ be a bideterministic automaton accepting L. Clearly, every automaton can be trimmed by removing any redundant states, without changing the language it accepts. Hence we can assume $\mathcal{A}$ to be trim. By Lemma 3.4, $\mathcal{A}$ is equal (or at least isomorphic) to $\mathcal{D}_L$. Thus $\mathcal{D}_L$ is bideterministic and therefore reversible with a unique final state. □

The characterization of the class $\mathcal{C}$ of reversible languages is far more challenging. This is mainly due to the fact that the minimal DFA of a reversible language is not reversible in general, as the following simple example demonstrates.

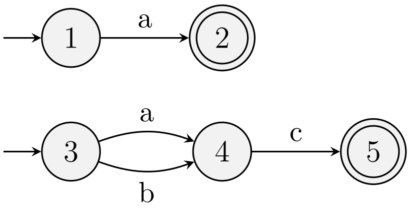
Example 3.6. Consider the language $L = \{a, ac, bc\}$. The non-empty left quotients are

$$1 := L, \quad 2 := a^{-1}L, \quad 3 := b^{-1}L, \quad 4 := (ac)^{-1}L = (bc)^{-1}L.$$

Hence, $\mathcal{D}_L$ is given by



Since $\mathcal{D}_L$ contains a forbidden configuration of type FC2, it is not reversible. However, L is a reversible language, as it is also accepted by the following reversible automaton:



Despite this example, the minimal DFA will serve as a starting point for both deciding the reversibility of a given language algorithmically as well as constructing a reversible automaton that accepts a given reversible language, see Chapter 4.

3.1 Group-theoretic characterization

In order to motivate the first characterization of $\mathcal{C}$, we briefly take a look at the relation between reversible languages and the class of *group languages*. As the name suggests, group languages are regular languages recognized by a finite group. They can also be characterized as the languages that are recognized by a permutation automaton, i.e., an automaton in which every letter induces a permutation on the set of states (see [12]) – as opposed to reversible automata, where every letter only induces a partial one-to-one map. Thus reversible languages can be viewed as a slight generalization of group languages, which suggests some characterization involving groups.

3.1.1 The free group and rational subgroups

Definition 3.7. For a set A let $A^{-1} = \{\bar{a} \mid a \in A\}$, where $\bar{a}$ is the (formal) inverse symbol of a, and let $\tilde{A} = A \uplus A^{-1}$. We denote by $\approx$ the congruence on $\tilde{A}^*$ generated by the relation $\{(a\bar{a}, \varepsilon) \mid a \in A\} \cup \{(\bar{a}a, \varepsilon) \mid a \in A\}$. Then the quotient $FG(A) = \tilde{A}^*/_{\approx}$ is called the *free group* and $\pi : \tilde{A}^* \to FG(A)$ defined by $w \mapsto [w]_{\approx}$ is the natural homomorphism.

Remark 3.8. Let A be a finite alphabet. Since the inverse of each letter is unique, every class $[w]_{\approx}$ in $FG(A)$ has a shortest representative $w_0 \in [w]_{\approx}$, namely the completely pruned word. We will always identify $FG(A)$ with the set of its representatives and therefore also consider $FG(A)$ as a subset of $\tilde{A}^*$.

Remark 3.9. The inverse of a word $w = a_1 \cdots a_k \in FG(A)$ is obtained by traversing backwards along the inverse letters, i.e., $\overline{w} = \overline{a_k} \cdots \overline{a_1}$.

There is a natural way to extend a given automaton $\mathcal{A} = (Q, A, E, I, F)$ to an automaton on $\tilde{A}$, by adding for each edge a corresponding reverse edge labelled by the reverse letter. To this end, set $\tilde{\mathcal{A}} = (Q, \tilde{A}, \tilde{E}, I, F)$, where

$$\tilde{E} = E \cup \{(q', \bar{a}, q) \mid (q, a, q') \in E\}.$$

The words accepted by $\tilde{\mathcal{A}}$ constitute a subset of $\tilde{A}^*$. However, we are only interested in the induced representatives in $FG(A)$.

Definition 3.10. Let $\mathcal{A} = (Q, A, E, I, F)$ be an automaton. The *subset of the free group accepted by* $\mathcal{A}$ is defined as

$$\|\mathcal{A}\| = \pi(|\tilde{\mathcal{A}}|).$$

Conversely, a subset $S \subseteq FG(A)$ is said to be accepted by a (reversible) automaton, if there exists a (reversible) automaton $\mathcal{A}$ on A, such that $S = \|\mathcal{A}\|$.

Lemma 3.11. *Let $\mathcal{A} = (Q, A, E, I, F)$ be an automaton. Then $|\mathcal{A}| = \|\mathcal{A}\| \cap A^*$.*

Proof. The left-to-right inclusion follows directly from $|\mathcal{A}| = \pi(|\mathcal{A}|) \subseteq \pi(|\tilde{\mathcal{A}}|) = \|\mathcal{A}\|$. On the other hand, $\|\mathcal{A}\| \subseteq |\tilde{\mathcal{A}}|$ and $|\tilde{\mathcal{A}}| \cap A^* = |\mathcal{A}|$, therefore $\|\mathcal{A}\| \cap A^* \subseteq |\mathcal{A}|$. □

Due to Lemma 3.11 we can revert to describing $\|\mathcal{A}\|$ instead of $|\mathcal{A}|$. The following simple observation will prove to be quite useful later.

Lemma 3.12. *The image of the natural morphism $\pi : \tilde{A}^* \to FG(A)$ is compatible with union, concatenation and Kleene star.*

Proof. Like every function, π preserves arbitrary unions. Let $U, V \in \tilde{A}^*$. Since π is a monoid homomorphism we have $\pi(UV) = \pi(U)\pi(V)$ and also $\pi(U^0) = \pi(\{\varepsilon\}) = \{\varepsilon\} = \pi(U)^0$. Putting that all together, we finally obtain

$$\pi(U^*) = \pi\left(\bigcup_{n\in\mathbb{N}} U^n\right) = \bigcup_{n\in\mathbb{N}} \pi(U)^n = \pi(U)^*.$$

□

Definition 3.13. We define the *rational subsets* of $FG(A)$ inductively as the smallest class $\mathcal{R}_A$ of subsets of $FG(A)$ that satisfies the following conditions:

(1) $S \in FG(A)$ and $|S| < \infty \implies S \in \mathcal{R}_A$,

(2) $S, T \in \mathcal{R}_A \implies ST \in \mathcal{R}_A$, $S \cup T \in \mathcal{R}_A$, $S^* \in \mathcal{R}_A$.

Lemma 3.14. *Let $S \in \mathcal{R}_A$ and denote by $\langle S\rangle$ the subgroup of $FG(A)$ generated by S. Then $\langle S\rangle \in \mathcal{R}_A$.*

Proof. We can express $\langle S\rangle$ as the submonoid of $FG(A)$ generated by S and S^{-1}, i.e., $\langle S\rangle = (S \cup S^{-1})^*$. Hence the result follows from condition (2), if we can show that S^{-1} is rational. Clearly, if S is finite then also S^{-1} is finite. Otherwise the result follows inductively from the equations

$$(ST)^{-1} = S^{-1}T^{-1}, \quad (S \cup T)^{-1} = S^{-1} \cup T^{-1}, \quad (S^*)^{-1} = (S^{-1})^*.$$

□

In particular, every finitely generated subgroup of $FG(A)$ is rational. With some more effort one can also show the converse:

Proposition 3.15. *A subgroup of $FG(A)$ is rational if and only if it is finitely generated.*

For the rather technical proof we refer to [2].

3.1.2 Reversible languages in the free group

We have now gathered all the requirements to prove the first characterization of $\mathcal{C}$.

Theorem 3.16. *A subset $S \subseteq FG(A)$ is accepted by a reversible automaton if and only if S is a finite union of left cosets of finitely generated subgroups of $FG(A)$.*

Proof. We show both implications:

$\boxed{\Rightarrow}$ Let $\mathcal{A} = (Q, A, E, I, F)$ be a reversible automaton with $S = \|\mathcal{A}\|$.

Recall that a reversible automaton can possess several initial and final states. To this end, set $\mathcal{A}_{p,q} = (Q, A, E, \{p\}, \{q\})$ for every $p, q \in Q$. By Lemma 3.12 we obtain

$$\tilde{\mathcal{A}} = \bigcup_{\substack{p\in I,\\ q\in F}} \tilde{\mathcal{A}}_{p,q} \quad\Longrightarrow\quad |\tilde{\mathcal{A}}| = \bigcup_{\substack{p\in I,\\ q\in F}} |\tilde{\mathcal{A}}_{p,q}| \quad\Longrightarrow\quad \|\mathcal{A}\| = \bigcup_{\substack{p\in I,\\ q\in F}} \|\mathcal{A}_{p,q}\|,$$

where we can always assume $\|\mathcal{A}_{p,q}\| \neq \emptyset$.

Next, choose any $g \in \|\mathcal{A}_{p,q}\|$. We claim that $\|\mathcal{A}_{p,q}\| = g\|\mathcal{A}_{q,q}\|$. Lemma 3.12 implies one inclusion:

$$g\|\mathcal{A}_{q,q}\| \subseteq \|\mathcal{A}_{p,q}\|\|\mathcal{A}_{q,q}\| = \|\mathcal{A}_{p,q}\|.$$

Conversely, let $w \in \|\mathcal{A}_{p,q}\|$. Since $\bar{g} \in \|\mathcal{A}_{q,p}\|$ we conclude $\bar{g}w \in \|\mathcal{A}_{q,q}\|$ and therefore

$$w = \varepsilon w = g\bar{g}w \in g\|\mathcal{A}_{q,q}\|.$$

Finally, we need to show that $\|\mathcal{A}_{q,q}\|$ is a finitely generated subgroup of $FG(A)$. Since the initial and final state are equal, $\|\mathcal{A}_{q,q}\|$ is evidently a subgroup of $FG(A)$. It remains to show that $\|\mathcal{A}_{q,q}\|$ is finitely generated. If $\|\mathcal{A}_{q,q}\|$ is finite this is clear. Otherwise recall that by Kleene's theorem $|\tilde{\mathcal{A}}_{q,q}|$ is rational and $\|\mathcal{A}_{q,q}\|$ is the image of $|\tilde{\mathcal{A}}_{q,q}|$ under π. Repeated application of Lemma 3.12 shows that $\|\mathcal{A}_{q,q}\|$ is built from unions, concatenations and stars of finite subsets of $FG(A)$. Consequently, $\|\mathcal{A}_{q,q}\|$ is rational and thus finitely generated, as stated in Proposition 3.15.

Altogether, we obtained the desired decomposition,

$$\|\mathcal{A}\| = \bigcup_{\substack{p\in I,\\ q\in F}} g_{p,q}\|\mathcal{A}_{q,q}\|,$$

where $g_{p,q}$ is some word in $\|\mathcal{A}_{p,q}\|$.

$\boxed{\Leftarrow}$ For the reverse implication we denote by $\mathcal{S}$ the class of all $S \subseteq FG(A)$ accepted by a reversible automaton. We need to show that $\mathcal{S}$ contains every finitely generated subgroup of $FG(A)$ and that $\mathcal{S}$ is closed under left cosets and finite union.

Let $S_1, S_2 \in \mathcal{S}$, i.e., they are accepted by reversible automata $\mathcal{A}_1, \mathcal{A}_2$. Then the union $S_1 \cup S_2$ is accepted by the reversible automaton $\mathcal{A}_1 \uplus \mathcal{A}_2$, see Lemma 3.12 again. Hence $S_1 \cup S_2 \in \mathcal{S}$.

