Minimal and Reduced Reversible Automata[*]

Giovanna J. Lavado   Giovanni Pighizzini   Luca Prigioniero

Dipartimento di Informatica
Università degli Studi di Milano, Italy
lavado@di.unimi.it − pighizzini@di.unimi.it − prigioniero@di.unimi.it

Abstract. A condition characterizing the class of regular languages which have several nonisomorphic minimal reversible automata is presented. The condition concerns the structure of the minimum automaton accepting the language under consideration. It is also observed that there exist reduced reversible automata which are not minimal, in the sense that all the automata obtained by merging some of their equivalent states are irreversible. Furthermore, a sufficient condition for the existence of infinitely many reduced reversible automata accepting a same language is given. It is also proved that, when the language is accepted by a unique minimal reversible automaton (that does not necessarily concide with the minimum deterministic automaton), then no other reduced reversible automata accepting it can exist.

Keywords: reversible automata, minimal automata, regular languages

1   Introduction

A device is said to be *reversible* when each configuration has exactly one predecessor and one successor, thus implying that there is no loss of information during the computation. On the other hand, as observed by Landauer, logical irreversibility is associated with physical irreversibility and implies a certain amount of heat generation [Lan61]. In order to avoid such a power dissipation and, hence, to reduce the overall power consumption of computational devices, the possibility of realizing reversible machines looks appealing.

A lot of work has been done to study reversibility in different computational devices. Just to give a few examples in the case of general devices as Turing machines, Bennet proved that each machine can be simulated by a reversible one [Ben73], while Lange, McKenzie, and Tapp proved that each deterministic machine can be simulated by a reversible machine which uses the same amount of space [LMT00]. As a corollary, in the case of a constant amount of space, this implies that each regular language is accepted by a *reversible two-way deterministic finite automaton*. Actually, this result was already proved by Kondacs and Watrous [KW97].

However, in the case of *one-way* automata, the situation is different. In fact, as shown by Pin, the regular language a^*b^* cannot be accepted by any reversible automaton [Pin92].[1] So the class of languages accepted by *reversible automata* is a proper subclass of the class of regular languages. Actually, there are some different notions of reversible automata in the literature. In 1982, Angluin introduced reversible automata in algorithmic learning theory, considering devices having only one initial and only one final state [Ang82]. On the other hand, the devices considered in [Pin92], besides a set of final states, can have multiple initial states, hence they can take a nondeterministic decision at the beginning of the computation. An extension which allows to consider nondeterministic transitions, without changing the class of accepted languages, has been considered by Lombardy [Lom02], introducing and investigating *quasi reversible automata*. Classical automata, namely automata with a single initial state and a set of final states, have been considered in the works by Holzer, Jakobi, and Kutrib [Kut14, HJK15, Kut15]. In particular, in [HJK15] the authors gave a characterization of regular languages which are accepted by reversible automata. This characterization is given in terms of the structure of the minimum deterministic automaton. Furthermore, they provide an algorithm that, in the case the language is acceptable by a reversible automaton, allows to transform the minimum automaton into an equivalent reversible automaton, which in the worst case is exponentially larger than the given minimum automaton. In spite of that, the resulting automaton is minimal, namely there are no reversible automata accepting the same language with a smaller number of states. However, it is not necessarily unique, in fact there could exist different reversible automata with the same number of states accepting the same language.

In this paper we continue the investigation of minimality in reversible automata. Our first result is a condition that characterizes languages having several different minimal reversible automata. Even this condition is on the structure of the transition graph of the minimum automaton accepting the language under consideration: there exist different minimal reversible automata accepting a reversible language L if and only if there are transitions on different letters entering in a same state in the "irreversible part" of the minimum automaton for L. We prove that such condition is always satisfied each time the "irreversible part" of the minimum automaton contains a loop.

We also observe that there exist reversible automata which are not minimal but they are reduced, in the sense that when we try to merge some of their equivalent states we always obtain an irreversible automaton. Investigating this phenomenon more into details, we are able to find a language for which there exist arbitrarily large, and hence infinitely many reduced reversible automata. Indeed, we present a general construction that allows to obtain arbitrarily large reversible automata for all languages whose minimum deterministic automata satisfy a further structural condition besides the one given in [HJK15]. As a consequence of such condition, for each reversible language whose minimum deterministic automaton contains a loop in the "irreversible part", it is possible to construct infinitely many arbitrarily large reduced reversible automata. We know that our condition is not necessary and we leave as an open problem to find a characterization of the class of the languages having infinitely many reduced reversible automata.

---

[1]From now on, we will consider only *one-way automata*. Hence we will omit to specify "one-way" all the times.

Finally, in the last part of the paper we prove that when the minimal reversible automaton accepting a language is unique, there does not exist any other equivalent reduced reversible automaton. However, such unique minimal reversible automaton can be larger than the minimum automaton accepting the same language.

2 Preliminaries

In this section we recall some basic definitions and results useful in the paper. We assume the reader is familiar with standard notions from automata and formal language theory (see, e.g., [HU79]). Given a set S, let us denote by $\#S$ its cardinality and by 2^S the family of all its subsets. Given an alphabet Σ, $|w|$ denotes the length of a string $w \in \Sigma^*$ and ε the empty string.

A *deterministic finite automaton* (DFA for short) is a tuple $A = (Q, \Sigma, \delta, q_I, F)$, where Q is the finite set of *states*, Σ is the *input alphabet*, $q_I \in Q$ is the *initial state*, $F \subseteq Q$ is the set of *accepting states*, and $\delta : Q \times \Sigma \to Q$ is the partial *transition function*. The *language accepted* by A is $L(A) = \{w \in \Sigma^* \mid \delta(q_I, w) \in F\}$.

The *reverse* transition function of A is a function $\delta^R : Q \times \Sigma \to 2^Q$, with $\delta^R(p, a) = \{q \in Q \mid \delta(q, a) = p\}$.

A state $p \in Q$ is *useful* if p is *reachable*, i.e., there is $w \in \Sigma^*$ such that $\delta(q_I, w) = p$, and *productive*, i.e., there is $w \in \Sigma^*$ such that $\delta(p, w) \in F$. In this paper we only consider automata with all useful states.

We say that two states $p, q \in Q$ are *equivalent* if and only if for all $w \in \Sigma^*$, $\delta(p, w) \in F$ exactly when $\delta(q, w) \in F$. When $p \neq q$ are equivalent states, we can reduce the size of the automaton by "merging" p and q. This would imply to merge all the states reachable from p and q by reading a same string, namely the states $\delta(p, w)$ and $\delta(q, w)$, for $w \in \Sigma^*$.

Two automata A and A' are said to be *equivalent* if they accept the same language, i.e., $L(A) = L(A')$.

Given two DFAs $A = (Q, \Sigma, \delta, q_I, F)$ and $A' = (Q', \Sigma, \delta', q_I', F')$, a *morphism* φ from A to A', in symbols $\varphi : A \to A'$, is a function $\varphi : Q \to Q'$ such that:

- $\varphi(q_I) = q_I'$,

- $\varphi(\delta(q, a)) = \delta'(\varphi(q), a)$, and

- $q \in F$ if and only if $\varphi(q) \in F'$,

for $q \in Q$, $a \in \Sigma$.

Notice that if there exists a morphism $\varphi : A \to A'$ then it is *unique* and, for $x, y \in \Sigma^*$, $\delta(q_I, x) = \delta(q_I, y)$ implies $\delta'(q_I', x) = \delta'(q_I', y)$, thus implying that A and A' are equivalent. We can observe that since in all automata we are considering all the states are useful, there exists the morphism $\varphi : A \to A'$ if and only if the automaton A' can be obtained

from A after merging all pairs of states p, q of A, with $\varphi(p) = \varphi(q)$ (and possibly renaming the states). Hence $\varphi^{-1}(s)$ is the set of states of A which are merged in the state s of A', and the number of states of A' cannot exceed that of A.

We point out that the notion of morphism is strictly related to the Myhill-Nerode equivalence relation [Myh57, Ner58] in the following sense. If R_A and $R_{A'}$ are the Myhill-Nerode relations associated with DFAs A and A', then $R_{A'}$ is a refinement of R_A if and only if there is a morphism from A to A'.

Let $\mathcal{C}$ be a family of DFAs and $A \in \mathcal{C}$. We consider the following notions:

- The automaton A is *reduced* in $\mathcal{C}$ if for each morphism $\varphi : A \to A'$, either φ is an isomorphism (i.e., A and A' are the same automaton up to a renaming of states) or the automaton A' does not belong to $\mathcal{C}$, that is, every automaton obtained from A by merging some equivalent states does not belong to $\mathcal{C}$.

- The automaton A is *minimal* in $\mathcal{C}$ if and only if each automaton in $\mathcal{C}$ has at least as many states as A.

- The automaton A is the *minimum* in $\mathcal{C}$ if and only if, for each automaton A' in $\mathcal{C}$, there exists a morphism $\varphi : A' \to A$.

Notice that each minimal automaton in a family $\mathcal{C}$ is reduced. Furthermore, if $\mathcal{C}$ contains a minimum automaton M, then M is also the only minimal and the only reduced automaton in $\mathcal{C}$. This happens, for instance, when $\mathcal{C}$ is the family of all DFAs accepting a given regular language L. However, a family $\mathcal{C}$ which does not have a minimum automaton, could contain reduced automata which are not minimal, as in some of the cases that will be presented in the paper.[2]

A *strongly connected component* (SCC) C of a DFA $A = (Q, \Sigma, \delta, q_I, F)$ is a maximal subset of Q such that in the transition graph of A there exists a path between every pair of states in C. A SCC consisting of a single state q, *without* a looping transition, is said to be *trivial*. Otherwise C is *nontrivial* and, for each state $q \in C$, there is a string $w \in \Sigma^+$ such that $\delta(q, w) = q$.

We consider a partial order $\preceq$ on the set of SCCs of A, such that, for two such components C_1 and C_2, $C_1 \preceq C_2$ when either $C_1 = C_2$ or no state in C_1 can be reached from a state in C_2, but a state in C_2 is reachable from a state in C_1. We write $C_1 \npreceq C_2$ when $C_1 \preceq C_2$ is false, namely, $C_1 \neq C_2$ and either $C_2 \preceq C_1$ or C_1 and C_2 are incomparable.

