Varieties Generated by Certain Models of Reversible Finite Automata

Marats Golovkins[1⋆] and Jean-Eric Pin[2]

[1] Institute of Mathematics and Computer Science, University of Latvia,
Raiņa bulv. 29, Riga, Latvia
[2] LIAFA, Université Paris VII and CNRS, Case 7014, 2 Place Jussieu,
75251 Paris Cedex 05, France
marats@latnet.lv, Jean-Eric.Pin@liafa.jussieu.fr

Abstract. Reversible finite automata with halting states (RFA) were first considered by Ambainis and Freivalds to facilitate the research of Kondacs-Watrous quantum finite automata. In this paper we consider some of the algebraic properties of RFA, namely the varieties these automata generate. Consequently, we obtain a characterization of the boolean closure of the classes of languages recognized by these models.

1 Introduction

In this paper we study reversible finite automata (RFA). Being entirely classical, the model is however a special case of Kondacs-Watrous quantum finite automata and was introduced in [5]. Quantum finite automata (QFA) are of a specific interest, since the family of these models represent finite memory real-time quantum mechanical devices. On the other hand, recently it has been demonstrated [3] that these models are worth studying also from the point of view of classical algebraic automata theory. The first models of QFA are due to [11] and [13]. Other models are proposed and studied, for example, in [9, 14, 6, 8, 3, 10, 4], etc. In principle, the different types of QFA reflect the different ways how the results of computation can be interpreted, i.e., quantum measurements. By applying various restrictions, it is even possible to get deterministic and probabilistic special cases of QFA. Such models sometimes prove to be extremely useful in the research of the properties of QFA.

In Section 2 we introduce the finite automata models discussed further in the paper. Section 3 recalls the notations of the varieties used in this paper. Section 4 deals with injective finite automata (IFA), which are in turn a special case of RFA. IFA are closely related to a deterministic special case of Brodsky-Pippenger QFA [9]. We give an exact characterization of languages which are recognized by IFA and conclude that the syntactic monoids of this class generates the variety of commuting idempotent monoids, **ECom**. In Section 5 we show

⋆ Supported by the Latvian Council of Science, grant No. 05.1528 and by the European Social Fund, contract No. 2004/0001/VPD1/ESF/PIAA/04/NP/3.2.3.1/0001/0063. The paper was prepared while visiting LIAFA, Université Paris VII and CNRS, and Electronics Research Laboratory, University of California, Berkeley

that the syntactic monoids of languages recognized by RFA generate the variety defined by the identity $x^\omega y^\omega x^\omega = x^\omega y^\omega$. Section 6 specifies algebraic conditions for a language to be recognized by RFA or IFA.

2 Preliminaries

In this paper, by *minimal automaton* of a regular language we understand a complete minimal deterministic finite automaton recognizing the language (the transition function is defined for any state and any input letter). Two automata (deterministic or not) are said to be *equivalent* if they accept the same language. We denote by L^c the complement of a language L. We do not recall the general definition for Kondacs-Watrous QFA, which can be found in [11]. The definition of RFA is obtained from Kondacs-Watrous QFA by adding the restriction that any transition is deterministic:

Definition 2.1. *A reversible finite automaton* $\mathcal{A} = (Q, \Sigma \cup \{\$\}, q_0, Q_a, Q_r, \cdot)$ *is specified by a finite set of states* Q*, a finite input alphabet* Σ*, an end-marker* $\$ \notin \Sigma$ *and an initial state* $q_0 \in Q$*. The set* Q *is the union of two disjoint subsets* Q_h *and* Q_n*, called the set of halting and non-halting states, respectively. Further, the set* Q_h *is the union of two disjoint subsets* Q_a *and* Q_r *of* Q*, called the set of accepting and rejecting states, respectively. The transition function* $(q, \sigma) \to q\cdot\sigma$ *from* $Q \times (\Sigma \cup \{\$\})$ *into* Q *satisfies the following conditions:*

$$\text{for all } \sigma \in \Sigma \cup \{\$\}, \quad q_1\cdot\sigma = q_2\cdot\sigma \text{ implies } q_1 = q_2; \tag{1}$$

$$\text{if } q \text{ is non-halting, then } q\cdot\$ \text{ is halting.} \tag{2}$$

The first condition is equivalent to each letter $\sigma \in \Sigma \cup \{\$\}$ inducing a bijection on Q. A RFA reads any input word starting with the first letter. As soon as the automaton enters a halting state, the computation is halted and the word is either accepted or rejected, depending on whether the state is accepting or rejecting. The end-marker \$ insures that any word is either accepted or rejected.