Regarding left cosets, let $S = \|\mathcal{A}\|$, where $\mathcal{A} = (Q, A, E, I, F)$ is reversible, and let $g \in FG(A)$. Then $I\bar{g} = \{q \in Q \mid q \cdot g \in I\}$ is the set of states that reach some state in I via g and we set $\mathcal{A}_g = (Q, A, E, I\bar{g}, F)$. It is easy to see that $gS = \|\mathcal{A}_g\|$ and since reversibility does not depend on the set of initial states $\|\mathcal{A}_g\|$ is also reversible, which implies $gS \in \mathcal{S}$.

Finally, let $H = \langle h_1, \dots, h_n\rangle$ be a finitely generated subgroup of $FG(A)$. We want to construct a reversible automaton $\mathcal{B}$ that accepts H. For every $i = 1, \dots, n$, we choose some $u_i \in \tilde{A}^*$, such that $\pi(u_i) = h_i$,[1] and set $U = \{u_1, \dots, u_n\}$. Due to Lemma 3.12 we have

$$\pi(|\tilde{\mathcal{B}}|) = \|\mathcal{B}\| \overset{!}{=} H = \langle(\pi(U)\rangle = (\pi(U) \cup \pi(U)^{-1})^* = \pi((U \cup U^{-1})^*), \qquad (3.1.1)$$

so the automaton $\tilde{\mathcal{B}}$ should exactly accept all concatenations of words from $U \cup U^{-1}$. This is achieved by the associated "flower" automaton $\mathcal{B} = (Q, A, E, \{1\}, \{1\})$, where

$$Q = \{1\} \cup \{(x, y) \in (\tilde{A}^+)^2 \mid xy \in U\}$$

and $E = E_1 \cup E_2 \cup E_3$ with

$$\begin{aligned}
E_1 &= \{(1, a, (a, y)) \mid a \in A, ay \in U\} \cup \{((\bar{a}, y), a, 1) \mid a \in A, \bar{a}y \in U\},\\
E_2 &= \{((x, a), a, 1) \mid a \in A, xa \in U\} \cup \{(1, a, (x, \bar{a})) \mid a \in A, x\bar{a} \in U\},\\
E_3 &= \{(x, ay), a, (xa, y) \mid a \in A, xay \in U\} \cup \{(xa, y), a, (x, ay) \mid a \in A, x\bar{a}y \in U\}.
\end{aligned}$$

By adding the reverse edges we obtain $\tilde{\mathcal{B}}$. Since each of the n "petals" of $\tilde{\mathcal{B}}$ constitutes a loop starting and ending in state 1 and accepting exactly one of the u_i's and its inverse $\overline{u_i}$ condition (3.1.1) is satisfied. In particular, $\mathcal{B}$ accepts H.

Unfortunately the automaton $\mathcal{B}$ is not reversible in general. However, it can be transformed into a reversible automaton in a very straightforward way. Consider a forbidden configuration as described earlier, which means that there are states $p_1, p_2, q \in Q$ and some letter $a \in A$, such that $p_1 \xrightarrow{a} q \xleftarrow{a} p_2$ or $p_1 \xleftarrow{a} q \xrightarrow{a} p_2$. Now we obtain a new automaton $\mathcal{B}'$ by just identifying p_1 and p_2. In general this yields $|\mathcal{B}'| \neq |\mathcal{B}|$ but still preserves $\|\mathcal{B}'\| = \|\mathcal{B}\|$, since $\tilde{\mathcal{B}}$ contains a path $a\bar{a}$ or $\bar{a}a$ from p_1 to p_2. This transformation decreases the number of states by 1, so after repeating it at most $|Q|$ times we obtain a reversible automaton accepting H. □

Corollary 3.17. *A regular language $L \subseteq A^*$ is reversible if and only if $L = S \cap A^*$, where S is a finite union of left cosets of finitely generated subgroups of $FG(A)$.*

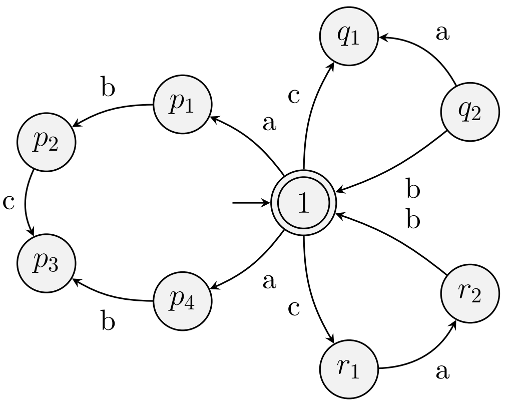
Example 3.18. To illustrate the second direction of the above proof, we will construct a reversible automaton accepting a given subset of the free group. Consider the word $g = a\bar{c}$ and $H = \langle abc\bar{b}\bar{a}, c\bar{a}b, cab\rangle$. Then gH is a left coset of a finitely generated subgroup of

[1] One possible choice would be $u_i = h_i$, which also minimizes the number of states in the following construction. However, every other word $u_i \in \tilde{A}^*$ from the same equivalence class works as well.

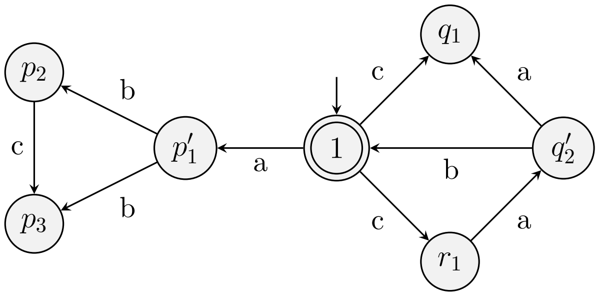
$FG(\{a,b,c\})$. First, we construct the flower automaton accepting H, where we renamed the states to

$$\begin{aligned}&p_1=(a,bc\bar{b}\bar{a}),\ p_2=(ab,c\bar{b}\bar{a}),\ p_3=(abc,\bar{b}\bar{a}),\ p_4=(abc\bar{b},\bar{a}),\\&q_1=(c,\bar{a}b),\ q_2=(c\bar{a},b),\\&r_1=(c,ab),\ r_2=(ca,b),\end{aligned}$$

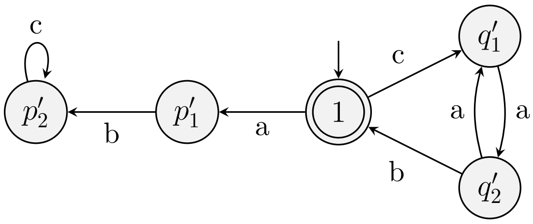
for the sake of readability.



Obviously, this automaton is not reversible yet, as there are several forbidden configurations. In a first step we identify the states p_1 and p_4 to a new state p_1', as well as the states q_2 and r_2 to a new state q_2'.



After that we can perform two more transformations. We we identify the states p_2 and p_3 to a new state p_2', as well as the states q_1 and r_1 to a new state q_1'.



Now there are no forbidden configurations left, so the above automaton is reversible and accepts H. In order for it to accept gH we only need to adjust the initial state from 1 to q_2', since $I\bar{g} = \{1\} \cdot c\bar{a} = \{q_2'\}$. This concludes the construction. The above example did not deal with the union of left cosets, however the result is just the union of the respective reversible automata and thus not really interesting.

To complete this section, recall that by Kleene's theorem the languages accepted by finite automata are exactly the regular languages, which are inductively defined as the closure of the finite languages w.r.t. finite unions, concatenations and stars. We can rephrase Theorem 3.16 as an analogous version of Kleene's theorem for reversible languages:

Theorem 3.19. *The subsets of $FG(A)$ accepted by a reversible automaton form the smallest class of subsets $\mathcal{F}$ such that*

(1) $\emptyset \in \mathcal{F}$ *and* $\{g\} \in \mathcal{F}$ *for every* $g \in FG(A)$,

(2) $S_1, S_2 \in \mathcal{F} \implies S_1 \cup S_2 \in \mathcal{F}$,

(3) $S \in \mathcal{F}, g \in FG(A) \implies gS \in \mathcal{F}$,

(4) $S \in \mathcal{F} \implies \langle S \rangle \in \mathcal{F}$.

Proof. Again, as in the proof of Theorem 3.16, we denote by $\mathcal{S}$ the class of all $S \in FG(A)$ accepted by a reversible automaton. We need to prove $\mathcal{F} = \mathcal{S}$.

For the left-to-right inclusion we show that $\mathcal{S}$ satisfies the conditions (1)-(4). Clearly, $\mathcal{S}$ contains the empty set and all the singletons. According to Theorem 3.16, $\mathcal{S}$ is closed under finite unions and under the operation $S \to gS$ for every $g \in FG(A)$. In order to show that $\mathcal{S}$ satisfies (4), first recall that due to Proposition 3.15 a subgroup of $FG(A)$ is finitely generated if and only if it is rational. Now, let $S \in \mathcal{S}$. Then S is a finite union of left cosets of rational sets and thus rational. Lemma 3.14 shows that $\langle S \rangle$ is rational, and therefore finitely generated, hence $\langle S \rangle \in \mathcal{S}$. It follows $\mathcal{F} \subseteq \mathcal{S}$.

Conversely, $\mathcal{F}$ satisfies (1) and (2) and thus contains the finite subsets of $FG(A)$. By applying (4), then (3) and finally (2) again, we obtain that $\mathcal{F}$ contains all finite unions of left cosets of finitely generated subgroups of $FG(A)$, and thus $\mathcal{S} \subseteq \mathcal{F}$. □

3.2 Algebraic characterization

This section covers not just one but two characterizations of $\mathcal{C}$, however they are quite similar. We will apply them later on in Chapter 4.

In contrast to the previous section, groups do not play a major role anymore. Instead, we will delve deeply into the realm of semigroup theory, with the central objects of interest being the syntactic monoid of a language and its idempotent elements.

3.2.1 The syntactic monoid of reversible languages

Definition 3.20. Let M be a monoid and $x \in M$. We say that x is *idempotent* if $x = x^2$.

Clearly, every idempotent x also satisfies $x = x^n$ for every integer $n > 0$.

Even though the letter e is mostly used for the unit element in the literature, it will from now on be the convention in this work to use e (and f) for idempotents.

Lemma 3.21. *The class of monoids with commuting idempotents is closed under division.*

Proof. Let M be a monoid with commuting idempotents and $P \preccurlyeq M$. Then there is a submonoid N of M and a surjective homomorphism $\beta : N \to P$. Clearly, the idempotents commute in every subset of M and therefore in N. Now let $e, f \in P$ be idempotent. Then there are $x, y \in N$, such that $\beta(x) = e$ and $\beta(y) = f$, and we obtain

$$ef = \beta(x)\beta(y) = \beta(xy) = \beta(yx) = \beta(y)\beta(x) = fe.$$

□

Lemma 3.22. *Let S be a finite semigroup. Then every element of S has an idempotent power, i.e., for every $a \in S$ there exists an integer $n \geq 1$, such that a^n is idempotent.*

Proof. By the pigeonhole principle, there are integers $m, p \geq 1$ such that $a^m = a^{m+p}$, and therefore $a^m = a^{m+kp}$ for every $k \geq 0$. Setting $b = a^m$ yields $b^{p+1} = a^{m+mp} = a^m = b$. It follows

$$(a^{mp})^2 = b^{2p} = b^{p+1}b^{p-1} = bb^{p-1} = b^p = a^{mp},$$

hence a^{mp} is idempotent. □

Using the basic results above we can already prove two properties of $\mathcal{C}$, which will later turn out to even be a proper characterization.

Proposition 3.23. *If $L \subseteq A^*$ is a reversible language, then*

(a) *the idempotents of $M(L)$ commute,*

(b) $\forall x, u, y \in A^* : (xu^+y \subseteq L \implies xy \in L)$.