---

[2]In the conference version of the paper [LPP16], we gave a weaker definition, by saying that A is minimum if it is the *unique* minimal automaton in $\mathcal{C}$. As we will show later in the paper (see Thm. 6.2), for the models we are considering the two notions are equivalent. However, in general, this is not true if we do not make any assumption about the family $\mathcal{C}$. For example, in $\mathcal{C} = \{A \mid A$ is a DFA s.t. $L(A) = a^*$ or $L(A) = (ab)^*\}$, the one state DFA accepting a^* is the only minimal automaton, while the two state DFA accepting $(ab)^*$ is reduced. Hence, the family $\mathcal{C}$ does not have a minimum automaton.

3   Reversible Automata

This section is devoted to recall basic notions and results related to reversible automata and to present some preliminary lemma that will be used in the paper.

Given a DFA $A = (Q, \Sigma, \delta, q_I, F)$, a state $r \in Q$ is said to be *irreversible* when $\#\delta^R(r, a) > 1$ for some $a \in \Sigma$, i.e., there are at least two transitions on the same letter entering r, otherwise r is said to be *reversible*. The DFA A is said to be *irreversible* if it contains at least one irreversible state, otherwise A is *reversible* (REV-DFA for short).

According to the notion of reversible and irreversible states, each DFA can be split in two parts: the *reversible part* and the *irreversible part*. Roughly speaking, the irreversible part consists of all states that can be reached with a path which starts in an irreversible state, and of all transitions connecting those states. The reversible part consists of the remaining states and transitions, namely the states that can be reached from the initial state by visiting *only* reversible states, and their outgoing transitions. We notice that some of these transitions lead to irreversible states. The set of these transitions represents the "border" between the reversible and the irreversible part of the DFA. In Figure 1 an example of this division is shown.
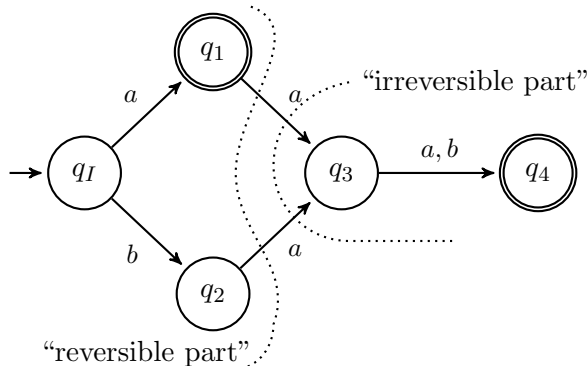

Figure 1:   A minimum DFA with its reversible part (states q_I, q_1, q_2 and outgoing transitions) and its irreversible part (states q_3, q_4). The transitions from q_1 and q_2 on the symbol a are at the border between the two parts

As pointed out in [Kut15], the notion of reversibility for a language is related to the computational model under consideration. In this paper we only consider DFAs. Hence, by saying that a language L is *reversible*, we refer to this model, namely we mean that there exists a REV-DFA accepting L.

The following result presents a characterization of reversible languages [HJK15, Thm. 2]:

Theorem 3.1. *Let L be a regular language and $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting L. L is accepted by a REV-DFA if and only if there do not exist useful states $p, q \in Q$, a letter $a \in \Sigma$, and a string $w \in \Sigma^*$ such that $p \neq q$, $\delta(p, a) = \delta(q, a)$, and $\delta(q, aw) = q$.*
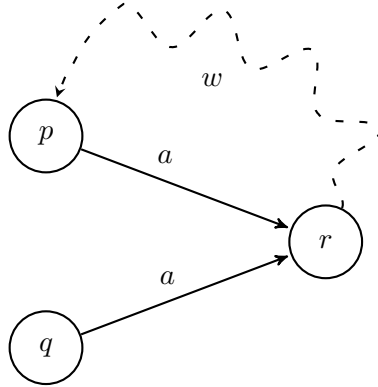
Figure 2: The "forbidden pattern": when it occurs in the transition graph, the minimum DFA cannot be converted into a REV-DFA. It is required that $p \neq q$, but p or q could be equal to r

According to Theorem 3.1, a language L is reversible exactly when the minimum DFA accepting it does not contain the "forbidden pattern" consisting of two transitions on a same letter a entering in a same state r, with one of these transitions arriving from a state in the same SCC as r. (See Figure 2.)

Notice that, since transitions entering in the initial state q_I can only arrive from states in the same SCC of q_I, if the language L is reversible, then the initial state q_I and all the states in the SCC containing it are reversible.

An algorithm for converting a minimum irreversible DFA M into an equivalent minimal REV-DFA A, when possible, has been obtained in [HJK15]. We present an outline of it. At the beginning A is a copy of M. Then, the algorithm considers (with respect to $\preceq$) a minimal SCC C_p that contains an irreversible state p and replace it with α of copies of itself, where α is equal to the maximum number of transitions on a same letter incoming in a state of C_p, i.e.,

$$\alpha = \max\{\#\delta^R(\hat{p}, a) \mid \hat{p} \in C_p, a \in \Sigma\}$$

and redistributes all incoming transitions among these copies, such that no state in the copies of C_p is the target of two or more transitions on the same letter. Notice that all transitions that witness the irreversibility of states in C_p come from outside of C_p, otherwise M would have the forbidden pattern. This process is iterated until all the states in A become reversible. (See Algorithm 1.) As pointed out in [HJK15], in some steps of the algorithm different choices are possible (see lines 3 and 6). As a consequence, different minimal DFAs equivalent to M could be produced.

We conclude this section by presenting some properties that will be used later in the paper to prove our results.

First of all, we observe that Algorithm 1, applied to a whatever DFA M which does not contain the forbidden pattern, produces an equivalent REV-DFA even when M is not minimum. For each SCC C of M which contains an irreversible state, the algorithm creates

Algorithm 1 Transformation from a minimum DFA M to a minimal REV-DFA.

1: Let A be a copy of M
2: **while** there are irreversible states in A **do**
3:     $C_p \leftarrow$ a minimal SCC in A with at least an irreversible state p
4:     $\alpha \leftarrow \max \left\{ \#\delta^R(\hat{p}, a) \mid \hat{p} \in C_p, a \in \Sigma \right\}$
5:     Replace C_p with α copies of itself
6:     Redistribute the transitions incoming to C_p between new copies

a number of copies which is equal to the maximum number of transitions entering in a state of C with a same letter. The following property will be used in Section 5 to prove Theorem 5.1:

Lemma 3.2. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting a reversible language and $M' = (Q', \Sigma, \delta', q'_I, F')$ be an equivalent DFA, with the morphism $\varphi' : M' \to M$, such that M' does not contain the forbidden pattern and its irreversible part is a copy of the corresponding part of M, i.e., $\varphi'^{-1}(\varphi'(p)) = \{p\}$ for each state p in the irreversible part of M'. Given a REV-DFA $A = (Q_A, \Sigma, \delta_A, q_{I_A}, F_A)$ obtained applying Algorithm 1 to M', with the morphism $\varphi : A \to M$, if $p', p'' \in Q_A$ are two copies of $p \in Q'$ created by the algorithm, i.e., $\varphi(p') = \varphi(p'') = \varphi'(p)$, then there exists $z \in \Sigma^*$, $t', t'' \in Q_A$, such that $\delta_A(t', z) = p'$, $\delta_A(t'', z) = p''$, $C_{\varphi(t')} \neq C_{\varphi'(p)}$ and $C_{\varphi(t'')} \neq C_{\varphi'(p)}$.*

Proof. During the step in which the component C_p of M' is evaluated, the algorithm creates α copies of C_p, where α is the maximum number of entering transitions in a same state $\hat{p}$ of C_p, with a same symbol $a \in \Sigma$ (Lines 3 and 4). Since M' does not contain the forbidden pattern, these transitions come from a different SCC of M'. No further changes to the part corresponding to the component C_p are done in the next steps of the algorithm. Let $z' \in \Sigma^*$ be a string such that $\delta'(\hat{p}, z') = p$ and $z = az'$. Then $\delta_A(t', z) = p'$ and $\delta_A(t'', z) = p''$, for two states t', t'' that in A are in SCCs different from those containing p' and p''. We are going to prove that in M the states $\varphi(t')$ and $\varphi(t'')$ are not in the same SCC which contains the state $\varphi(p') = \varphi(p'') = \varphi'(p)$.

If t' and t'' are not equivalent, i.e., $\varphi(t') \neq \varphi(t'')$, then in M the states $\varphi(t')$ and $\varphi(t'')$ cannot belong to the same SCC as $\varphi'(p)$, otherwise M should contain the forbidden pattern. If t' and t'' are equivalent, suppose that the state $t = \varphi(t') = \varphi(t'')$ belongs to the same SCC as $\varphi'(p)$. Then it should exist a string $w \in \Sigma^*$ such that $\delta(\varphi'(p), w) = t$. Furthermore, because $\delta(t, z) = \varphi'(p)$, there is a sequence of states $p_0, t_1, p_1, t_2, \ldots$ of M' such that $p_0 = p$, $t_i = \delta'(p_{i-1}, w)$, $p_i = \delta'(t_i, z)$ for $i > 0$. (Notice that $\varphi(p_i) = \varphi'(p)$ and $\varphi(t_i) = t$.) At some point the sequence should contain a state which already appeared. It can be verified that this implies that M' contains the forbidden pattern, which is a contradiction. Hence, we conclude that $\varphi(t')$ and $\varphi(t'')$ are not in the same SCC as $\varphi'(p)$. $\square$

A structural characterization of minimal REV-DFAs, which can be formulated as follows, has been obtained in [HJK15, Thm. 6]:

Theorem 3.3. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be a minimum DFA and $A = (Q_A, \Sigma, \delta_A, q_{I_A}, F_A)$ be a REV-DFA equivalent to it, with the morphism $\varphi : A \to M$. Then A is minimal*

if and only if for every $q \in Q$, when the set $\varphi^{-1}(q)$ consisting of all states of A which are equivalent to q is not singleton, i.e., $\#\varphi^{-1}(q) > 1$, there exists a word $x \in \Sigma^+$ such that for each $q' \in \varphi^{-1}(q)$, $\delta_A^R(q', x)$ is defined and there are $q'_A, q''_A \in \varphi^{-1}(q)$ and $p'_A, p''_A \in Q_A$ such that $\delta_A(p'_A, x) = q'_A$, $\delta_A(p''_A, x) = q''_A$, and p'_A and p''_A are not equivalent, i.e., $\varphi(p'_A) \neq \varphi(p''_A)$.