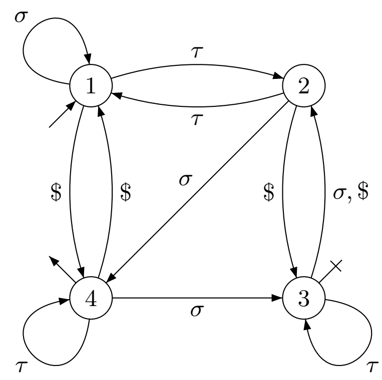

Fig. 1. A reversible finite automaton.

In the example of Figure 1, state 4 is accepting and state 3 is rejecting. States 1 and 2 are non-halting.

A reversible finite automaton is called *end-decisive* [9], if it accepts a word only after reading the end-marker \$. Dually, if the automaton rejects a word only after reading \$, it is called *co-end-decisive*. If a reversible finite automaton is either end-decisive or co-end-decisive, it will be called a *deterministic Brodsky-Pippenger automaton* (DBPA).

It can be noticed that any RFA $\mathcal{A} = (Q, \Sigma \cup \{\$\}, q_0, Q_a, Q_r, \cdot)$ can be transformed into a classical finite automaton $\mathcal{B} = (Q, \Sigma, q_0, F, \cdot_{\mathcal{B}})$, where $F = Q_a \cup \{q \in Q_n \mid q\cdot \$ \in Q_a\}$ and the new transition function is defined in the following way: for all $\sigma \in \Sigma$ and $q \in Q$,

$$q \cdot_{\mathcal{B}} \sigma = \begin{cases} q\cdot\sigma & \text{if } q \text{ is non-halting,} \\ q & \text{if } q \text{ is halting.} \end{cases} \tag{3}$$

By eliminating in $\mathcal{B}$ the states which are not accessible from the initial state, we obtain an automaton $\mathcal{A}' = (Q', \Sigma, q_0, F', \cdot)$, where $F' = Q' \cap F$, which recognizes the same language as $\mathcal{A}$. For instance, if $\mathcal{A}$ is the automaton represented in Figure 1, the automata $\mathcal{B}$ and $\mathcal{A}'$ are represented in Figure 2.

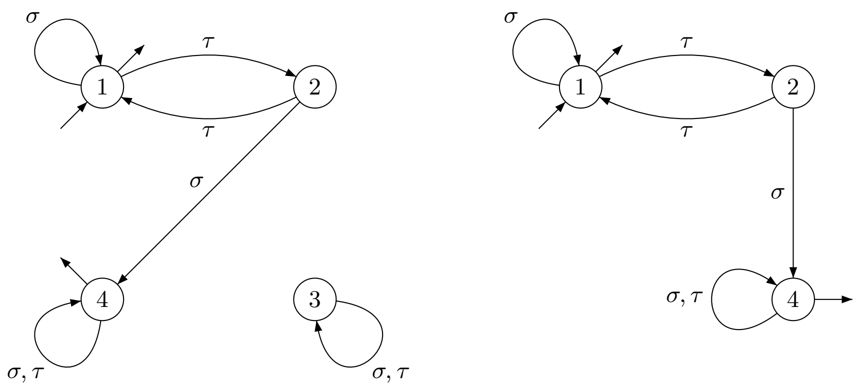

Fig. 2. The automata $\mathcal{B}$ and $\mathcal{A}'$.

A state q such that, for every $\sigma \in \Sigma$, $q \cdot_{\mathcal{B}} \sigma = q$, will be called *absorbing*.