Proof. Let $\mathcal{A} = (Q, A, E, I, F)$ be a reversible automaton accepting L and let e be an idempotent of the transition monoid $M(\mathcal{A})$,[2] i.e., $\tau_e \circ \tau_e = \tau_e$.[3] In other words, if $q \cdot e$ is defined for a state $q \in Q$, then $(q \cdot e) \cdot e = q \cdot e$. In that case, since $\mathcal{A}$ is reversible, there is also a reverse transition that leads back to q, thus $q \cdot e = q$. Consequently, if two idempotent

[2] The transition monoid is technically only defined for DFAs. For reversible automata (where the transition maps τ_w are only partial functions), we implicitly add a trap state, in order to make the definition still work. A state being "undefined" then corresponds to being the trap state.

[3] As mentioned earlier, here we implicitly identify a word $w \in A^*$ with its induced class $[\tau_w] \in M(\mathcal{A})$.

transitions are defined on a state, they act neutrally on it and therefore commute. Hence the idempotents commute in $M(\mathcal{A})$. Since $M(L)$ divides $M(\mathcal{A})$, Lemma 3.21 implies that the idempotents also commute in $M(L)$.

Let $x, u, y \in A^*$, such that $xu^+y \subseteq L$. Since L is a regular language, $M(\mathcal{A})$ is a finite monoid. By Lemma 3.22, there is an integer $n > 0$ such that u^n is idempotent in $M(\mathcal{A})$. Since $xu^ny \in L$, there are states $q_0 \in I, q_f \in F$ with $q_0 \cdot xu^ny = q_f$. In particular, $q_0 \cdot xu^n$ is defined and consequently there is a state $p \in Q$ with $(q_0 \cdot x) \cdot u^n = p = (q_0 \cdot xu^n) \cdot u^n$. As in the proof of (a), the reversibility of $\mathcal{A}$ implies $q_0 \cdot x = q_0 \cdot xu^n$. It immediately follows that $q_0 \cdot xy = q_0 \cdot xu^ny = q_f$ and thus $xy \in L$. □

Condition (b) essentially states that "plus" is equivalent to the Kleene star. Keeping possible algorithmic applications in mind, this formulation seems to be potentially problematic. A priori it is not clear whether it can even be verified in a finite amount of time. Even though we will show that (b) can indeed be verified in polynomial time (see Chapter 4), it would still be nice to have a purely algebraic version, which replaces the infinite monoid A^* by the finite monoid $M(L)$. This gives rise to our second characterization.

Proposition 3.24. *Let $L \subseteq A^*$ be a regular language. Then the following conditions are equivalent:*

(b) $\forall x, u, y \in A^* : (xu^+y \subseteq L \implies xy \in L)$,

(c) $\forall s, e, t \in M(L), e$ *idempotent*: $(set \in \eta(L) \implies st \in \eta(L))$.

Proof. First, assume that (b) holds and let $s, e, t \in M(L)$ such that e is idempotent and $set \in \eta(L)$. Since η is a surjective homomorphism, there are $x, u, y \in A^*$ with $\eta(x) = s, \eta(u) = e$ and $\eta(y) = t$, and it follows

$$\eta(xu^ny) = \eta(x)\eta(u)^n\eta(y) = set \in \eta(L) \quad \implies \quad xu^ny \in \eta^{-1}(\eta(L)),$$

for every integer $n > 0$. Since $\eta(L)$ recognizes L, we have $\eta^{-1}(\eta(L)) = L$ and therefore $xu^+y \subseteq L$. Condition (b) now implies $xy \in L$ and thus $st = \eta(xy) \in \eta(L)$.

Conversely, let (c) be satisfied and let $x, u, y \in A^*$ such that $xu^+y \subseteq L$. Due to Lemma 3.22 – as $M(L)$ is finite – there is an integer $n > 0$ such that $e = \eta(u)^n$ is idempotent in $M(L)$. We set $s = \eta(x), t = \eta(y)$, and obtain $set = \eta(xu^ny) \in \eta(L)$. Condition (c) then implies

$$\eta(xy) = st \in \eta(L) \quad \implies \quad xy \in \eta^{-1}(\eta(L)) = L.$$

□

3.2.2 Green's relations and regular elements

While it was rather straightforward to show that (a) and (b) – or (a) and (c) – are necessary conditions for the reversibility of a regular language, their sufficiency is much more difficult to prove. In particular, we need some terminology from semigroup theory.

Definition 3.25. Let M be a monoid. An element $x \in M$ is called *regular* if there is a element $y \in M$ such that $xyx = x$ and $yxy = y$.

We will now proceed to define ideals of semigroups and Green's relations, which are important notions for the study of semigroups. Some of the definitions are rather natural for monoids but need to be tweaked to be meaningful for semigroups by adjoining a unit. To that end, let S be a semigroup. We denote by S^1 the induced monoid $S \cup \{1\}$ with $1 \cdot s = s = s \cdot 1$ for all $s \in S$. If S is already a monoid, then we set $S^1 = S$.

Definition 3.26. Let S be a semigroup. A subset $I \subseteq S$ is called *right ideal* (*left ideal*) of S if $IS \subseteq I$ ($SI \subseteq I$) or, equivalently, $IS^1 = I$ ($S^1I = I$). An *ideal* of S is a subset $I \subseteq S$ which is both a right ideal and a left ideal or, equivalently, satisfies $S^1IS^1 = I$.

Let S be a semigroup. For a subset $G \subseteq S$ the set S^1GS^1 clearly is an ideal containing G. Let $H \subseteq S$ be another ideal containing G. Then $S^1GS^1 \subseteq S^1HS^1 = H$, so S^1GS^1 is indeed the smallest ideal containing G and thus called the ideal *generated* by G. Left and right ideals generated by a subset are defined analogously.

Definition 3.27. Let S be a semigroup. A minimal element among the set of nonempty ideals of S is called *minimal ideal* of S.

Proposition 3.28. *A nonempty finite semigroup has exactly one minimal ideal.*

Proof. Let $S = \{s_1, \ldots, s_n\}$ be a finite semigroup. There are only finitely many (at most 2^n) ideals of S, but at least one, namely S itself. The intersection of two ideals I_1, I_2 of S is an ideal:

$$S^1(I_1 \cap I_2)S^1 \subseteq S^1I_1S^1 \cap S^1I_2S^1 = I_1 \cap I_2.$$

Let J be the intersection of all nonempty ideals of S. Then $J \subseteq I$ for every ideal I of S. Furthermore, $p = s_1 \cdots s_n \in S^1IS^1 = I$ for every nonempty ideal I. Hence, $p \in J$, so J is nonempty and therefore indeed the minimal ideal of S. □

Of particular interest are *principal ideals*, i.e., those generated by a single element. Their induced equivalence relations are known as *Green's relations.* For a more detailed study we refer to [11] and [4].

Definition 3.29. Let S be a semigroup and $s, t \in S$. Green's relations are defined by:

$$\begin{aligned}
s\,\mathcal{R}\,t &\iff sS^1 = tS^1,\\
s\,\mathcal{L}\,t &\iff S^1s = S^1t,\\
s\,\mathcal{J}\,t &\iff S^1sS^1 = S^1tS^1,\\
s\,\mathcal{D}\,t &\iff \exists u \in S : (s\,\mathcal{R}\,u \wedge u\,\mathcal{L}\,t) \iff \exists u \in S : (s\,\mathcal{L}\,u \wedge u\,\mathcal{R}\,t),\\
s\,\mathcal{H}\,t &\iff s\,\mathcal{R}\,t \wedge s\,\mathcal{L}\,t.
\end{aligned}$$

It can be immediately checked that $\mathcal{R}$ and $\mathcal{L}$ can be equivalently defined by

$$\begin{aligned} s\,\mathcal{R}\,t &\iff \exists u, v \in S : (s = tu \wedge t = sv), \\ s\,\mathcal{L}\,t &\iff \exists u, v \in S : (s = ut \wedge t = vs). \end{aligned}$$

This definition emphasizes the interpretation of Green's relation as "a noncommutative generalisation to semigroups of the standard notion of being a multiple among integers or polynomials" ([11]).

Definition 3.30. Let $\mathcal{G}$ be any of Green's relations. We call a $\mathcal{G}$-class *regular* if it contains a regular element.

From now on, we will denote the $\mathcal{R}$-class of an element s by $R(s)$, its $\mathcal{L}$-class by $L(s)$, and so on.

Lemma 3.31. *Let S be a semigroup and $s \in S$. Then the following statements are equivalent:*

(1) *s is regular,*

(2) *$R(s)$ is regular,*

(3) *$R(s)$ contains an idempotent.*

The same result holds for $L(s)$.

Proof. First, we show the equivalence of (1) and (3). If s is regular, then there is some $t \in S$ such that $s = sts$. Clearly, $st \in R(s)$. Moreover, $st = (sts)t = (st)^2$ implies that st is idempotent. Conversely, let $e \in R(s)$ be idempotent. Then there are $u, v \in S$ such that $s = eu$ and $e = sv$, and therefore $ees = es = eeu = eu = s$. We set $\bar{s} = vsv$ and obtain

$$\begin{aligned} s\bar{s}s &= s(vsv)s = (sv)(sv)s = ees = s, \\ \bar{s}s\bar{s} &= (vsv)s(vsv) = v(sv)(sv)sv = v(ees)v = vsv = \bar{s}, \end{aligned}$$

thus s is regular.

The implication (1) $\implies$ (2) is trivial. Conversely, let $R(s)$ be regular. Then $R(s)$ contains a regular element t. By (3), $R(s) = R(t)$ contains an idempotent, hence s is regular. □

Lemma 3.32. *The minimal ideal of a nonempty finite semigroup S contains an idempotent.*

Proof. Let $J \subseteq S$ be the minimal ideal of S. Like every ideal, J is a subsemigroup of S:

$$JJ = (S^1JS^1)(S^1JS^1) = S^1J(S^1S^1JS^1) \subseteq S^1JS^1 = J.$$

Due to Lemma 3.22, every $a \in J$ has an idempotent power. Since J is nonempty, such an idempotent indeed exists in J. □

Definition 3.33. A semigroup S is called *simple* if it contains no proper ideals, i.e., $\emptyset$ and S are the only ideals of S.

Lemma 3.34. *A simple semigroup S contains only one $\mathcal{J}$-class.*

Proof. Let $a, b \in S$. Since a and b generate the same ideal, we have $S^1 a S^1 = S^1 b S^1$. Hence, by definition, $a \mathcal{J} b$. □

Proposition 3.35 ([11]). *In a finite semigroup, $\mathcal{J}$ and $\mathcal{D}$ are equal.*

Proposition 3.36 ([11]). *Let D be a $\mathcal{D}$-class of a semigroup S. If D contains an idempotent, it contains at least one idempotent in each $\mathcal{R}$-class and in each $\mathcal{L}$-class.*

Proposition 3.37 ([11]). *Let H be an $\mathcal{H}$-class of a semigroup S. H contains an idempotent e if and only if H is a group with unit e.*

Lemma 3.38. *Let S be a finite simple semigroup and let $e \in S$ be idempotent. If e is the only idempotent of S, then S is a group with unit e.*

Proof. By Lemma 3.34, there is only one $\mathcal{J}$-class, i.e., $J(e) = S$. Proposition 3.35 then implies $D(e) = S$. Since e is the only idempotent in $D(e)$, Proposition 3.36 shows that $D(e)$ contains only one $\mathcal{R}$-class and only one $\mathcal{L}$-class, hence $R(e) = L(e) = D(e) = S$. Since $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$, it finally follows that $H(e) = S$. By Proposition 3.37, S is a group with unit e. □

Proposition 3.39 ([4]). *If a semigroup S contains a minimal ideal I, then I is a simple subsemigroup of S.*

The following result is a special case of the Location theorem, see [11] for a proof.