From Theorem 3.3 it follows that among all the states of a minimal REV-DFA which are equivalent to a state in the irreversible part of the minimum automaton, there are two states which can be distinguished by "moving back" (i.e., considering the reverse transition function), with a same string x. We now prove that the same holds for each REV-DFA. More precisely, we prove the following property, which will be used later in Section 5 to prove Theorem 5.1:

Lemma 3.4. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be a minimum DFA and let $A = (Q_A, \Sigma, \delta_A, q_{I_A}, F_A)$ be a REV-DFA equivalent to it, with the morphism $\varphi : A \to M$. For each state q in the irreversible part of M there exist $x \in \Sigma^+$, $q'_A, q''_A \in \varphi^{-1}(q)$, and $p'_A, p''_A \in Q_A$ such that $\delta_A(p'_A, x) = q'_A$, $\delta_A(p''_A, x) = q''_A$, and p'_A and p''_A are not equivalent, i.e., $\varphi(p'_A) \neq \varphi(p''_A)$.*

Proof. Being q in the irreversible part, it should exist an irreversible state $q' \in Q$ and a string $z \in \Sigma^*$ such that $\delta(q', z) = q$. Furthermore, since q' is irreversible, by definition there exists $a \in \Sigma$ such that $\#\delta^R(q', a) > 1$. By taking $x = az$ and choosing two states p', p'' in $\delta^R(q', a)$, with $p' \neq p''$, we obtain $\delta(p', x) = \delta(p'', x) = q$.

Given $p'_A, p''_A \in Q_A$ equivalent to p', p'', respectively, and considering $q'_A = \delta_A(p'_A, x)$, $q''_A = \delta_A(p''_A, x)$, we obtain $\varphi(q'_A) = \varphi(q''_A) = q$. From $p' \neq p''$ it follows that $p'_A \neq p''_A$ and then $q'_A \neq q''_A$, otherwise A cannot be reversible. $\qquad\square$

4 Minimal Reversible Automata

In [HJK15] it has been observed that there are reversible languages having several nonisomorphic minimal REV-DFAs. In this section we deepen that investigation by presenting a characterization of the languages having a unique minimal REV-DFA.

Let us start by presenting a series of preliminary results, that will be used later. Hence, from now on, let us fix a reversible language L and the minimum DFA $M = (Q, \Sigma, \delta, q_I, F)$ accepting it.

Lemma 4.1. *Let $A' = (Q', \Sigma, \delta', q'_I, F')$ be a REV-DFA and $A'' = (Q'', \Sigma, \delta'', q''_I, F'')$ be a minimal REV-DFA both accepting L. Given the morphisms $\varphi' : A' \to M$ and $\varphi'' : A'' \to M$, it holds that $\#\varphi'^{-1}(s) \geq \#\varphi''^{-1}(s)$, for each $s \in Q$.*

Proof. By contradiction, suppose $\#\varphi'^{-1}(q) < \#\varphi''^{-1}(q)$ for some state q.

Let us partition Q in the set $Q_L = \{p \mid \exists w \in \Sigma^* \ \delta(p, w) = q\}$ of the states from which q is reachable and the set Q_R of remaining states. The sets Q' and Q'' are partitioned in a similar way, by defining $Q'_L = \varphi'^{-1}(Q_L)$, $Q'_R = \varphi'^{-1}(Q_R)$, $Q''_L = \varphi''^{-1}(Q_L)$, $Q''_R = \varphi''^{-1}(Q_R)$.

First, let us suppose $\#\varphi'^{-1}(p) \le \#\varphi''^{-1}(p)$ for each $p \in Q_L$. We build another automaton $A''' = (Q''', \Sigma, \delta''', q_I''', F''')$, which starts the computation by simulating A' using the states in Q_L' and, at some point, continues by simulating A'' using the states in Q_R''. In particular:

- $Q''' = Q_L' \cup Q_R''$

- The transitions are defined as follows:

  - For $s \in Q_R''$, $a \in \Sigma$: $\delta'''(s, a) = \delta''(s, a)$.
  - For $s \in Q_L'$, $a \in \Sigma$, such that $\delta'(s, a) \in Q_L'$: $\delta'''(s, a) = \delta'(s, a)$.
  - The remaining transitions, i.e., $\delta'''(s, a)$, in the case $s \in Q_L'$, $a \in \Sigma$, and $\delta'(s, a) \in Q_R'$, are obtained in the following way:
    Let us consider the set of states $\{s_1, s_2, \ldots, s_k\}$ which are equivalent to s in A', i.e., $\varphi'(s_i) = \varphi'(s)$ for $i = 1, \ldots, k$ (notice that $s = s_h$ for some $h \in \{1, \ldots, k\}$), and the set of states $\{r_1, r_2, \ldots, r_j\}$ which are equivalent to s in A'', i.e., $\varphi''(r_i) = \varphi'(s)$ for $i = 1, \ldots, j$. Since $j \ge k$ we can safely define $\delta'''(s_i, a) = \delta''(r_i, a)$, for $i = 1, \ldots, k$.

The resulting automaton A''' still recognizes the language L, it is reversible and it has $\#Q_L' + \#Q_R''$ states. From $\#\varphi'^{-1}(p) \le \#\varphi''^{-1}(p)$, for each $p \in Q_L$, and $\#\varphi'^{-1}(q) < \#\varphi''^{-1}(q)$, it follows that $\#Q_L' < \#Q_L''$, thus implying that the number of states of A''' is smaller than the one of A'', which is a contradiction.

In case $\#\varphi'^{-1}(p) > \#\varphi''^{-1}(p)$ for some $p \in Q_L$, we can apply the same construction, after switching the role of A' and A'', so producing an equivalent REV-DFA $\hat{A}'$ which is smaller than A' and still verifies $\#\hat{\varphi}'^{-1}(q) < \#\varphi''^{-1}(q)$, for the morphism $\hat{\varphi}' : \hat{A}' \to M$. Then, we iterate the proof on the two REV-DFAs $\hat{A}'$ and A''.

Hence, we can conclude that $\#\varphi'^{-1}(s) \ge \#\varphi''^{-1}(s)$, for each $s \in Q$. $\qquad\square$

Lemma 4.1 allows to associate with each reversible language L and the minimum DFA $M = (Q, \Sigma, \delta, q_I, F)$ accepting it, the function $c : Q \to \mathbf{N}^+$ such that, for $q \in Q$, $c(q)$ is the number of states equivalent to q in any minimal REV-DFA A equivalent to M, i.e., $c(q) = \#\varphi^{-1}(q)$ for the morphism $\varphi : A \to M$. Notice that $c(q) = 1$ if and only if q is in the reversible part of M. As observed in Section 3, the initial state of M is always in the reversible part. Hence $c(q_I) = 1$. Furthermore, each REV-DFA accepting L should contain at least $c(q)$ states equivalent to q. These facts are summarized in the following result, where we also show that $c(q)$ has the same value for all states belonging to the same SCC of M.

Lemma 4.2. *Let A be a REV-DFA accepting L, with the morphism $\varphi : A \to M$. If two states p, q of M belong to the same SCC of M then $\#\varphi^{-1}(p) = \#\varphi^{-1}(q) \ge c(p)$. Furthermore, if A is minimal then $c(p) = c(q) = \#\varphi^{-1}(p)$.*

Proof. Observe that since p, q belong to the same SCC there exists $x \in \Sigma^*$ such that $\delta(q, x) = p$. Let $\{q_1, q_2, \ldots, q_k\} = \varphi^{-1}(q)$ and $\{p_1, p_2, \ldots, p_j\} = \varphi^{-1}(p)$ be the sets of states in A which are equivalent to q and p, respectively. We are going to prove that $k = j$.
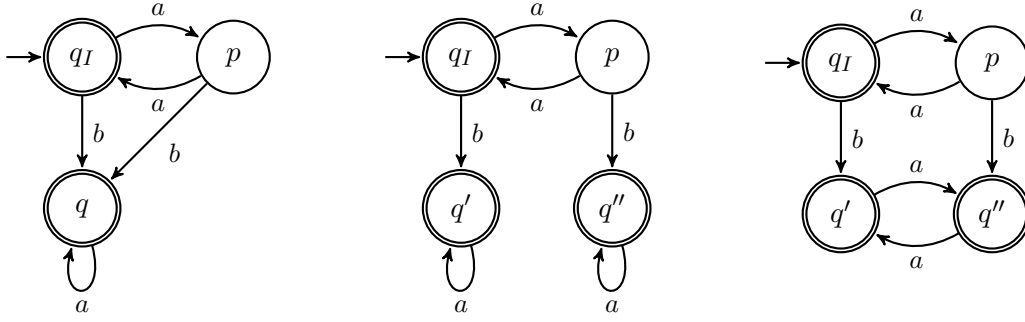
Figure 3: The minimum DFA accepting the language $L = (aa)^* + a^*ba^*$, with two minimal nonisomorphic REV-DFAs

For each q_i, there exists p_{h_i} such that $\delta(q_i, x) = p_{h_i}$. Suppose $j < k$. In this case there are two indices i', i'' such that $p_{h_{i'}} = p_{h_{i''}}$ and then $\delta(q_{i'}, x) = \delta(q_{i''}, x) = p_{h_{i'}}$, implying that the state $p_{h_{i'}}$ is irreversible, which is a contradiction. This means that $j \geq k$. In the same way, by interchanging the roles of p and q, we can prove that $k \geq j$, which leads to the conclusion $j = k$.

The facts that $\#\varphi^{-1}(p) \geq c(p)$ and, for A minimal, $\#\varphi^{-1}(p) = c(p)$, follow from Lemma 4.1.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

In the following, for each SCC C of the transition graph of M, we use $c(C)$ to denote the value $c(q)$, for $q \in C$. Considering Algorithm 1, we can observe that if C' is another SCC, then $C \preceq C'$ implies $c(C) \leq c(C')$.