Proposition 2.2. *If $\mathcal{A}'$ is non-trivial, a state of Q' is absorbing if and only if it is halting.*

Consider the non-absorbing states of $\mathcal{A}'$, which are also, by Proposition 2.2, the non-halting states. It follows from (3) that each letter of Σ acts on these states as a partial injective function. All the absorbing states in F' are equivalent, so they can be merged. The same applies to non-final absorbing states.

The resulting deterministic automaton is equivalent to $\mathcal{A}$. It has at most two absorbing states and each letter defines a partial injective function on the set of non-absorbing states. An automaton with these properties will be called a *classical reversible finite automaton* (CRFA). Conversely, it is possible to show that any CRFA can be transformed into an equivalent RFA. Thus we have established the following result.

Proposition 2.3. *Any RFA is equivalent to some CRFA. Conversely, any CRFA is equivalent to some RFA.*

If a CRFA has no absorbing states, it is a *group automaton* (all letters define permutations on the set of states) and it recognizes a *group language*. If it has at most one absorbing state, it will be called an injective finite automaton (IFA), to illustrate the connection of this model to partial injective functions, as discussed in the next section. Similarly as RFA are equivalent to CRFA, IFA are equivalent to DBPA. We call IFA-A (resp. IFA-R) an injective automaton whose absorbing state (if it exists) is final (resp. nonfinal). IFA-A are equivalent to co-end-decisive automata and IFA-R to end-decisive automata. As we shall later see, the closure of IFA-R under finite union is equivalent to Pin's reversible automata [16, 17].

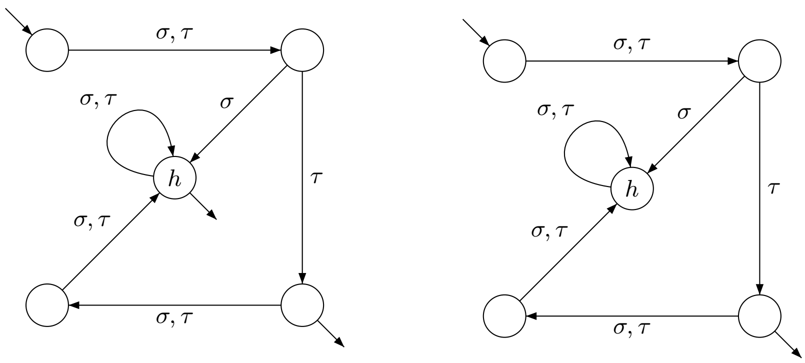

Fig. 3. An IFA-A (on the left) and an IFA-R (on the right).

3 Varieties

If x is an element of a monoid M, we denote by x^ω the unique idempotent of the subsemigroup of M generated by x.

An *ordered monoid* $(M, \leq)$ is a monoid M equipped with a *stable* order relation $\leq$ on M which means that, for every $u, v, x \in M$, $u \leq v$ implies $ux \leq vx$ and $xu \leq xv$.

Let M be a monoid and let s be an element of M. An *inverse* of s is an element $\bar{s}$ such that $s\bar{s}s = s$ and $\bar{s}s\bar{s} = \bar{s}$. An *inverse monoid* is a monoid in which every element has exactly one inverse. It is well known that the relation $\leq$ on M defined by

$$x \leq y \text{ if and only if } x = ye \text{ for some idempotent } e \text{ of } M$$

is a stable partial order, called the *natural order* of M.

Following [20], we call *ordered inverse monoid* an inverse monoid M, equipped with its natural order. We also call *dually ordered inverse monoid* an inverse monoid ordered by the dual order of its natural order.

A general overview on varieties of finite semigroups and monoids is given in [15], whereas introduction to varieties of ordered semigroups and monoids can be found in [18]. Given two varieties of ordered monoids $\mathbf{V}$ and $\mathbf{W}$, their semidirect product $\mathbf{V} * \mathbf{W}$ and Malcev product $\mathbf{V} Ⓜ \mathbf{W}$ are defined as in [20]. Theorems in [20, Section 3] imply that the semidirect product is an associative operation on varieties of ordered monoids.