Proposition 3.40. *Let D be a $\mathcal{D}$-class of a finite semigroup S and let $s, t \in D$. Then, $st \in R(s) \cap L(t)$ if and only if $st \in D$.*

Lemma 3.41. *Let S be a finite semigroup with commuting idempotents. Then the minimal ideal of S is a group whose unit is idempotent.*

Proof. Since S is finite, the minimal ideal I exists and, by Lemma 3.32, contains an idempotent e. By Proposition 3.39, I is a simple semigroup. Due to Lemma 3.38, it remains to show that e is the only idempotent of I.

Let $f \in I$ be another idempotent. Since I is a subgroup, $ef \in I$. Since all the idempotents commute, $(ef)^2 = e^2 f^2 = ef$, thus ef is idempotent as well. By Lemma 3.34 and Proposition 3.35, I contains only one $\mathcal{D}$-class, hence $D(e) = D(f) = D(ef)$. Now Proposition 3.40 implies $ef \in R(e) \cap L(f)$, i.e., $e \mathcal{R} ef \mathcal{L} f$. This means that there are $u, v \in S$, such that $e = (ef)u$ and $f = v(ef)$. It follows,

$$e = (ef)u = ef(efu) = efe = e^2 f = ef^2 = fef = (vef)ef = v(ef) = f,$$

hence e is the unique idempotent in I. □

At this point it may seem that we deviated quite a bit from the original topic of reversible automata. However, we need the last result for showing the following properties of $\mathcal{R}$-classes, which will later turn out to be crucial for proving the reversibility of a certain automaton.

Proposition 3.42. *Let M be a finite monoid with commuting idempotents and let R be a regular $\mathcal{R}$-class. Then*

(1) *R contains a unique idempotent e,*

(2) $\forall x \in R : ex = x$,

(3) $\forall u, v, s \in M : ((u \mathrel{\mathcal{R}} v \mathrel{\mathcal{R}} us \wedge us = vs) \implies u = v)$.

Proof. Since R is regular, it contains an idempotent by Lemma 3.31. If $x \in R$, then $e \mathrel{\mathcal{R}} x$ and thus $e = xy$ and $x = ez$ for some $x, y \in M$. It follows that $ex = eez = ez = x$, hence (2) holds.

Now let f be another idempotent of R. Then, by (2), $e = fe = ef = f$, hence (1) holds.

It remains to show (3). The relation $u \mathrel{\mathcal{R}} v \mathrel{\mathcal{R}} us$ implies $u = ust$ and $v = ua$ for some $t, a \in M$. Now we define the subset $S = \{x \in M \mid ux = u\}$ of M, which is clearly a finite semigroup. By Lemma 3.41, the minimal ideal I of S is a group with an idempotent f as unit. In particular, we have $uf = u$ and it follows,

$$\begin{aligned} u(stf) &= (ust)f = uf = u, \\ u(fastf) &= (uf)astf = (ua)stf = (vs)tf = (us)tf = u. \end{aligned}$$

This means $stf, fastf \in S$. Since f is an idempotent contained in I, we conclude

$$\begin{aligned} stf &= (stf)ff \in S^1IS^1 = I, \\ fastf &= (fastf)ff \in S^1IS^1 = I. \end{aligned}$$

Since I is a group, also $fa \in I \subseteq S$, i.e., $u(fa) = u$. On the other hand, $(uf)a = ua = v$, hence $u = v$, which completes the proof. □

Remark 3.43. As mentioned before, the extensive preparation steps of this subsection solely aim at proving property (3) of the previous proposition. In particular, they are supposed to be a breakdown of the proof given in [10] – the paper this entire section is based on. However, there is also a much more direct proof of (3), which does not require Lemma 3.41, see [1].

We need one more result, which provides a decomposition of a word by maximizing the sizes of its regular substrings w.r.t. some homomorphic image.

Proposition 3.44 ([1])**.** *Let M be a finite monoid with commuting idempotents, and let $\psi : A^* \to M$ be a monoid homomorphism. Then there exists an integer $N > 0$ such that every word $w \in A^*$ admits a factorization of the form $w = u_0v_1u_1 \cdots v_ku_k$ with*

(1) *$u_0, u_k \in A^*$, $u_1, \dots, u_{k-1} \in A^+$, $v_1, \dots, v_k \in A^+$,*

(2) *$\psi(v_1), \dots, \psi(v_k)$ are regular elements of M,*

(3) *if a_i (b_i) denotes the first (last) letter of u_i, then $\psi(b_{i-1}v_i)$ and $\psi(v_i a_i)$ are not regular,*

(4) *$|u_0 \cdots u_k| \leq N$.*

3.2.3 Proving reversibility

So far we have shown that the conditions (a) and (b) – respectively (a) and (c) – are necessary for a regular language to be reversible. We will now prove that they are also sufficient.

Proposition 3.45. *Every regular language $L \subseteq A^*$ satisfying (a) and (c) is reversible.*

Proof. Let r be the maximum size of an $\mathcal{R}$-class of $M(L)$. This number is well-defined since $M(L)$ is finite and therefore contains only finitely many $\mathcal{R}$-classes. By condition (a), the idempotents of $M(L)$ commute, hence we can apply Proposition 3.44 to the syntactic homomorphism $\eta : A^* \to M(L)$ and obtain a corresponding integer $N > 0$. Now the set

$$\mathcal{F} := \{\mathcal{B} = (Q, A, E, I, F) \mid \mathcal{B} \text{ reversible, } |Q| \leq r(N+1),\ |\mathcal{B}| \subseteq L\}$$

is finite, since there are only finitely many automata with a fixed number of states. Hence the disjoint union $\mathcal{A}$ of the automata contained in $\mathcal{F}$ is a reversible automaton again and satisfies $|\mathcal{A}| \subseteq L$. It remains to show the other inclusion.

To that aim, let $w \in L$. In order to show $w \in |\mathcal{A}|$, we need find a reversible automaton $\mathcal{B} \in \mathcal{F}$ with $w \in |\mathcal{B}|$.

First we generalize condition (c) from a statement about $\eta(L)$ to a statement about any subset $X \subseteq M(L)$: We say that X satisfies (c), if

$$\forall s, e, t \in M(L), e \text{ idempotent} : (set \in X \implies st \in X).$$

Now we set $m = \eta(w)$ and define $P(m)$ as the smallest subset of $M(L)$ that contains m and satisfies (c). Since $\eta(L)$ contains m and satisfies (c) we obtain $P(m) \subseteq \eta(L)$. It follows

$$L(m) := \eta^{-1}(P(m)) \subseteq \eta^{-1}(\eta(L)) = L,$$

resulting in the diagram below:

$$\begin{tikzcd}
L(m) \arrow[r, bend left, "\eta"] \arrow[d, phantom, sloped, "\subseteq"] & P(m) \arrow[l, bend left, "\eta^{-1}"] \arrow[d, phantom, sloped, "\subseteq"] \\
L \arrow[r, bend left, "\eta"] & \eta(L) \arrow[l, bend left, "\eta^{-1}"]
\end{tikzcd}$$

For the rest of the proof we consider two cases. To roughly outline the idea: If m is a regular element of $M(L)$, we can define an automaton $\mathcal{B} \in \mathcal{F}$ accepting $L(m)$. Since $w \in \eta^{-1}(m) \subseteq \eta^{-1}(P(m)) = L(m)$, this already implies $w \in |\mathcal{B}|$. If m is not regular, we can use the factorization of w given by Proposition 3.44 to reduce this case to the first one.

- ⇝ First, let m be regular. By Proposition 3.42, its $\mathcal{R}$-class $R = R(m)$ contains a unique idempotent e. We define the automaton $\mathcal{B} = (R, A, E, \{e\}, \{m\})$, where

  $$E = \{(x, a, x \cdot \eta(a)) \mid x \in R, a \in A, x \cdot \eta(a) \in R\}.$$

  We claim that $|\mathcal{B}| = L(m)$. To see that we define

  $$S = \{x \in S \mid ex = m\}.$$

  By definition, $|\mathcal{B}| = \eta^{-1}(S)$, hence it suffices to show that $S = P(m)$. Proposition 3.42 implies $em = m$ and therefore $m \in S$. To show that S satisfies (c), let $sft \in S$ for some $s, f, t \in M(L)$ such that f is idempotent. Since $e \mathcal{R} m$, there is some $y \in M(L)$ with $e = my$. It follows

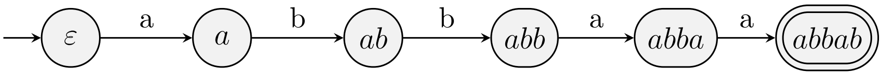
  $$es = (my)s = m(ys) = e(sft)(ys) = (esf)tys,$$

  and therefore $es \mathcal{R} esf \mathcal{R} (es)f = (esf)f$. Proposition 3.42 implies $es = esf$, and thus $est = esft = m$, which means that $st \in S$. Thus S satisfies (c) and contains m, but $P(m)$ is the smallest subset of $M(L)$ with these properties, hence $P(m) \subseteq S$. To show the other inclusion, let $x \in S$. Then $1ex = ex = m \in P(m)$, where $1 = \eta(\varepsilon)$ is the unit of $M(L)$. By condition (c), it follows $s = 1s \in P(m)$. Thus we have shown $S = P(m)$ and thereby $|\mathcal{B}| = L(m)$.

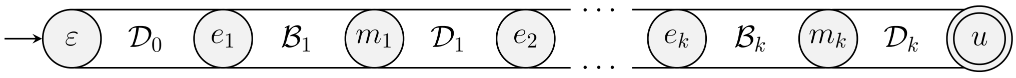
  We still need to verify that $\mathcal{B} \in \mathcal{F}$. We first notice that $\mathcal{B}$ is deterministic by definition. Now let $a \in A$ and $x, y \in R$ such that $x \cdot \eta(a) = y \cdot \eta(a) \in R$. Then Proposition 3.42 implies $x = y$, hence $\mathcal{B}$ is also codeterministic and therefore reversible. Furthermore, $|\mathcal{B}| = L(m) \subseteq L$, and $\mathcal{B}$ has $|R| \leq r \leq r(N + 1)$ states. As a result, $\mathcal{B}$ is indeed contained in $\mathcal{F}$.

- ⇝ If m is not regular, then consider a factorization $w = u_0 v_1 u_1 \cdots v_k u_k$, as given by Proposition 3.44. For every $i = 1, \ldots, k$, we set $m_i = \eta(v_i)$. Since m_i is regular, its $\mathcal{R}$-class $R(m_i)$ contains a unique idempotent e_i. According to the first case, with E_i defined similar to E before, $L(m_i)$ is then accepted by the automaton $\mathcal{B}_i = (R(m_i), A, E_i, \{e_i\}, \{m_i\}) \in \mathcal{F}$.

  We cannot do the same for the u_i, as they are not regular. However, since the length of the word $u = u_0 u_1 \cdots u_k$ is bounded by N, it is sufficient to just consider the minimal DFAs $\mathcal{D}_i$ of $\{u_i\}$, which are just "string" automata. For instance, the minimal DFA of the word $abbab$ is given by

  Clearly, every automaton $\mathcal{D}_i$ is reversible. Now we joint all the automata $\mathcal{D}_i$ and $\mathcal{B}_i$ together in the order $\mathcal{D}_0, \mathcal{B}_1, \mathcal{D}_1, \ldots, \mathcal{B}_k, \mathcal{D}_k$. We do this by identifying the final state of $\mathcal{D}_i$ with e_{i+1} ($i = 0, \ldots, k-1$) and by identifying the initial state of $\mathcal{D}_i$ with m_i ($i = 1, \ldots, k$). The resulting automaton $\tilde{\mathcal{B}}$ then is of the following form:



By construction, $\tilde{\mathcal{B}}$ accepts the language

$$K = u_0 L(m_1) u_1 \cdots L(m_k) u_k,$$

in particular, $w \in |\tilde{\mathcal{B}}|$.