As a consequence of Lemma 4.2, all the minimal REV-DFAs accepting L have the same "state structure", in the sense that they should contain exactly $c(q)$ states equivalent to the state q of M. However, they could differ in the transitions (see Figure 3 for an example).

Lemma 4.3. *Let $A' = (Q', \Sigma, \delta', q_I', F')$ and $A'' = (Q'', \Sigma, \delta'', q_I'', F'')$ be two REV-DFAs accepting L. Given the morphism $\varphi'' : A'' \to M$, if there are no morphisms $\varphi : A' \to A''$ then there exists a state $p \in Q$ with $\#\varphi''^{-1}(p) > 1$ such that either $p = q_I$, or*

$$\delta^R(p, a) \neq \emptyset \text{ and } \delta^R(p, b) \neq \emptyset,$$

for two symbols $a, b \in \Sigma$, with $a \neq b$.

Proof. Since there are no morphisms $\varphi : A' \to A''$, there exist $x, y \in \Sigma^*$ such that $\delta'(q_I', x) = \delta'(q_I', y)$ and $\delta''(q_I'', x) \neq \delta''(q_I'', y)$. Among all couples of strings with this property we choose one with $|xy|$ minimal. Furthermore, we observe that it cannot be possible that $x = y = \varepsilon$.

When $x = \varepsilon$, we have $\delta'(q_I', \varepsilon) = \delta'(q_I', y) = q_I'$ and, since M is minimum, $\delta(q_I, y) = q_I$. Hence, $\varphi''(\delta''(q_I'', y)) = \varphi''(q_I'') = q_I$. From $\delta''(q_I'', y) \neq q_I'' = \delta''(q_I'', \varepsilon)$, we conclude that $\#\varphi''^{-1}(q_I) > 1$. The case $y = \varepsilon$ is similar.

We now consider $x \neq \varepsilon$ and $y \neq \varepsilon$, i.e., $x = ua$, $y = vb$ for some $u, v \in \Sigma^*$ and $a, b \in \Sigma$. Let $\delta'(q_I', u) = q'$, $\delta'(q_I', v) = r'$, $\delta'(q', a) = \delta'(r', b) = \bar{p}$, $\delta''(q_I'', u) = q''$, $\delta''(q_I'', v) = r''$, $\delta''(q'', a) = s$, and $\delta''(r'', b) = t$, for states $q', r', \bar{p} \in Q'$, $q'', r'', s, t \in Q''$, with $s \neq t$.

Suppose $a = b$. Since A' is reversible from $\delta'(q', a) = \delta'(r', a) = \bar{p}$ we get $q' = r'$. Furthermore $q'' \neq r''$, otherwise A'' would be nondeterministic. Hence, on the strings u, v the automaton A' reaches the same state, while A'' reaches two different states, against the minimality of $|xy|$. Thus $a \neq b$.

Given the morphism $\varphi' : A' \to M$, let $p = \varphi'(\bar{p})$. Since M is minimum, it turns out that $\varphi''(s) = \varphi''(t) = \varphi'(\bar{p}) = p$. From $s \neq t$, we conclude that $\#\varphi''^{-1}(p) > 1$. Furthermore, from the previous discussion, the reader can observe that there are transitions on symbols a and b entering in p. $\qquad\square$

We are now able to prove the following:

Theorem 4.4. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting a reversible language L. The following statements are equivalent:*

1. *There exists a state $p \in Q$ such that $c(p) > 1$, $\delta^R(p, a) \neq \emptyset$, $\delta^R(p, b) \neq \emptyset$, for two symbols $a, b \in \Sigma$, with $a \neq b$.*

2. *There exist at least two minimal nonisomorphic REV-DFAs accepting L.*

Proof. (2) implies (1): By Lemma 4.3, given two minimal nonisomorphic REV-DFAs A' and A'' accepting L, there is a state p such that $c(p) = \#\varphi''^{-1}(p) > 1$. Furthermore, since $c(q_I) = 1$, $p \neq q_I$. Hence, $\delta^R(p, a) \neq \emptyset$, $\delta^R(p, b) \neq \emptyset$, for two symbols $a, b \in \Sigma$, with $a \neq b$.

(1) implies (2): Let $w \in \Sigma^*$ be a string of minimal length such that $\delta(q_I, w) = p$, $a \in \Sigma$ be its last symbol, i.e., $w = xa$, with $x \in \Sigma^*$. Let $b \in \Sigma$ be a symbol with $b \neq a$ and $\delta^R(p, b) \neq \emptyset$. Given a minimal REV-DFA $A' = (Q', \Sigma, \delta', q_I', F')$ accepting L and the morphism $\varphi' : A' \to M$, we consider the state $\hat{p} = \delta'(q_I', w)$. Then $\varphi'(\hat{p}) = p$.

We show how to build a minimal REV-DFA A'' nonisomorphic to A'. The idea is to use the set of states Q' as in A' and to modify only the transitions which simulates the transitions that in M enter the state p with the letter b. There are different cases.

When $\delta'^R(\hat{p}, b) = \emptyset$, it should exist $\tilde{p} \in \varphi'^{-1}(p)$ such that $\tilde{p} \neq \hat{p}$ and $\delta'(\tilde{q}, b) = \tilde{p}$, for some $\tilde{q} \in Q'$. The automaton A'' is defined as A', with the only difference that the transition $\delta'(\tilde{q}, b) = \tilde{p}$ is replaced by $\delta''(\tilde{q}, b) = \hat{p}$. To prove that it is nonisomorphic to A', we consider a string $y \in \Sigma^*$ of minimal length such that $\delta'(q_I', y) = \tilde{q}$. Then $\delta'(q_I', yb) = \tilde{p} \neq \delta'(q_I', w) = \hat{p}$, while $\delta''(q_I', yb) = \hat{p} = \delta''(q_I', w)$.

When $\delta'^R(\hat{p}, b) \neq \emptyset$ we can use one of the following possibilities:

- If there exists $\tilde{p} \neq \hat{p}$ such that $\delta'^R(\tilde{p}, b) \neq \emptyset$, then it should also exist $\tilde{q}, \hat{q} \in Q'$ with $\tilde{q} \neq \hat{q}$ such that $\delta'(\tilde{q}, b) = \tilde{p}$ and $\delta'(\hat{q}, b) = \hat{p}$. The automaton A'' is defined by switching the destinations of these two transitions, namely by replacing them by

11

$\delta''(\tilde{q}, b) = \hat{p}$ and $\delta''(\hat{q}, b) = \tilde{p}$. The proof that A' and A'' are non isomorphic is exactly the same as in the previous case.

- If there exists $\tilde{p} \neq \hat{p}$ such that $\delta'^R(\tilde{p}, b) = \emptyset$, then we can consider $\hat{q}$ such that $\delta'(\hat{q}, b) = \hat{p}$, and define A'' by replacing this transition by $\delta''(\hat{q}, b) = \tilde{p}$. Let $y \in \Sigma^*$ be a string of minimal length such that $\delta'(q_I', y) = \hat{q}$. Then $\delta'(q_I', yb) = \hat{p} = \delta'(q_I', w)$. On the other hand $\delta''(q_I', yb) = \tilde{p} \neq \hat{p} = \delta''(q_I', w)$. Hence, A' and A'' are nonisomorphic.

Finally, we observe that the construction preserves the reversibility and, in both cases, the automaton A'' has the same number of states as A'. Hence, A'' is minimal. $\qquad\square$

In other terms, Theorem 4.4 gives a characterization of reversible languages having a unique minimal REV-DFA as the languages such that in the their minimum DFAs all transitions entering in each state in the irreversible parts are on the same symbol.

When the minimum DFA accepting a reversible language contains a loop in the irreversible part, the previous condition is always false, hence there exist at least two minimal nonisomorphic REV-DFAs. This is proved in the following result:

Theorem 4.5. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting a reversible language L. If there exists an irreversible state $q \in Q$ such that the language accepted by computations starting in q is infinite, then there exists a state $p \in Q$ such that $c(p) > 1$, $\delta^R(p, a) \neq \emptyset$ and $\delta^R(p, b) \neq \emptyset$, for two symbols $a, b \in \Sigma$, with $a \neq b$.*

Proof. Let $p \in Q$ be a state reachable from q which belongs to a nontrivial SCC C. Hence $c(p) > 1$. Among all possibilities, we choose p in such a way that all the other states on a fixed path from q to p does not belong to C. Since C is nontrivial, it should exist a transition from a state of C, which enters in p. Let $a \in \Sigma$ be the symbol of such transition. Furthermore, it should exist another transition which enters in p from a state which does not belong to C. (If $p \neq q$ then we can take the last transition on the fixed path. Otherwise, since the initial state is always reversible, we have $q \neq q_I$, and so we can take the last transition entering in q on a path from q_I.) Let b the symbol of such transition. If $a = b$ the automaton M would contain the forbidden pattern (cfr. Theorem 3.1), thus implying that L is not reversible. Hence, we conclude $a \neq b$. $\qquad\square$

As a consequence of Theorems 4.4 and 4.5, we obtain the following:

Corollary 4.6. *Let L be a reversible language accepted by a unique minimal REV-DFA, and let $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA for L. Then all the loops in M are in the reversible part. Furthermore, for each state q in the irreversible part of M, all the transition incoming to q are on a same letter, i.e., $\#\{a \in \Sigma \mid \delta^R(q, a) \neq \emptyset\} = 1$.*

We point out that there are reversible languages whose minimum DFA does not contain any loop in the irreversible part, which does not have a unique minimal REV-DFA. Indeed, in [HJK15] an example with a finite language is presented.
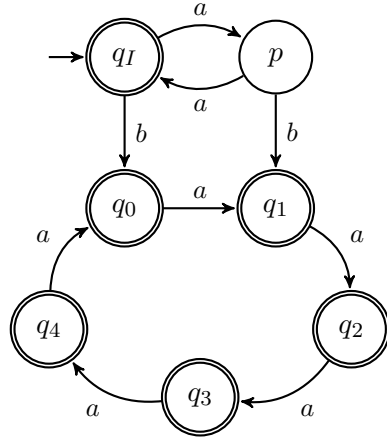
Figure 4: A reduced REV-DFA

5   Reduced Reversible Automata

In this section we show that there exist REV-DFAs which are reduced but not minimal, namely they have more states than equivalent minimal REV-DFAs, but merging some of their equivalent states would produce an irreversible automaton. Furthermore, we will prove that there exist reversible languages having arbitrarily large reduced REV-DFAs and, hence, infinitely many reduced REV-DFAs.