It remains to show that $\tilde{\mathcal{B}}$ is contained in $\mathcal{F}$. Clearly, $\tilde{\mathcal{B}}$ is reversible, as it is constructed as a "sequence" of reversible (even bideterministic) automata. Furthermore, for every $i = 1, \ldots, k$, the automaton $\mathcal{B}_i$ has $|R(m_i)| \leq r$ states. In the worst case, $u_0 = u_k = \varepsilon$ and the other u_i are all just single letters. Then $N \geq |u| = |u_1 \cdots u_{k-1}|$ implies $k \leq N + 1$ and the identification process eliminates all the states that would be added from the $\mathcal{D}_i$, hence $\tilde{\mathcal{B}}$ has at most $r(N+1)$ states.

To prove $|\tilde{\mathcal{B}}| \subseteq L$, it suffices to show $\eta(K) \subseteq P(m)$, since then

$$|\tilde{\mathcal{B}}| = K \subseteq \eta^{-1}(\eta(K)) \subseteq \eta^{-1}(P(m)) = L(m) \subseteq L.$$

Set $s_i = \eta(u_i)$ for $i = 0, \ldots, k$. Then we have $\eta(K) = s_0 P(m_1) s_1 \cdots P(m_k) s_k$ and $m = s_0 m_1 s_1 \cdots m_k s_k$. We define

$$T = \{(t_1, \ldots, t_k) \in P(m_1) \times \cdots \times P(m_k) \mid s_0 t_1 s_1 \cdots t_k s_k \in P(m)\}.$$

Since $m \in P(m)$, it follows that $(m_1, \ldots, m_k) \in T$. Next, let $(t_1, \ldots, t_k) \in T$, where $t_i = x_i f_i y_i$ with f_i idempotent. Then

$$\begin{aligned} (s_0 t_1 \cdots s_{i-1} x_i) f_i (y_i s_i \cdots s_k t_k) \in P(m) &\overset{\text{(c)}}{\Longrightarrow} s_0 t_1 \cdots s_{i-1} x_i y_i s_i \cdots s_k t_k \in P(m) \\ &\Longrightarrow (t_1, \ldots, t_{i-1}, x_i y_i, t_{i+1}, \ldots, t_k) \in T. \end{aligned}$$

Repeating this procedure for every $i = 1, \ldots, k$ yields $(x_1 y_1, \ldots, x_k y_k) \in T$. Hence, T is actually equal to $P(m_1) \times \cdots \times P(m_k)$, which implies $\eta(K) \subseteq P(m)$. □

Theorem 3.46. *Let $L \subseteq A^*$ be a regular language. Then the following statements are equivalent:*

(1) *L is reversible,*

(2) *L satisfies* (a) *and* (b)*,*

(3) *L satisfies* (a) *and* (c)*.*

Proof. If L is reversible, then (a) and (b) hold by Proposition 3.23. Due to Proposition 3.24 this is equivalent to (a) and (c). Finally, if (a) and (c) are satisfied, then Proposition 3.45 proves the reversibility of L. □

3.3 Topological characterization

3.3.1 The profinite topology

For our last characterization we consider a topology on A^*, the so-called *profinite group topology*, introduced in [12]. Recall that the *order* of a finite group G, denoted by $\operatorname{ord}(G)$, is the number of its elements.

Definition 3.47. Let $u, v \in A^*$ be two words. We say that u and v can be *separated* by a finite group if there exists a finite group G and a monoid homomorphism $\varphi : A^* \to G$ such that $\varphi(u) \neq \varphi(v)$. We define

$$\begin{aligned} r(u,v) &= \min\{\operatorname{ord}(G) \mid G \text{ is a finite group separating } u \text{ and } v\}, \\ d(u,v) &= e^{-r(u,v)}, \end{aligned}$$

with the conventions $\min \emptyset = \infty$, and $e^{-\infty} = 0$.

The idea behind the definition of d is the following: Two words $u, v \in A^*$ shall be considered very similar, if a group of high order is necessary to separate them. On the other hand, if it is "easy" to separate them, i.e., it only takes a small group, then they shall be considered far apart. In fact, the only case in which u and v cannot be separated at all, i.e., $d(u,v) = 0$, is when $u = v$. To put it differently:

Lemma 3.48. *Two distinct words $u, v \in A^*$ can always be separated by a finite group.*

Proof. Let $u, v \in A^*$ such that $u \neq v$. Then $L = \{u, v\}$ is accepted by the following "fork" automaton: Let $p \in A^*$ be the longest common prefix of u and v, i.e., there are words $u', v' \in A^*$ with different first letters, such that $u = pu'$, $v = pv'$. Then we append both the minimal DFA of $\{u'\}$ and $\{v'\}$ to the minimal DFA of $\{p\}$, like we did in the proof of Proposition 3.45. In the resulting automaton $\mathcal{A}$ – which now resembles a two-pronged fork – we inherit the initial state q_0 from the minimal DFA of $\{p\}$ and the two final states $q_u \neq q_v$ from the minimal DFAs of $\{u'\}$ and $\{v'\}$. Clearly, $\mathcal{A}$ accepts L, whereby $q_0 \cdot u = q_u$ and $q_0 \cdot v = q_v$.

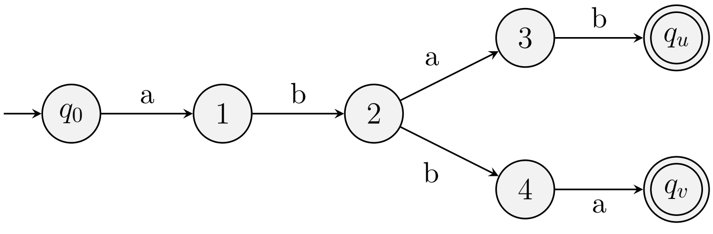


Figure 3.2: Fork automaton $\mathcal{A}$ for $u = abab$ and $v = abba$ with $p = ab$.

By construction, $\mathcal{A} = (Q, A, E, \{q_0\}, \{q_u, q_v\})$ is reversible, i.e., every letter induces a partial injective map from Q to itself. In particular, $\mathcal{A}$ can be completed to a permutation automaton $\mathcal{B}$, i.e., an automaton where every letter $a \in A^*$ induces a permutation $\pi_a \in S_Q$, where S_Q denotes the symmetric group over Q. Note that, in general, there are multiple ways to complete $\mathcal{A}$ to a permutation automaton.

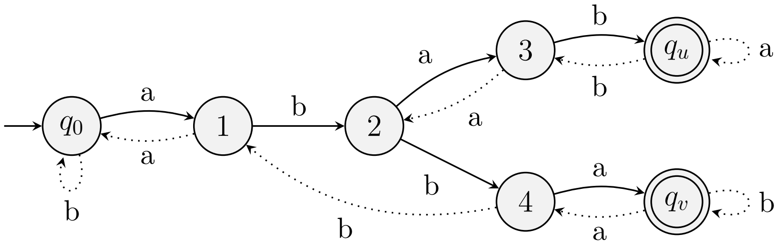


Figure 3.3: Possible completion of $\mathcal{A}$ to a permutation automaton $\mathcal{B}$.

Now, let $G = \langle\{\pi_a \mid a \in A\}\rangle$ be the subgroup of S_Q generated by the induced permutations of A. Since S_Q has $|Q|!$ elements, G is finite as well. Set $\tau * \sigma := \sigma \circ \tau$ for permutations $\tau, \sigma \in S_Q$. Let

$$\pi : A^* \to (G, *),\ w \mapsto \pi_w$$

be the induced monoid homomorphism of the map $a \mapsto \pi_a$, i.e., its natural extension from A to A^*. Then we compute

$$\pi_u(q_0) = q_0 \cdot u = q_u \neq q_v = q_0 \cdot v = \pi_v(q_0),$$

and therefore $\pi_u \neq \pi_v$. Thus G separates u and v. □

Proposition 3.49. *The function d is an (ultra-)metric on A^*.*

Proof. Lemma 3.48 implies that $d(u, v) = 0$ if and only if $u = v$. Moreover, d is obviously symmetric. It remains to show the strong triangle equation,

$$d(u, w) \leq \max(d(u, v), d(v, w)).$$

Let G be a finite group with $\operatorname{ord}(G) = r(u, w)$ that separates u and w. Then there is a monoid homomorphism $\varphi : A^* \to G$, such that $\varphi(u) \neq \varphi(w)$, and therefore $\varphi(u) \neq \varphi(v)$ or $\varphi(v) \neq \varphi(w)$. Let w.l.o.g. $\varphi(u) \neq \varphi(v)$. Then G separates u and v, hence

$$r(u, v) \leq \operatorname{ord}(G) = r(u, w) \quad \Longrightarrow \quad d(u, w) \leq d(u, v) \leq \max(d(u, v), d(v, w)).$$

Thus, d is indeed an ultrametric. □

Definition 3.50. The topology induced by d is called the *profinite group topology* on A^*.

Remark 3.51. There are several equivalent definitions of this topology. For instance, in [12] it is characterized as the initial topology w.r.t. all monoid homomorphisms from A^* into any discrete finite group, i.e., the coarsest topology such that all these homomorphisms are continuous.

Lemma 3.52 ([9]). *The concatenation on (A^*, d) is uniformly continuous.*

Having a topology on A^* allows us to consider sequences of words and their limits. The following example of a converging sequence will later turn out to be quite useful.

Proposition 3.53. *For every word $w \in A^*$, $\lim_{n\to\infty} w^{n!} = \varepsilon$.*

Proof. Let $\varphi : A^* \to G$ be a homomorphism into a finite group G of order k with unit 1. It suffices to show that from some index on, $\varphi(w^{n!}) = \varphi(\varepsilon)$. If $n \geq k$, then k divides $n!$. Thus every element $g \in G$ satisfies $g^{n!} = g^k = 1$, and it follows $\varphi(w^{n!}) = (\varphi(w))^{n!} = 1 = \varphi(\varepsilon)$. □

3.3.2 Closed languages and their reversibility

Proposition 3.54. *Every reversible language is closed in the profinite group topology.*

Proof. Let $L \subseteq A^*$ be accepted by a reversible automaton $\mathcal{A} = (Q, A, E, I, F)$. We will show that L^c is open. To this end, let $w \notin L$. We need to find an open set U with $w \in U \subseteq L^c$.

Set $w = uv$, where u is the longest prefix of w that can be read by $\mathcal{A}$, i.e., there are states $q_0 \in I, q \in Q$ with $q_0 \cdot u = q$. Now we modify $\mathcal{A}$ similarly to the proof of Lemma 3.48: We append the minimal DFA of $\{v\}$ to $\mathcal{A}$, by identifying its initial state with q. We do not alter the initial and final states. By construction, the resulting automaton $\mathcal{A}'$ is still reversible and reads – but does not accept – the word w.

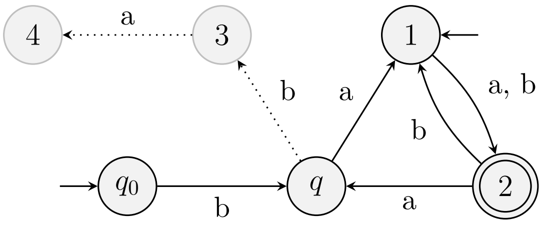


Figure 3.4: Constructing $\mathcal{A}'$ from $\mathcal{A}$ for $w = bababa = (baba)(ba) = uv$.

Guided again by the proof of Lemma 3.48, we complete $\mathcal{A}'$ to a permutation automaton $\mathcal{B}$ and consider the homomorphism $\pi : A^* \to G$, $w \mapsto \pi_w$, mapping each word to its induced permutation. By Remark 3.51, π is continuous. Since G is equipped with the discrete topology, every singleton is open. Hence, $U = \pi^{-1}(\{\pi_w\})$ is open and satisfies $w \in U$. For every $w' \in U$, we have

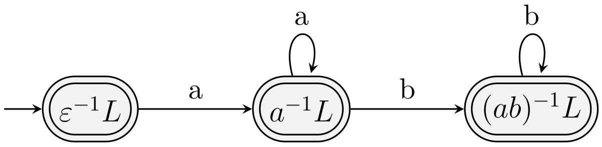
$$\pi_{w'} = \pi(w') = \pi(w) = \pi_w \quad \Longrightarrow \quad I \cdot w' = I \cdot w \subseteq Q \setminus F.$$

It follows $w' \in L^c$ and therefore $U \subseteq L^c$, which finishes the proof. □

The converse of Proposition 3.54 is not true in general.