In Figure 4 a reduced REV-DFA equivalent to the DFAs in Figure 3 is depicted. If we try to merge two states in the loop, then the loop collapses to unique state, so producing the minimum DFA, which is irreversible. Actually, this example can be modified by using a loop of N states: if (and only if) N is prime, we get a reduced automaton. This is a special case of the construction which we are now going to present:

Theorem 5.1. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting a reversible language L. Suppose that M contains a loop and a path from a state in the loop to some state $s \in Q$ on a nonempty string which ends by the symbol $a \in \Sigma$. If there is a symbol $b \in \Sigma$, with $b \neq a$, $\delta^R(s, b) \neq \emptyset$, and either $\#\delta^R(s, b) > 1$ or there is $r \in Q$ such that $\delta(r, b) = s$ and $c(r) > 1$, then there exist infinitely many nonisomorphic reduced REV-DFAs accepting L.*

Proof. First of all, we notice that the hypothesis on the transitions entering in s implies that $c(s) > 1$. Let ℓ be the loop satisfying the condition in the statement. Let us fix a state q in ℓ.

Let A be a minimal REV-DFA accepting L, obtained applying Algorithm 1 and $N \geq c(q)$ an integer. The idea is to modify A by replacing the part corresponding to the SCC C_q containing q, with N copies of each state in C_q and arranging the transitions in such a way that all the states in these N copies form one SCC, without changing the accepted language. Furthermore, all SCCs that follow C_q will be replicated a certain number of times. More precisely, we build a DFA $A_N = (Q_N, \Sigma, \delta_N, q_{I_N}, F_N)$ using the following steps:

13

(i) We put in A_N all the states of A which correspond to SCCs C of M with $C_q \not\preceq C$ and all the transitions between these states.

(ii) We add N copies of the states in C_q to the set of states of A_N. Given a state $r \in C_q$, let us denote its copies as $r_0, r_1, \ldots, r_{N-1}$.

(iii) We fix a transition $\delta(q, \sigma) = q'$ of M, with $q, q' \in C_q$ and $\sigma \in \Sigma$. For $i = 0, \ldots, N-1$, we define $\delta_N(q_i, \sigma) = q'_{(i+1) \bmod N}$, and for the remaining transitions, namely $\delta(r, \gamma) = r'$ with $(r, \gamma) \neq (q, \sigma)$, we define $\delta_N(r_i, \gamma) = r'_i$. In this way in A_N we have N copies of the SCC C_q, modified in such a way that the transition from q_i on σ in copy i leads to the state $q'_{(i+1) \bmod N}$ in copy $(i+1) \bmod N$.

(iv) We add to A_N each transition that in A leads from a state added in (i) to one state in the first $c(q)$ copies of C_q added in (ii).

(v) We complete the construction by adding to the part of automaton obtained in steps (i-iv) one copy of each remaining SCC C of M, namely SCCs C such that $C_q \preceq C$ with $C_q \neq C$, and suitable transitions from the already constructed part, in order to accept L. We apply Algorithm 1 to the DFA M, in order to derive a REV-DFA.

Let A_N be the REV-DFA accepting L so obtained. Considering the hypothesis of the theorem, we now prove that A_N contains two states s' and s'' equivalent to s and two states r' and r'' such that $\delta_N(r', b) = s'$, $\delta_N(r'', b) = s''$ and the states $\delta(r', x)$ and $\delta(r'', x)$ are not equivalent, for a string $x \in \Sigma^*$.

- If $\#\delta^R(s, b) > 1$ then M should contain two inequivalent states such that, reading the symbol b, the state s is reached. Hence, in A_N there are r' and r'' which are not equivalent, while the states $\delta_N(r', b)$ and $\delta(r'', b)$ are equivalent to s. In this case we take $x = \varepsilon$.

- Otherwise, there is $r \in Q$ such that $\delta(r, b) = s$ and $c(r) > 1$. By Lemma 3.4, among all the states equivalent to r in A_N, it should exist r' and r'' such that $\delta_N^R(r', x)$ and $\delta_N^R(r'', x)$ are not equivalent for a string $x \in \Sigma^+$.

In both cases we choose $s' = \delta_N(r', b)$ and $s'' = \delta_N(r'', b)$.

Moreover, we observe that from the existence of a path from the loop ℓ (and hence from q) to s, the automaton A_N contains at least N states $s_0, s_1, \ldots, s_{N-1}$ that are copies of s (not necessarily different from s', s''), each one of them having an entering transition on the letter a. More precisely, $\delta_N(q_i, u) = s_i$, for $i = 0, \ldots, N-1$, where u is the string labeling the path from q to s.

(vi) We modify A_N in such a way that s', s'' belong to $\{s_0, s_1, \ldots, s_{N-1}\}$. (E.g., if $s' \notin \{s_0, s_1, \ldots, s_{N-1}\}$ then we can move the transition from r' on b to a state s_i which does not have any entering transition on b, if any; if s_i already has an entering transition on b, we can move it to s', that is, making a switch — this transformation preserves reversibility and the accepted language — then s_i becomes the "new" s'.)

We are now going to prove that if N is prime then the automaton A_N finally obtained by this process is reduced. To this aim we shall prove that if we try to merge two equivalent states p', p'' ($p' \neq p''$) of A_N then we obtain an irreversible automaton. The proof is divided in three cases:

(1) p', p'' are equivalent to a state p of M with $C_q \npreceq C_p$, where C_p denotes the SCC containing p.

These states have been added at step (i), copying them from the minimal REV-DFA A. By Lemma 4.2, A contains exactly $c(p)$ states equivalent to p. Hence, merging p' and p'', the resulting automaton would contain less than $c(p)$ states equivalent to p and, hence, it cannot be reversible.

(2) p', p'' are equivalent to a state p of M belonging to C_q.

First, suppose $p' = q_0$ and $p'' = q_j$, $0 < j < N$. Considering step (iii), we observe that there is a string z such that $\delta(q', z) = q$, then $\delta(q, w) = q$ and $\delta_N(q_i, w) = q_{(i+1) \bmod N}$, where $w = \sigma z$. Thus, for each $k \geq 0$, $\delta(q_0, w^{k(N-j)}) = q_{k(N-j) \bmod N}$ and $\delta(q_j, w^{k(N-j)}) = q_{j+k(N-j) \bmod N} = q_{(k-1)(N-j) \bmod N}$. Hence, merging q_0 and q_j would imply merging all the states whose indices are in the set $\{k(N-j) \bmod N \mid k \geq 0\}$, which, being N prime, coincides with $\{0, \dots, N-1\}$. As a consequence, all states q_i should collapse in a unique state. Since considering step (vi) $\delta(q_i, u) = s_i$, this would also imply that s' and s'' collapses. However, since the states $\delta_N^R(s', xb) = \delta_N^R(r', x)$ and $\delta_N^R(s'', xb) = \delta_N^R(r'', x)$ are not equivalent, this would introduce some irreversible state.

If $p' \neq q_0$, then we can always find a string y such that $\delta_N(p', y) = q_0$. Using the transitions introduced at step (iii), we get that $\delta_N(p'', y) = q_j$, for some $0 < j < N$. Hence, merging p' and p'' would imply merging q_0 and q_j, so reducing to the previous case.

(3) p', p'' are equivalent to a state p of M, such that $C_q \neq C_p$ and $C_q \preceq C_p$.

Let $\varphi : A_N \to M$ be the morphism from A_N to M. Hence, $\varphi(p') = \varphi(p'') = p$.

 (a) If $C_p = C_{q_I}$ then some copies of the component q_I have been made. Since, as observed in Section 3, the initial state is always reversible ($c(q_I) = 1$) and C_{q_I} is minimum with respect to $\preceq$, the only way to obtain copies of C_{q_I} is to add them in step (ii), i.e., $C_q = C_{q_I}$, thus implying $C_q = C_p$ which gives a contradiction.

 (b) If $C_p \neq C_{q_I}$, then by Lemma 3.2 there exist states $t', t'' \in Q_N$ such that $\delta_N(t', z) = p'$, $\delta_N(t'', z) = p''$ for some $z \in \Sigma^*$ where $C_{\varphi(t')} \neq C_p$ and $C_{\varphi(t'')} \neq C_p$. Now we analyze some cases:

   • If t', t'' are not equivalent then we cannot merge p' and p''. In fact, it would imply to introduce some irreversible states.
   • If t', t'' are equivalent and hence $\varphi(t') = \varphi(t'') = t \in Q$ then we have the following possibilities:
     (I) $C_t = C_q$: this brings us to the case (2).
     (II) $C_q \npreceq C_t$: this brings us to the case (1).

15

(III) $C_q \preceq C_t$ (and $C_q \neq C_t$): we can iterate case (3) we are considering, by substituting p' and p'' with t' and t'', respectively. At some time, we will finally stop either because t' and t'' are not equivalent or because we reach one of the cases (I) or (II), or because t' and t'' are equivalent to a state in the component C_{q_I}, so obtaining case (a).

In summary, for each prime number $N \geq c(q)$ we obtained a reduced REV-DFA A_N with more than N states accepting the language L. Hence, we can conclude that there exist infinitely many nonisomorphic reduced REV-DFA accepting L. $\qquad\square$

In Theorem 5.1 we presented a sufficient condition for the existence of infinitely many reduced REV-DFAs accepting a given language. The condition requires the existence (in the irreversible part of the minimum DFA) of a state s entered by a transition a, on a path starting in a loop, and by another symbol b, different from a, such that the symbol b has a "double" transition entering in s in the following sense: either M contains two transitions on b entering in s, or the only transition on b entering in s is from another state r in the irreversible part, thus implying that in each equivalent REV-DFA this transition should be duplicated (with the two states r and s).