Example 3.55. Let $A = \{a, b\}$. The regular language $L = a^*b^*$ is closed in A^*, but not reversible. To see that L is indeed closed, we utilize a result proven in [9]: For open languages $L_0, \ldots, L_k \subseteq A^*$ and letters $a_1, \ldots, a_k \in A$, the language $L_0a_1L_1 \cdots a_kL_k$ is open as well. Since A^* itself is open, this implies that $L^c = A^*bA^*aA^*$ is open, hence L is closed.

We already know from Proposition 3.23 that – by condition (a) – the idempotents of the syntactic monoid of a reversible language always commute. The minimal DFA $\mathcal{D}_L$ of L is given by



Now, $M(L)$ is isomorphic to $M(\mathcal{D}_L)$ and we obtain

$$M(L) = \{[\varepsilon], [a], [b], [ab], [ba]\}.$$

Clearly, $[a]$ and $[b]$ are idempotent, but do not commute, since $[a][b] = [ab] \neq [ba] = [b][a]$. Hence, L is not reversible.

After this example, one could conjecture that adding condition (a) is already sufficient for a closed language to be reversible. This is indeed true.

Theorem 3.56. *A regular language $L \subseteq A^*$ is reversible if and only if it is closed in the profinite group topology and the idempotents of $M(L)$ commute.*

Proof. If L is reversible, then it is closed by Proposition 3.54 and the idempotents of $M(L)$ commute by Proposition 3.23.

Conversely, it suffices to show that every closed language L satisfies (b), since (a) and (b) are equivalent to reversibility by Theorem 3.46. Let $x, u, y \in A^*$ such that $xu^+y \subseteq L$. Then, $xu^{n!}y \in L$ for every integer $n > 0$. Since L is closed and the concatenation of words is continuous, it follows by Proposition 3.53 that

$$xy = x\varepsilon y = x\Big(\lim_{n\to\infty} u^{n!}\Big)y = \lim_{n\to\infty} xu^{n!}y \in L,$$

hence (b) holds. □

As a side effect, this result immediately yields a characterization of closed regular languages.

Theorem 3.57. *A regular language $L \subseteq A^*$ is closed in the profinite group topology if and only if it satisfies condition* (b) *(or* (c)*).*

4 Algorithms

4.1 The membership problem

It is an easy task to decide whether a regular language L is accepted by a bideterministic automaton. According to Theorem 3.5 we just compute the minimal DFA $\mathcal{D}_L$ and check for forbidden configurations of type `FC2` as well as the number of final states. There are polynomial time algorithms to compute $\mathcal{D}_L$ from any automaton accepting L in polynomial time w.r.t. the number of states, see for instance Hopcroft's minimization algorithm [7], which even has a runtime of $\mathcal{O}(n \log n)$. Clearly, the search for forbidden configurations can be done in polynomial time as well.

However, since we demonstrated in Example 3.6 that the minimal DFA of a reversible language does not need to be reversible, deciding whether a regular language is reversible is not that straightforward, albeit possible. In fact, using the algebraic characterization given in Section 3.2, Pin [10] derived an algorithm to solve this problem in polynomial time.

It roughly works by searching the minimal DFA for certain configurations. Those configurations involve entire words as opposed to just letters, as seen in the definition of reversible automata. Therefore it is necessary to give a more thorough definition.

Definition 4.1. A *path* in a finite automaton is a sequence of consecutive transitions. Given a word $w = a_1 \cdots a_n$, and a path $q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \;\cdots\; q_{n-1} \xrightarrow{a_n} q_n$, we also shortly write $q_0 \overset{w}{\rightsquigarrow} q_n$.

Definition 4.2. Let $\mathcal{A} = (Q, A, \cdot)$ be a DFA.[1] We define an infinite labelled graph $G(\mathcal{A}) = (Q, E)$, with $E = \{(q, w, q \cdot w) \mid q \in Q, w \in A^+\}$ being the infinite set of paths in $\mathcal{A}$. A *configuration* present in $\mathcal{A}$ is a labelled subgraph of $G(\mathcal{A})$.

We will later use the following construction to efficiently search for configurations in a DFA.

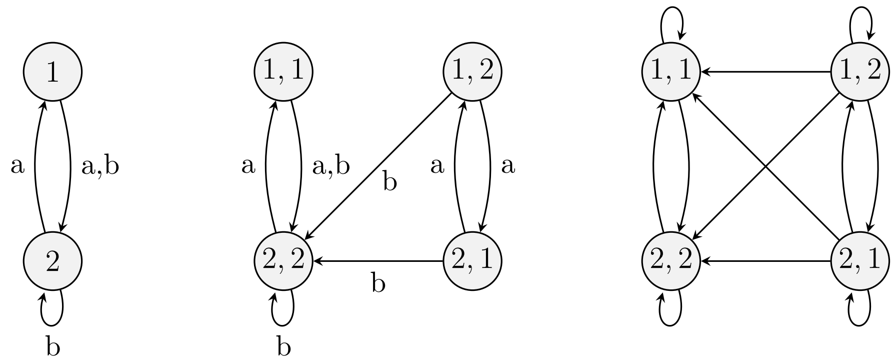
Definition 4.3. Let $\mathcal{A} = (Q, A, \cdot)$ be a DFA. For every positive integer k we define the *direct product* $\mathcal{A}^k = (Q^k, A, *)$, where $(q_1, \ldots, q_k) * a = (q_1 \cdot a, \ldots, q_k \cdot a)$. Furthermore, we denote by $G_k(\mathcal{A})$ the transitive closure of the unlabelled directed graph defined by $\mathcal{A}^k$.

By Theorem 3.46, a regular language $L \subseteq A^*$ is reversible if and only if

(a) the idempotents of $M(L)$ commute,

(b) $\forall x, u, y \in A^* : (xu^+y \subseteq L \implies xy \in L)$.

[1] We omit the initial and final states in the signature, whenever they are irrelevant in the current situation.

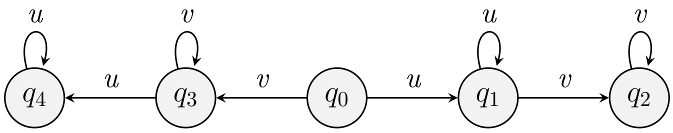


(a) $\mathcal{A}$ (b) $\mathcal{A}^2$ (c) $G_2(\mathcal{A})$

Figure 4.1: Example of the construction given in Definition 4.3.

We will now show that both these conditions are equivalent to the absence of certain configurations in the minimal DFA of L.

Theorem 4.4. *Let $L \subseteq A^*$ be a regular language. The idempotents of $M(L)$ commute if and only if $\mathcal{D}_L = (Q, A, \cdot, \{q_i\}, F)$ contains no configuration of the form*



with $u, v \in A^+$ and $q_2 \neq q_4$.

Proof. We start with the left-to-right implication. Assume that the idempotents of $M(L)$ commute and consider a configuration of the form above. By Lemma 3.22, since $M(L)$ is finite, there is an integer $n > 0$ such that $\eta(u^n)$ and $\eta(v^n)$ are both idempotent. Hence, they commute in $M(L) \simeq M(\mathcal{D}_L)$, i.e., $q \cdot u^n v^n = q \cdot v^n u^n$ for every $q \in Q$. In particular, we obtain

$$q_2 = q_0 \cdot u^n v^n = q_0 \cdot v^n u^n = q_4.$$

Conversely, assume that the above configuration does not occur in $\mathcal{D}_L$. Let $e, f \in M(L)$ be idempotent, where w.l.o.g. $e, f \neq [\varepsilon]$. Then we can choose words $u, v \in A^+$ with $\eta(u) = e$ and $\eta(v) = f$. Now let $q_0 \in Q$. We need to show $q_0 \cdot uv = q_0 \cdot vu$. To this end, define

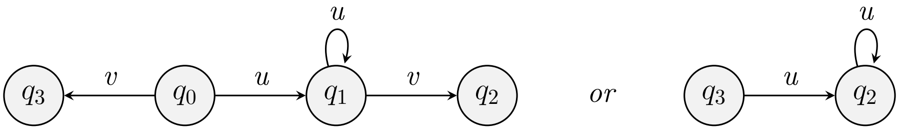
$$q_1 = q_0 \cdot u, \quad q_2 = q_1 \cdot v, \quad q_3 = q_0 \cdot v, \quad q_4 = q_3 \cdot u.$$

Since τ_u and τ_v are idempotent in $M(\mathcal{D}_L)$, it follows

$$\begin{aligned} q_1 \cdot u &= q_0 \cdot u^2 = q_0 \cdot u = q_1, \\ q_2 \cdot v &= q_1 \cdot v^2 = q_1 \cdot v = q_2, \\ q_3 \cdot v &= q_0 \cdot v^2 = q_0 \cdot v = q_3, \\ q_4 \cdot u &= q_3 \cdot u^2 = q_3 \cdot u = q_4. \end{aligned}$$

Our assumption implies $q_2 = q_4$, otherwise we would have a forbidden configuration. Hence $q_0 \cdot uv = q_2 = q_4 = q_0 \cdot vu$, which means that e and f commute in $M(L)$. □

Theorem 4.5. *Let $L \subseteq A^*$ be a regular language. Then L satisfies condition* (b) *if and only if $\mathcal{D}_L = (Q, A, \cdot, \{q_i\}, F)$ contains no configuration of the form*



with $u, v \in A^+$, $q_2 \in F$ and $q_3 \notin F$.

Proof. First assume that (b) holds. If the left configuration exists in $\mathcal{D}_L$, then there is a word $w \in A^*$ such that $q_i \cdot w = q_0$, since every state of $\mathcal{D}_L$ is accessible. It follows

$$q_i \cdot wu^nv = q_0 \cdot u^nv = q_1 \cdot v = q_2 \in F,$$

and therefore $wu^nv \in L$ for every integer $n > 0$. Condition (b) implies $wv \in L$, which in turn yields $q_3 = q_0 \cdot v = q_i \cdot wv \in F$. The proof for the right configuration is virtually the same.

Conversely, assume that $\mathcal{D}_L$ contains none of the configurations above. To show condition (b), let $x, u, y \in A^*$ with $xu^+y \subseteq L$. By Lemma 3.22, there is an integer $n > 0$ such that $\eta(u^n)$ is idempotent in $M(L)$. Let $w = u^n$. We consider two cases.

- If $y = \varepsilon$, then we set $q_3 = q_i \cdot x$ and $q_2 = q_3 \cdot w$. Since τ_w is idempotent in $M(\mathcal{D}_L)$, we obtain $q_2 = q_3 \cdot w^2 = q_2 \cdot w$. Moreover, $xw = xu^n\varepsilon \in L$ and therefore $q_2 = q_i \cdot xw \in F$. Hence, $q_i \cdot x = q_3 \in F$, otherwise $\mathcal{D}_L$ would contain the right configuration. It follows $xy = x \in L$ and (b) holds.
- The case $y \neq \varepsilon$ is similar: We set $q_0 = q_i \cdot x$, $q_1 = q_0 \cdot w = q_0 \cdot w^2 = q_1 \cdot w$ and $q_2 = q_1 \cdot y$. Then $q_2 = q_i \cdot xwy \in F$, since $xwy \in L$. Consequently, $q_i \cdot xy = q_0 \cdot y \in F$, otherwise $\mathcal{D}_L$ would contain the left configuration. It follows $xy \in L$ and (b) holds as well. □

The two results above show that the reversibility of a regular language can be decided by searching for the above configurations in the minimal DFA. We will now prove that this procedure can be run in polynomial time.