These situations are presented in Figure 5 and Figure 6. In particular, in the minimum DFA in Figure 5 there are two transitions on the letter b entering in the state s, while in the minimum DFA in Figure 6, the state r with $\delta(r, b) = s$ is in the irreversible part. Figure 7 instead shows a minimum DFA which does not satisfy such sufficient condition: the state s is the unique in the irreversible part and $\#\delta^R(s, b) = 1$. If we try to expand the loop, we can reduce the obtained automata to the minimal one. Hence, for this example, it is not possible to build infinitely many reduced REV-DFAs.

We point out that the condition in Theorem 5.1 is not necessary. In fact it is possible to build infinitely many reduced REV-DFAs accepting a same language even in other situations [Ivá16].

All three examples show a minimum DFA containing a loop in the reversible part. Using Theorem 5.1 we now prove that when the loop is in the irreversible part, it is always possible to construct an infinite family of reduced REV-DFAs (for an example see Figure 4).

Corollary 5.2. *Let* $M = (Q, \Sigma, \delta, q_I, F)$ *be the minimum* DFA *accepting a reversible language* L. *If* M *contains a loop in the irreversible part, then there exist infinitely many nonisomorphic reduced* REV-DFA*s accepting* L.

Proof. Let us consider a nontrivial SCC C in the irreversible part of M. As observed in Section 3, C should be different from the SCC C_{q_I} containing the initial state. Then there exist a string $y \in \Sigma^*$, a symbol $b \in \Sigma$, a state r not in C and a state s in C such that $\delta(q_I, y) = r$ and $\delta(r, b) = s$, i.e., the SCC C is reached from the initial state after reading the whole string yb. Since C is in the irreversible part, we can find y, b, r, s in such a way that either $c(r) > 1$ or $\#\delta^R(s, b) > 1$.

Furthermore, since C is nontrivial there should exist a string $x \in \Sigma^+$ such that $\delta(s, x) = s$. Let a be the last symbol of x. Then $a \neq b$, otherwise M should contain the forbidden
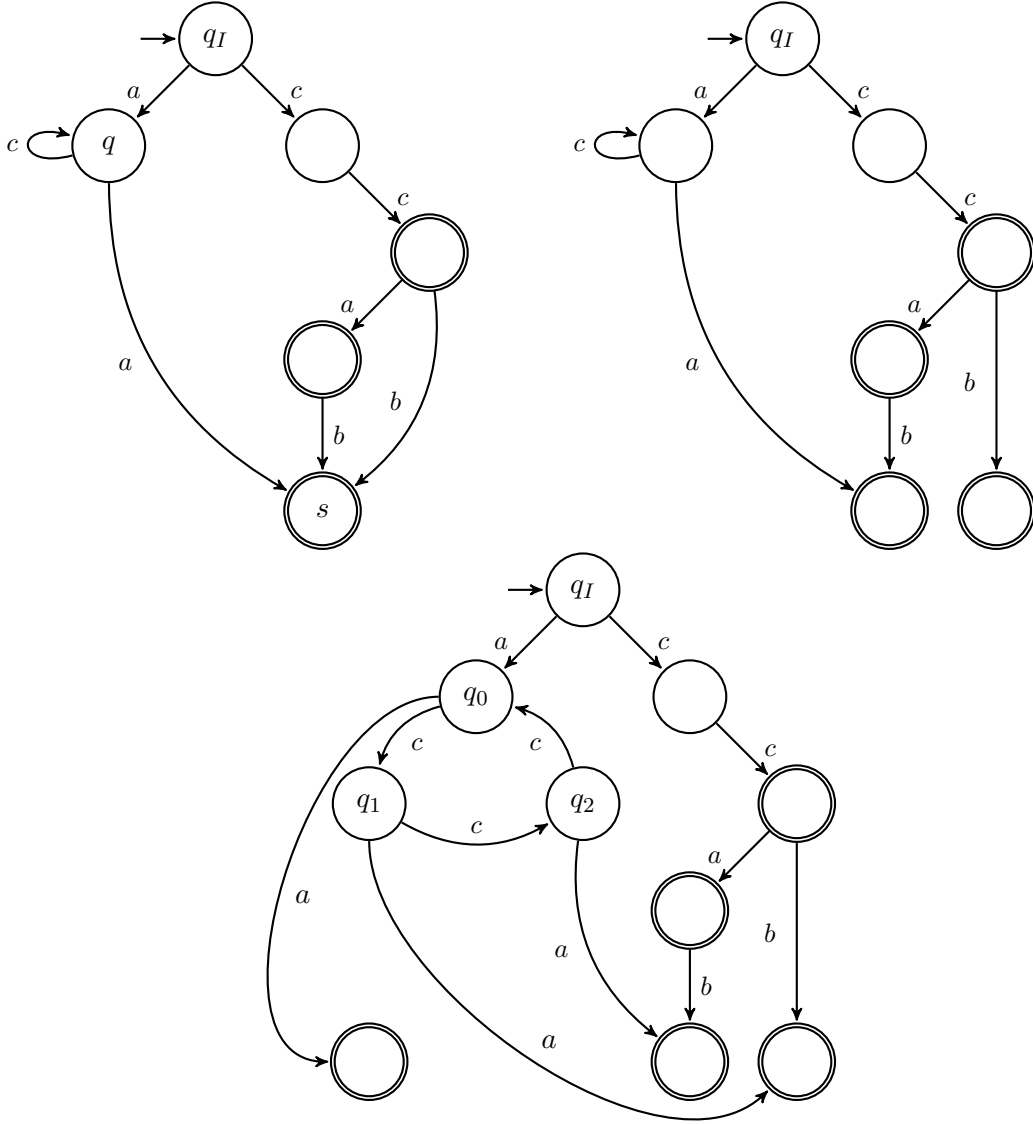
16

Figure 5: The minimum DFA accepting a reversible language $L = ac^*a + cc(\varepsilon + a)(\varepsilon + b)$, with an equivalent minimal REV-DFA and an equivalent reduced REV-DFA
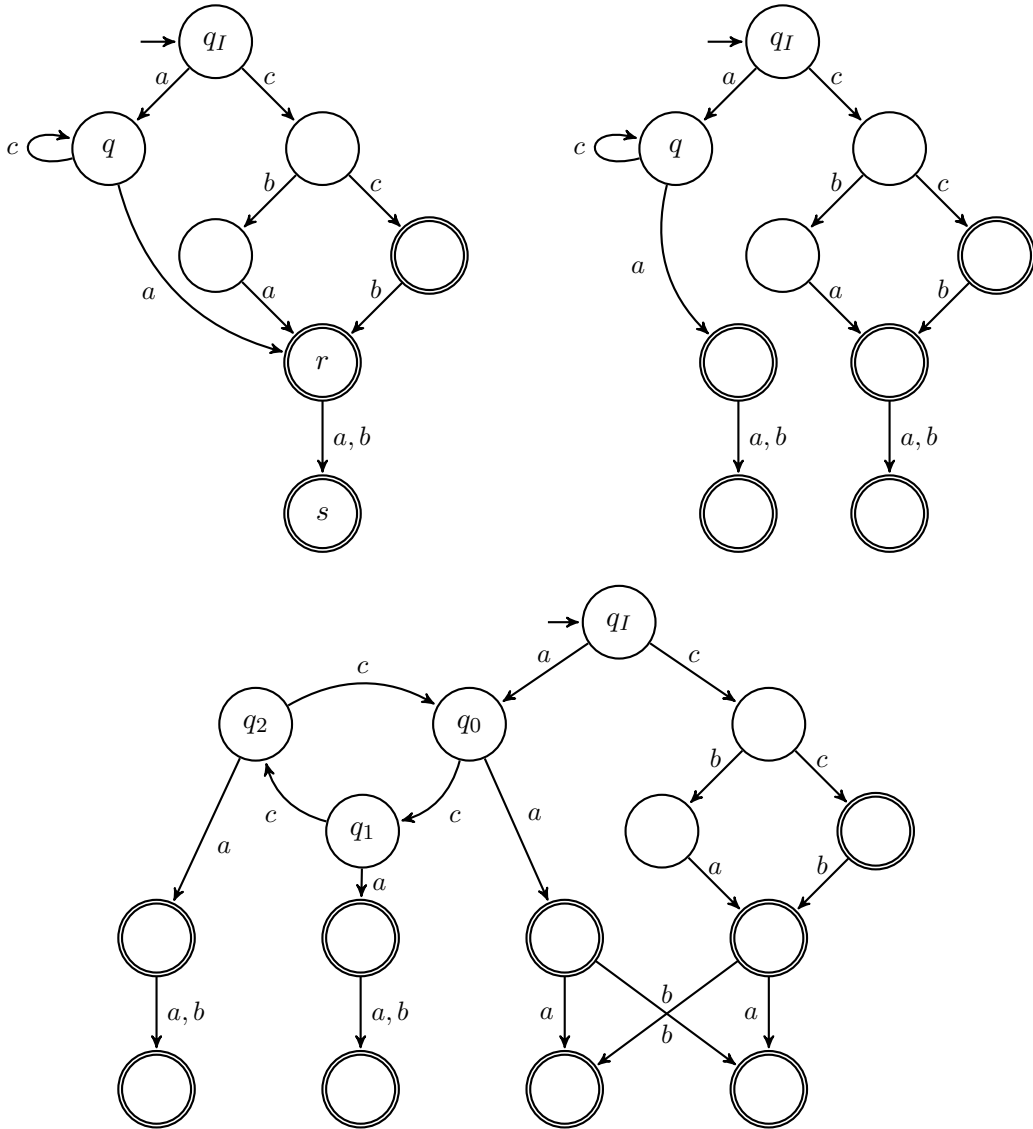
17

Figure 6: The minimum DFA accepting the language $L = cc + (ac^*a + c(cb + ba))(\varepsilon + a + b)$, an equivalent minimal REV-DFA, and an equivalent reduced REV-DFA
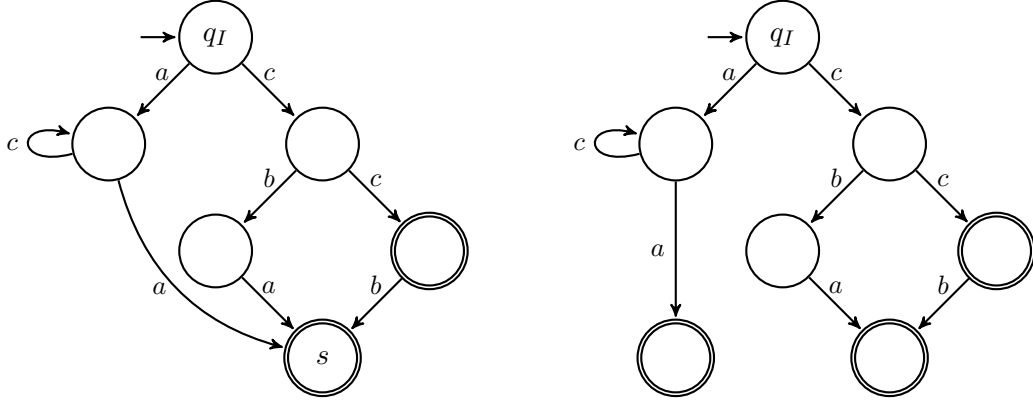
Figure 7: The minimum DFA accepting the language $L = ac^*a + c(c + cb + ba)$, with an equivalent minimal REV-DFA

pattern. This allows to conclude that M satisfied the condition of Theorem 5.1. Hence, there are infinitely many reduced automata equivalent to M.