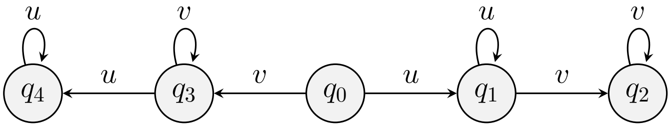
Theorem 4.6. *Let $L \subseteq A^*$ be a regular language and let $\mathcal{A}$ be a DFA accepting L. There is a polynomial time algorithm (w.r.t. the size of $\mathcal{A}$) that decides the reversibility of L.*

Proof. The algorithm consists of multiple steps:

(1) First, we compute the minimal DFA $\mathcal{D}_L$. As already mentioned, this can be done in polynomial time, for instance by running Hopcroft's algorithm. We denote by n the number of states of $\mathcal{D}_L$.

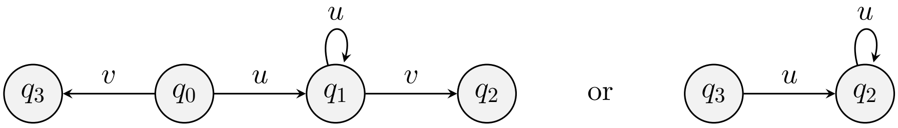
(2) Next, we construct $G_2(\mathcal{D}_L)$ and $G_4(\mathcal{D}_L)$. For any fixed positive integer k, the unlabelled directed graph defined by the direct product $\mathcal{D}_L^k$ has n^k vertices and can clearly be computed in polynomial time. Now, there are several options for computing its transitive closure $G_k(\mathcal{D}_L)$, for instance the Floyd-Warshall algorithm with unit weights or just repeated depth-first search from each vertex. They all run in polynomial time.

(3) Now we test whether the idempotents of $M(L)$ commute. By Theorem 4.4, we need to search $\mathcal{D}_L$ for configurations of the form



with $q_2 \neq q_4$. This can be done efficiently by searching $G_4(\mathcal{D}_L)$ for edges of the form $((q_0, q_1, q_3, q_4), (q_1, q_1, q_4, q_4))$ and $((q_0, q_1, q_2, q_3), (q_3, q_2, q_2, q_3))$ with $q_2 \neq q_4$.

(4) Similarly, we test whether (b) holds. By Theorem 4.5, we need to search $\mathcal{D}_L$ for configurations of the form



with $q_2 \in F$ and $q_3 \notin F$. The left configuration corresponds to edges of the form $((q_0, q_1), (q_1, q_1))$ and $((q_0, q_1), (q_3, q_2))$ in $G_2(\mathcal{D}_L)$ with $q_2 \in F$ and $q_3 \notin F$, whereas the right configuration corresponds to an edge of the form $((q_3, q_2), (q_2, q_2))$ with $q_2 \in F$ and $q_3 \notin F$. □

4.2 Construction of reversible automata

Unfortunately, the algorithm presented in the previous section only solves the membership problem and provides no indication on how to construct a reversible automaton accepting a given reversible language. Such a construction was first published by S. Lombardy [8]. The idea is to compute a so-called *quasi-reversible* automaton from the minimal DFA, which can then easily be transformed into a reversible automaton, which accepts the same language.

The resulting quasi-reversible automaton can have up to 2^n states, where n is the number of states of the minimal DFA. Moreover, the algorithm runs in exponential time.

Building on the same ideas, P. García, M. Vázquez de Parga and D. López [5] improved this construction considerably. Not only does their algorithm return a quasi-reversible automaton with at most n states, but it also runs in polynomial time. Before we describe the procedure, we need to establish some new concepts.

Definition 4.7. Let $L \subseteq A^*$ be a regular language. The *universal automaton* of L is defined as $\mathcal{U}_L = (Q, A, E, I, F) = (Q, A, \delta, I, F)$, where

$$\begin{aligned} Q &= \{u_1^{-1}L \cap \cdots \cap u_k^{-1}L \mid k \geq 0, u_1, \ldots, u_k \in A^*\}, \\ I &= \{q \in Q \mid q \subseteq L\}, \\ F &= \{q \in Q \mid \varepsilon \in q\}, \\ E &= \{(u^{-1}L, a, q) \mid u \in A^*, a \in A, q \subseteq (ua)^{-1}L\}. \end{aligned}$$

We will also write E as a function $\delta(u^{-1}L, a) = \{q \in Q \mid q \subseteq (ua)^{-1}L\}$, which – as usual – extends naturally from letters to words.

Definition 4.8. Let $\mathcal{A} = (Q, A, \delta, I, F)$ be a finite automaton and $q \in Q$. We call

$$R_q = \{w \in A^* \mid \delta(q, w) \cap F \neq \emptyset\}$$

the *right language* of q.

Definition 4.9. Let $L \subseteq A^*$ be a regular language. A *residual finite state automaton* (RFSA) for L is a finite automaton $\mathcal{A}$ with the property that every right language is equal to some left quotient, i.e., for every $q \in Q$ there is a word $u \in A^*$ such that $R_q = u^{-1}L$.

Example 4.10. By definition, every trim DFA is a RFSA. Another special case is the minimal DFA $\mathcal{D}_L$, since the states are exactly the left quotients, in particular, we have $R_{u^{-1}L} = u^{-1}L$.

Definition 4.11. Let $L \subseteq A^*$ be a regular language. The *saturated* RFSA of $\mathcal{D}_L$ is defined as the subautomaton of $\mathcal{U}_L$ induced by the set of states of $\mathcal{D}_L$. We will denote it by $\mathcal{S}_L$.

This naming is indeed justified:

Proposition 4.12. *Let $L \subseteq A^*$ be a regular language. Then $\mathcal{S}_L$ is an RFSA.*

Proof. The states of $\mathcal{S}_L$ are exactly the left quotients of L. Hence, we claim $R_{u^{-1}L} = u^{-1}L$ for every $u \in A^*$. Indeed:

$$\begin{aligned} w \in R_{u^{-1}L} &\iff \delta(u^{-1}L, w) \cap F \neq \emptyset \\ &\iff \exists v \in A^* : v^{-1}L \in F \text{ and } v^{-1}L \in \delta(u^{-1}L, w) \\ &\iff \exists v \in A^* : \varepsilon \in v^{-1}L \text{ and } v^{-1}L \subseteq (uw)^{-1}L \\ &\iff \varepsilon \in (uw)^{-1}L \\ &\iff uw \in L \\ &\iff w \in u^{-1}L. \end{aligned}$$

□

The saturated RFSA of the minimal DFA of a reversible language will play a crucial role in the construction of a reversible automaton. It usually contains more transitions and initial states than the minimal DFA, but still accepts the same language.

Proposition 4.13. *Let $L \subseteq A^*$ be a regular language. Then $|\mathcal{S}_L| = |\mathcal{D}_L|$.*

Proof. By definition, $|\mathcal{D}_L| \subseteq |\mathcal{S}_L|$. For other implication, let $w \in |\mathcal{U}_L|$. We need to show that $w \in L$.

Let $\mathcal{U}_L = (Q, A, \delta, I, F)$. Then there are words $u, v \in A^*$ such that $u^{-1}L \in I$, $v^{-1}L \in F$ and $v^{-1} \in \delta(u^{-1}L, w)$, and therefore $v^{-1} \subseteq (uw)^{-1}L$. Now, the definitions of I and F imply $u^{-1}L \subseteq L$ and $\varepsilon \in v^{-1}L$. Putting that all together, we obtain

$$\varepsilon \in v^{-1}L \subseteq (uw)^{-1}L = w^{-1}(u^{-1}L) \subseteq w^{-1}L,$$

and thus $w \in L$. □

Definition 4.14. A *strongly connected component* (SCC) of a finite automaton is a maximal subautomaton containing at least one transition, where all states are strongly connected, i.e., for all states q, p there is a path from p to q and a path from q to p.

Note that this definition deviates from the analogue notion for directed graphs. By our definition, the SCCs of a finite automaton do not necessarily form a partition of the states. If there are states that are not strongly connected to any other state, they belong to no SCC.

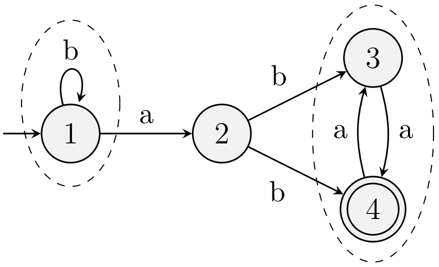
The final piece of preparation, before we move on to describing the algorithm, is the already mentioned concept of quasi-reversible automata, as introduced in [8].

Definition 4.15. A finite automaton $\mathcal{A}$ is called *quasi-reversible*, if no transition occurring in a forbidden configuration of type `FC1` or `FC2` belongs to a SCC. To put it differently, $\mathcal{A}$ is quasi-reversible, if it satisfies the following two conditions:

(1) Given two transitions $(r, a, p), (r, a, q)$ with $p \neq q$, none of them belongs to a SCC.

(2) Given two transitions $(p, a, r), (q, a, r)$ with $p \neq q$, none of them belongs to a SCC.

Example 4.16. The following automaton is not reversible, as it contains one forbidden configuration of type `FC1`, namely $3 \xleftarrow{b} 2 \xrightarrow{b} 4$. However, it is quasi-reversible since neither $(2, b, 3)$ nor $(2, b, 4)$ belongs to any SCC (dashed ellipses).



Proposition 4.17. *Let $\mathcal{A} = (Q, A, E, I, F)$ be a quasi-reversible automaton. Then one can construct a reversible automaton $\mathcal{B}$ with $|\mathcal{A}| = |\mathcal{B}|$.*

Proof. We prove the statement by induction on the number of forbidden configurations in $\mathcal{A}$. If $\mathcal{A}$ contains no forbidden configurations, it is already reversible and we are done.

If there are $n+1$ forbidden configurations, choose one of them, with $e_1, e_2 \in E$ being its two "critical" transitions. Since $\mathcal{A}$ is quasi-reversible, neither e_1 nor e_2 belongs to any SCC. Thus, there exists no path containing both e_1 and e_2. As a result, $|\mathcal{A}|$ is a union of two languages: those words that can be accepted without using e_1 and those words that can be accepted without using e_2. Those two languages are respectively accepted by $\mathcal{A}_1 = (Q, A, E \setminus \{e_1\}, I, F)$ and $\mathcal{A}_2 = (Q, A, E \setminus \{e_2\}, I, F)$, i.e., $|\mathcal{A}| = |\mathcal{A}_1| \cup |\mathcal{A}_2|$.

Now, $\mathcal{A}_1$ and $\mathcal{A}_2$ are quasi-reversible automata with n forbidden configurations each. By the induction hypothesis, they can both be transformed into a reversible automaton accepting the same language. Hence, the statement follows from the simple fact, that the finite union of reversible automata is a reversible automaton again. □

Next, we define two sets of "undesired" transitions.

Definition 4.18. Let $\mathcal{A} = (Q, A, E, I, F)$ be a finite automaton. We define two subsets of E: We say that a transition (r, a, p) is in E_1 if and only if there is another transition (r, a, q) with $p \neq q$ that belongs to a SCC. Similarly, a transition (p, a, r) is in E_2 if and only if there is another transition (q, a, r) with $p \neq q$ that belongs to a SCC.

Deleting those transitions from a given automaton clearly transforms it into a quasi-reversible automaton. However, the resulting automaton will usually accept a different language. Using the algebraic characterization of reversible languages, one can show that this is not the case for the saturated RFSA of $\mathcal{D}_L$ for a reversible language L.