$\square$

6 Unique Minimal Reversible Automata

In this section we resume the investigation about the existence of a unique minimal REV-DFA (cfr. Section 4), by proving that when the family of REV-DFAs accepting a given language L contains a unique minimal REV-DFA A then each equivalent REV-DFA can be reduced to it. As a consequence, A is the *minimum* REV-DFA accepting L and no reduced REV-DFAs other than A can exist.

We remind the reader that a reversible language has a unique minimal reversible automaton if and only if all the transitions entering in a state in the irreversible part of the minimum DFA are on the same symbol (Theorem 4.4).

Lemma 6.1. *Let $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting a reversible language L such that, for each state $q \in Q$ with $c(q) > 1$, all incoming transitions to q are on the same symbol, that is $\#\{a \in \Sigma \mid \delta^R(q, a) \neq \emptyset\} = 1$. Let $\mathcal{W}_q$ be the set of pairs (r, x) where r is a reversible state and $x \in \Sigma^*$ such that, starting from r and reading x, the state q is reached, passing only through states in the irreversible part, i.e.,*

$$\mathcal{W}_q = \{(r, x) \mid \delta(r, x) = q, \, c(r) = 1, \, \forall x = uv, \, u \in \Sigma^+, v \in \Sigma^* \implies c(\delta(r, u)) > 1\}.$$

Then the minimum number of states equivalent to q in the minimal REV-DFA accepting L is equal to the cardinality of $\mathcal{W}_q$, i.e., $c(q) = \#\mathcal{W}_q$.

Proof. Let $A = (Q_A, \Sigma, \delta_A, q_{I_A}, F_A)$ be a minimal REV-DFA equivalent to M with the morphism $\varphi : A \to M$. We consider all the paths in A from states p, where $\varphi(p) = r$ is

reversible, reading a string x such that $(r, x) \in \mathcal{W}_q$ and reaching some state in $\varphi^{-1}(q)$. If two such paths share a same state t, other than the initial state p of the path, then at least two transitions enter in t. Since A is reversible, such transitions should be on different letters. However, this is not possible because of the hypothesis on the incoming transitions on a same symbol to the states in the irreversible part of M. Furthermore, we notice that each state in $\varphi^{-1}(q)$ should be reached by some of those paths. Hence we conclude that $c(q) = \#\mathcal{W}_q$. $\square$

An example related to Lemma 6.1 is shown in Figure 8: considering the minimum DFA M (on the top left), we can observe that $\mathcal{W}_q = \{(r_1, ba), (r_2, ba)\}$. So, the sufficient and necessary number of copies of q is $c(q) = \#\mathcal{W}_q = 2$, as shown in the equivalent minimal REV-DFA (on the top right).

We are now ready to prove the following:

Theorem 6.2. *Let L be a reversible language and $M = (Q, \Sigma, \delta, q_I, F)$ be the minimum DFA accepting it. If there exists a unique minimal REV-DFA A_m accepting L, then each REV-DFA A other than A_m accepting L is not reduced.*

Proof. From Corollary 4.6 it follows that there are no loops in the irreversible part of M and all incoming transitions to each state $q \in Q$ with $c(q) > 1$ are on the same symbol. As a consequence, also in any DFA equivalent to M all incoming transitions to any state which is equivalent to q are on the same symbol.

Let $A = (Q_A, \Sigma, \delta_A, q_{I_A}, F_A)$ be a REV-DFA accepting L with the morphism $\varphi : A \to M$. Suppose A is different from A_m. Then A is not minimal and, as a consequence of Lemma 4.1, it should exist $q \in Q$ such that $\#\varphi^{-1}(q) > c(q)$. We are going to prove that from A it is possible to obtain a smaller REV-DFA accepting L.

1. If q is in the reversible part, i.e., $c(q) = 1$, from A we obtain a smaller DFA $B = (Q_B, \Sigma, \delta_B, q_{I_B}, F_B)$ by merging together all states which are equivalent to a same state belonging to the reversible part of M (which would imply to merge also all the states that are reachable reading a same string from states that have been merged). Hence, the DFA B so obtained consists of a copy of the reversible part of M together with some other states and transitions which are derived from A and which correspond to the irreversible part of M.

   Suppose that B contains an irreversible state p_B, namely there exist two entering transitions in p_B with a same symbol a from two different states, say $r'_B, r''_B \in Q_B$. This should imply that p_B is equivalent to a state $p \in Q$ in the irreversible part of M. So, p_B has been obtained merging some equivalent states $p_1, p_2, \ldots, p_k \in Q_A$, where $\varphi(p_i) = p$, $i = 1, \ldots, k$. Since the *only* way to enter in $p_1, p_2, \ldots, p_k$ is with the symbol a, this happens if and only if there exist states $r_1, r_2, \ldots, r_k \in Q_A$, with $\delta(r_i, a) = p_i$, $i = 1, \ldots, k$, which have been merged in a state $r_B \in Q_B$, obtaining $\delta_B(r_B, a) = p_B$. Since no other transitions can enter in $p_1, p_2, \ldots, p_k$, it follows that $r'_B = r''_B = r_B$, which is a contradiction to the hypothesis that p_B is irreversible. Thus, we conclude that B is reversible and it is smaller than A.
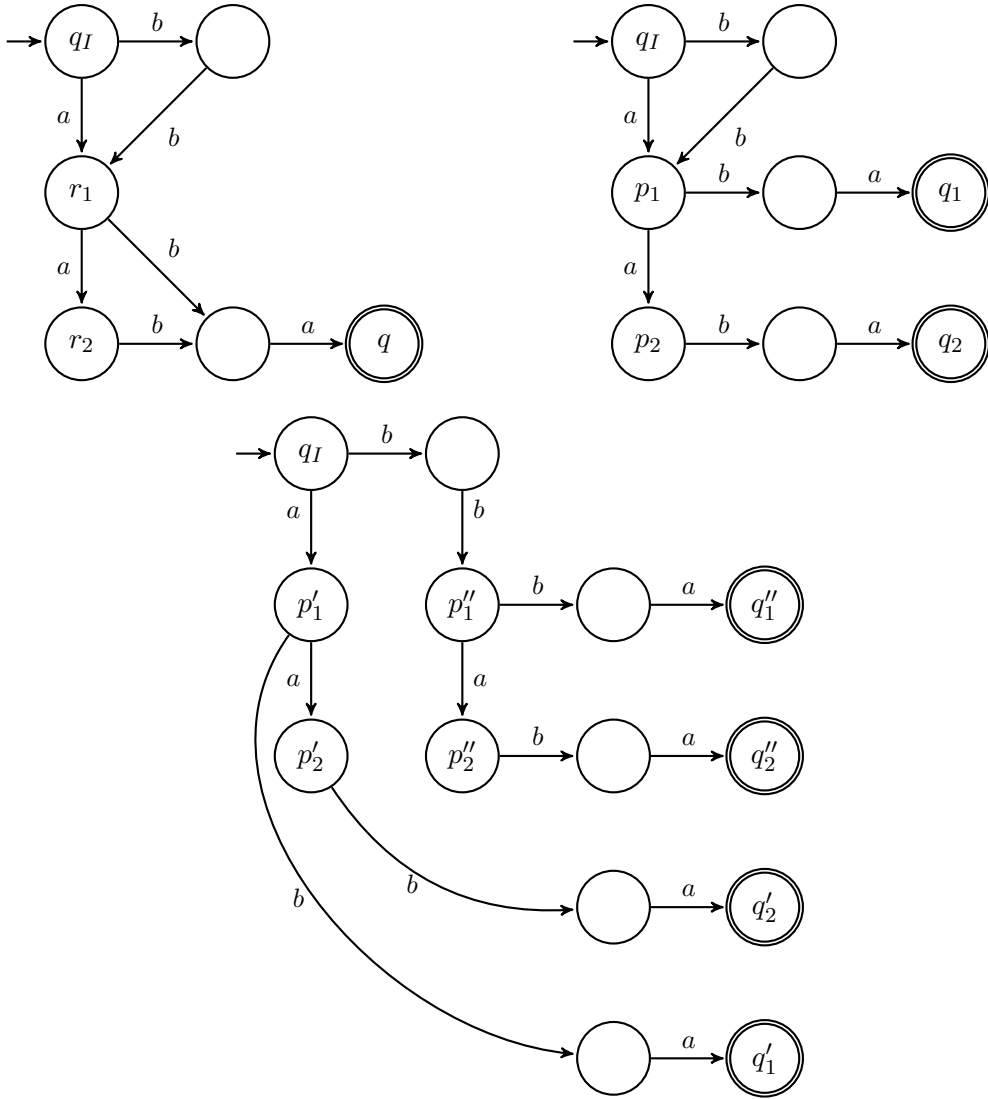
20

Figure 8: The minimum DFA accepting the language $L = (bb + a)(ab + b)a$ (top left), with an equivalent minimal REV-DFA (top right) and an equivalent non minimal REV-DFA (bottom). Notice that the minimum DFA (on the top left) accepting the language is different from the minimum REV-DFA

2. If q is in the irreversible part, i.e., $c(q) > 1$, let $\varphi^{-1}(q) = \{q_1, \ldots, q_k\}$ with $k = \#\varphi^{-1}(q) > c(q)$. Let $\mathcal{W}_q$ be the set defined in Lemma 6.1. There exist couples $(r_1, x_1), \ldots, (r_k, x_k) \in \mathcal{W}_q$ and $p_1, \ldots, p_k \in Q_A$ such that $r_i = \varphi(p_i)$, and $\delta_A(p_i, x_i) = q_i$, $i = 1, \ldots, k$. By Lemma 6.1, $\#\mathcal{W}_q = c(q)$ so, since $k > c(q)$, two of such couples coincide, i.e., there are two indices i, j, $i \neq j$, such that $(r_i, x_i) = (r_j, x_j)$. If $p_i = p_j$ then it should be $\delta_A(p_i, x_i) = \delta_A(p_j, x_j)$, that is $q_i = q_j$, which is a contradiction to the hypothesis that $\#\varphi^{-1}(q) = k$. Thus, $p_i \neq p_j$, but $\varphi(p_i) = r_i = r_j = \varphi(p_j)$. Hence, $\#\varphi^{-1}(r_i) > 1$, where r_i is in the reversible part of M. This brings us to case (1).

As a consequence, the automaton A is not reduced. □

By Theorem 6.2, when a language L is accepted by a unique minimal REV-DFA A_m, then any other REV-DFA A accepting L can be reduced, by merging states, to A_m, that is there exists a morphism from A to A_m. Hence, A_m is the *minimum* REV-DFA accepting L. Notice that A_m could differ from the minimum DFA accepting L. This is illustrated (together some of the ideas in the proofs of Lemma 6.1 and Theorem 6.2) in Figure 8.

7 Conclusion

We studied the existence of many minimal and reduced REV-DFAs. In some cases the minimum DFA accepting a language is already reversible, so assuring that the language is reversible. However, in general a minimum DFA does not need to be reversible, although the accepted language could be reversible. Using Theorem 3.1 and the construction from [HJK15] outlined in Section 2, in the case the language is reversible, from a given minimum DFA we can obtain an equivalent minimal REV-DFA.

Minimal REV-DFAs are not necessarily unique (see Figure 3 for an example, while Figure 9 shows a case with a unique minimal REV-DFA). In Section 4 we gave a characterization of the languages having a unique minimal REV-DFA, in terms of the structure of the minimum DFA. As shown in Section 6, if a language has a unique minimal REV-DFA, then each equivalent REV-DFA can be reduced to it, namely the minimal REV-DFA is the minimum REV-DFA for the language under consideration.

Figure 9: The minimum DFA and the minimum REV-DFA accepting the language $L = (aa)^* + a^*b$

When the minimal REV-DFA is not unique, reduced not minimal REV-DFAs could exist. In

Theorem 5.1 we gave a sufficient condition for the existence of arbitrarily large and, hence, infinitely many reduced REV-DFAs accepting a same reversible language. However, there are also languages having only finitely many reduced non minimal REV-DFAs. An example is given in Figure 10, where the accepted language is finite, thus implying that only finitely many automata with useful states and, hence, finitely many reduced REV-DFAs, can exist.
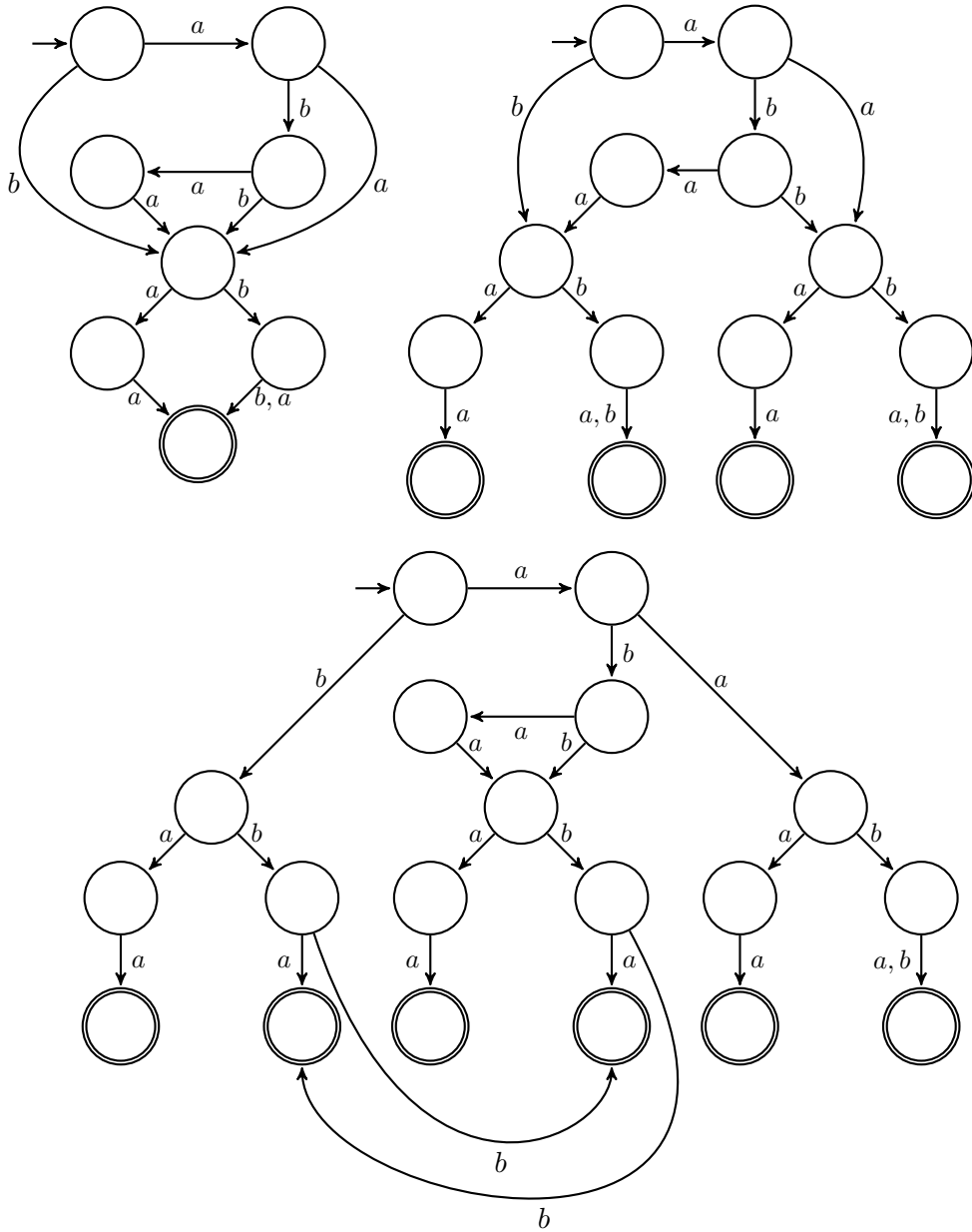

Figure 10: The minimum DFA accepting the language $L = (a(bb+a+baa)+b)(aa+ba+bb)$, an equivalent minimal REV-DFA, and an equivalent reduced non minimal REV-DFA

23

References

[Ang82]   Dana Angluin. Inference of reversible languages. *J. ACM*, 29(3):741–765, 1982.

[Ben73]   C.H. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, 17(6):525–532, 1973.

[HJK15]   Markus Holzer, Sebastian Jakobi, and Martin Kutrib. Minimal reversible deterministic finite automata. In Igor Potapov, editor, *Developments in Language Theory - 19th International Conference, DLT 2015, Liverpool, UK, July 27-30, 2015, Proceedings.*, volume 9168 of *Lecture Notes in Computer Science*, pages 276–287. Springer, 2015.

[HU79]   John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages and Computation.* Addison-Wesley, 1979.

[Ivá16]   Szabolcs Iván. Private communication, September 2016.

[Kut14]   Martin Kutrib. Aspects of reversibility for classical automata. In Cristian S. Calude, Rusins Freivalds, and Kazuo Iwama, editors, *Computing with New Resources - Essays Dedicated to Jozef Gruska on the Occasion of His 80th Birthday*, volume 8808 of *Lecture Notes in Computer Science*, pages 83–98. Springer, 2014.

[Kut15]   Martin Kutrib. Reversible and irreversible computations of deterministic finite-state devices. In Giuseppe F. Italiano, Giovanni Pighizzini, and Donald Sannella, editors, *Mathematical Foundations of Computer Science 2015 - 40th International Symposium, MFCS 2015, Milan, Italy, August 24-28, 2015, Proceedings, Part I*, volume 9234 of *Lecture Notes in Computer Science*, pages 38–52. Springer, 2015.

[KW97]   Attila Kondacs and John Watrous. On the power of quantum finite state automata. In *FOCS*, pages 66–75. IEEE Computer Society, 1997.

[Lan61]   R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, July 1961.

[LMT00]   Klaus-Jörn Lange, Pierre McKenzie, and Alain Tapp. Reversible space equals deterministic space. *J. Comput. Syst. Sci.*, 60(2):354–367, 2000.

[Lom02]   Sylvain Lombardy. On the construction of reversible automata for reversible languages. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings*, volume 2380 of *Lecture Notes in Computer Science*, pages 170–182. Springer, 2002.

[LPP16]   Giovanna J. Lavado, Giovanni Pighizzini, and Luca Prigioniero. Minimal and reduced reversible automata. In *Descriptional Complexity of Formal Systems*, volume 9777 of *Lecture Notes in Computer Science*, pages 168–179. Springer, 2016.

[Myh57]   John R. Myhill. Finite automata and the representation of events. Technical Report WADC TR-57-624, Wright-Paterson Air Force Base, 1957.

[Ner58]   Anil Nerode. Linear automaton transformations. *Proceedings of the American Mathematical Society*, 9(4):541–544, 1958.

[Pin92]   Jean-Eric Pin. On reversible automata. In Imre Simon, editor, *LATIN '92, 1st Latin American Symposium on Theoretical Informatics, São Paulo, Brazil, April 6-10, 1992, Proceedings*, volume 583 of *Lecture Notes in Computer Science*, pages 401–416. Springer, 1992.