Theorem 4.19 ([5])**.** *Let $L \subseteq A^*$ be a reversible language and let $\mathcal{S}_L = (Q, A, E, I, F)$ be the saturated RFSA of $\mathcal{D}_L$. Then $\mathcal{Q}_L = (Q, A, E \setminus (E_1 \cup E_2), I, F)$ is a quasi-reversible automaton and $|\mathcal{Q}_L| = |\mathcal{S}_L|$.*

This result already provides a way to compute a quasi-reversible automaton that accepts a given reversible language. Verifying the claimed polynomial runtime requires an efficient way to decide whether a regular language is contained in another regular language.

Lemma 4.20. *Let $L_1, L_2 \subseteq A^*$ be two regular languages that are respectively accepted by the DFAs $\mathcal{A}_1 = (Q, A, \cdot_1, \{q_1\}, F_1)$ and $\mathcal{A}_2 = (Q, A, \cdot_2, \{q_2\}, F_2)$. Then one can decide in polynomial time w.r.t. $|Q|$, whether L_1 is contained in L_2.*

Proof. First, note that $L_1 \subseteq L_2$ if and only if $L_1 \cap L_2^c = \emptyset$. Clearly, L_2^c is accepted by the automaton $\mathcal{A}_2^c = (Q, A, \cdot_2, \{q_2\}, Q \setminus F_2)$. Furthermore, the intersection of two regular languages is accepted by the direct product of their respective automata. In particular, $L_1 \cap L_2^c$ is accepted by

$$\mathcal{A}_1 \times \mathcal{A}_2^c = (Q \times Q, A, *, \{(q_1, q_2)\}, F_1 \times (Q \setminus F_2)),$$

where $(q, p) * a = (q \cdot_1 a, p \cdot_2 a)$. Now one simply needs to check if this automaton accepts any word, for instance by performing a depth-first search. □

Theorem 4.21. *Let $L \subseteq A^*$ be a reversible language and let n be the number of states of $\mathcal{D}_L$. Then there is a polynomial time algorithm that transforms $\mathcal{D}_L$ into a quasi-reversible automaton accepting L with at most n states.*

Proof. First, we compute $\mathcal{S}_L$. Recall that both $\mathcal{D}_L$ and $\mathcal{S}_L$ contain the same set of states $Q = \{u^{-1}L \mid u \in A^*\}$. In order to compute the transition relation E and the initial states of $\mathcal{S}_L$, we need to know the subset relation on $Q \times Q$. This can be achieved by applying Lemma 4.20 to each of the n^2 different pairs of left quotients, resulting in a polynomial runtime. A rough upper bound is $\mathcal{O}(n^4)$, see [5].

Next, we compute $\mathcal{Q}_L$ by deleting all the transitions occurring in E_1 or E_2. To obtain these two subsets of E, we require the SCCs of $\mathcal{S}_L$, which can even be computed in $\mathcal{O}(n \log n)$, see [3]. Finding all forbidden configurations in $\mathcal{S}_L$ is a procedure that will depend on the data structure. However, even a naive implementation, which iterates for every state through all incident edges, is clearly polynomial.

Hence, the algorithm as a whole is polynomial. □

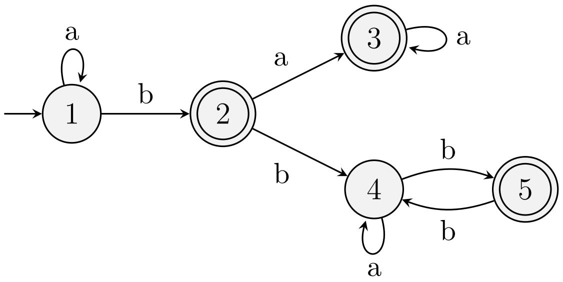
To conclude this work, we demonstrate the full construction of a reversible automaton that accepts a given reversible language, by means of an example.

Example 4.22. Consider the language $L = (a + bb)^*b + a^*ba^*$ over $A = \{a, b\}$.

(1) The left quotients of L are given by $L_1 \coloneqq L$ and

$$\begin{aligned} a^{-1}L_1 &= L_1, & b^{-1}L_3 &= \emptyset, \\ b^{-1}L_1 &= b(a+bb)^*b + a^* =: L_2, & a^{-1}L_4 &= L_4, \\ a^{-1}L_2 &= a^* =: L_3, & b^{-1}L_4 &= b(a+bb)^*b + \varepsilon =: L_5, \\ b^{-1}L_2 &= (a+bb)^*b =: L_4, & a^{-1}L_5 &= \emptyset, \\ a^{-1}L_3 &= L_3, & b^{-1}L_5 &= L_4. \end{aligned}$$

We will shortly denote the states by $1 = L_1, \ldots, 5 = L_5$. The empty word is contained in $2, 3$ and 5, which therefore constitute the final states. Thus, $\mathcal{D}_L = (Q, A, \cdot, \{1\}, \{2, 3, 5\})$ is given by the following automaton:

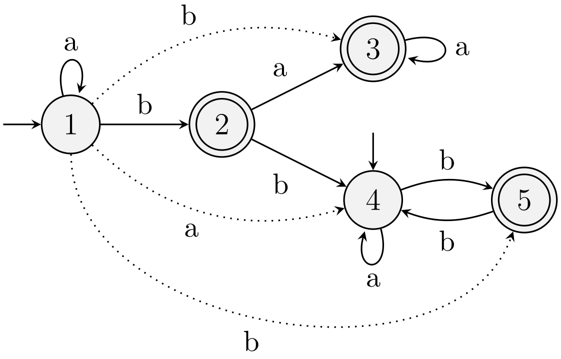


(2) The simplicity of this example allows us to determine the subset relation on $Q \times Q$ by just looking at the regular expressions: The states 1 and 2 are disjoint, 4 is contained in 1, and $3 \uplus 5 = 2$. Consequently, to obtain $\mathcal{S}_L$, the state 4 must be added to

the set of initial states. The set E of transitions contains all the transitions of $\mathcal{D}_L$. Additionally, we have

$$\begin{aligned}(1,a,1) \in E \text{ and } 4 \subseteq 1 &\implies (1,a,4) \in E,\\ (1,b,2) \in E \text{ and } 3 \subseteq 2 &\implies (1,b,3) \in E,\\ (1,b,2) \in E \text{ and } 5 \subseteq 2 &\implies (1,b,5) \in E,\end{aligned}$$

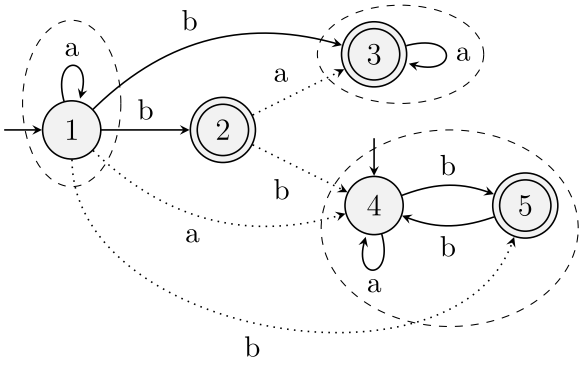
thus $\mathcal{S}_L$ is the automaton below:



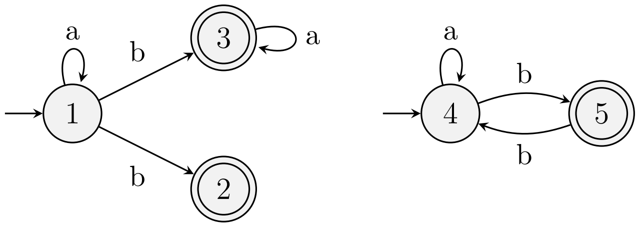
(3) Next, we draw the SCCs and then compute E_1 and E_2. For instance, $(2,a,3) \in E_2$, since $(3,a,3)$ belongs to a SCC. In total we have

$$\begin{aligned}E_1 &= \{(1,a,4)\},\\ E_2 &= \{(1,a,4),(1,b,5),(2,a,3),(2,b,4)\}.\end{aligned}$$

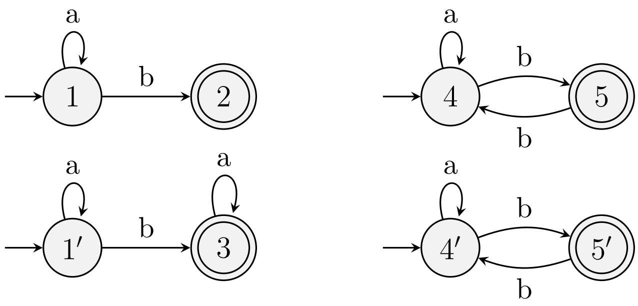
These transitions will be deleted and are drawn dotted:



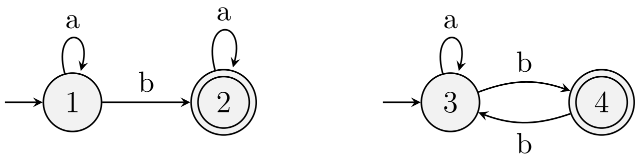
(4) Deleting the states in E_1 and E_2 now yields the quasi-reversible automaton $\mathcal{Q}_L$, as depicted below. $\mathcal{Q}_L$ is clearly not reversible, as the transitions $(1,b,2)$ and $(1,b,3)$ form a forbidden configuration of type `FC1`.



(5) Following the inductive proof of Proposition 4.17, we can finally transform $\mathcal{Q}_L$ into a reversible automaton that accepts L. We just split $\mathcal{Q}_L$ into a union of two new automata, one without $(1, b, 2)$ and one without $(1, b, 3)$ and technically obtain the following reversible automaton:



Obviously, the splitting procedure generates a lot of redundancy, but in theory the algorithm ends at this point. Nevertheless, the top two out of the four connected components above can be deleted without altering the accepted language. Thus, L is also accepted by the following reversible automaton, which is even smaller than $\mathcal{D}_L$:



Bibliography

[1] C. J. Ash and T. E. Hall. Finite semigroups with commuting idempotents. *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics*, 43:81 – 90, 1987.

[2] J. Berstel. *Transductions and Context-Free Languages.* Vieweg & Teubner Verlag, 1979.

[3] R. Bloem, H. Gabow, and F. Somenzi. An algorithm for strongly connected component analysis in $n \log n$ symbolic steps. volume 28, 09 2000.

[4] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups, Volume I.* Number 7 in Mathematical Surveys. American Mathematical Society, Providence, Rhode Island, 1961.

[5] P. García, M. Vázquez de Parga, and D. López. On the efficient construction of quasi-reversible automata for reversible languages. *Inf. Process. Lett.*, 107(1):13–17, 2008.

[6] S. Hetzl. Automata and Formal Languages. `https://www.dmg.tuwien.ac.at/hetzl/teaching/afl_2023.pdf`, 2023. [accessed on 08.04.2023].

[7] J. Hopcroft. An $n \log n$ algorithm for minimizing states in a finite automaton. In Z. Kohavi and A. Paz, editors, *Theory of Machines and Computations*, pages 189–196. Academic Press, 1971.

[8] S. Lombardy. On the construction of reversible automata for reversible languages. In *29th International Colloquium on Automata, Languages and Programming (ICALP 2002)*, volume 2380 of *LNCS*, pages 170–182, Malaga, Spain, July 2002. Springer.

[9] J.-É. Pin. Topologies for the free monoid. *Journal of Algebra*, 137:297–337, 1991.

[10] J.-É. Pin. On reversible automata. In I. Simon, editor, *Proceedings of the first LATIN conference*, Lecture Notes in Computer Science 583, pages 401–416, Saõ-Paulo, Brazil, 1992. Springer.

[11] J.-É. Pin. Mathematical Foundations of Automata Theory. `https://www.irif.fr/~jep/PDF/MPRI/MPRI.pdf`, 2022. [accessed on 08.04.2023].

[12] C. Reutenauer. Une topologie du monoide libre. *Semigroup forum*, 18:33–50, 1979.