In this paper, we shall use the following varieties of ordered monoids, which are defined by some simple identities:

(1) $\mathbf{G} = [\![x^\omega = 1]\!]$, the variety of groups;
(2) $\mathbf{J_1} = [\![x^2 = x,\ xy = yx]\!]$, the variety of commutative and idempotent monoids;
(3) $\mathbf{J_1^+} = [\![x^2 = x,\ x \le 1]\!]$, the variety of ordered idempotent monoids in which the identity is the maximum element. Order implies $xy \le y$, $xy \le x$, and since monoids are idempotent, $xy \le yx$. Hence $xy = yx$, and $\mathbf{J_1^+} \subset \mathbf{J_1}$;
(4) $\mathbf{J_1^-} = [\![x^2 = x,\ 1 \le x]\!]$, the variety of ordered idempotent monoids in which the identity is the minimal element. Similarly, $\mathbf{J_1^-} \subset \mathbf{J_1}$;
(5) $\mathbf{R_1} = [\![xyx = xy]\!]$, the variety of idempotent and $\mathcal{R}$-trivial monoids;
(6) $\mathbf{ECom} = [\![x^\omega y^\omega = y^\omega x^\omega]\!]$, the variety of monoids with commuting idempotents: the set of idempotents form a submonoid which belongs to the variety $\mathbf{J_1}$. This variety is known [7] to be equal to $\mathbf{Inv}$, the variety of monoids generated by inverse monoids. Further, by [12], $\mathbf{Inv} = \mathbf{J_1} * \mathbf{G} = \mathbf{J_1} Ⓜ \mathbf{G} = \mathbf{ECom}$;
(7) $\mathbf{ECom}^+ = [\![x^\omega y^\omega = y^\omega x^\omega,\ x^\omega \le 1]\!]$, the variety of ordered monoids whose idempotents form an ordered submonoid which belongs to the variety $\mathbf{J_1^+}$. This variety is known [20] to be equal to $\mathbf{Inv}^+$, the variety of ordered monoids generated by ordered inverse monoids, and also to $\mathbf{J_1^+} * \mathbf{G}$;
(8) $\mathbf{ECom}^- = [\![x^\omega y^\omega = y^\omega x^\omega,\ 1 \le x^\omega]\!]$ the variety of ordered monoids whose idempotents form an ordered submonoid which belongs to the variety $\mathbf{J_1^-}$. One can show that this variety is equal to $\mathbf{Inv}^-$, the variety of ordered monoids generated by dually ordered inverse monoids, and also to $\mathbf{J_1^-} * \mathbf{G}$.

By Vagner-Preston theorem [24, 23], transition monoids of IFA, IFA-A, IFA-R generate the varieties $\mathbf{Inv}$, $\mathbf{Inv}^+$, $\mathbf{Inv}^-$, respectively. We elaborate this fact in the next section.

4 Injective Finite Automata

In this section we shall describe the languages recognized by IFA, as well as an algebraic characterization of the boolean closure of this class of languages. The transition monoid generated by an injective automaton is isomorphic to a submonoid of the monoid of injective partial functions from a finite set into itself, which justifies the name chosen for the model.

The classes of languages recognized by IFA-A and IFA-R will be denoted by $\mathbf{L}$ and $\mathbf{L^c}$, respectively. The intersection of $\mathbf{L}$ and $\mathbf{L^c}$ is the class of group languages. Recall that a class of languages is closed under inverse morphism if for any monoid morphism $\varphi : \Sigma^* \to \Gamma^*$ and for any language L in the class, the language $\varphi^{-1}(L)$ is also in the class. Given a word u and a language L of Σ^*, recall that the quotient of L by u on the left (resp. right) is the language $u^{-1}L = \{v \in \Sigma^* \mid uv \in L\}$ (resp. $Lu^{-1} = \{v \in \Sigma^* \mid vu \in L\}$).

Theorem 4.1. *The classes* $\mathbf{L}$ *and* $\mathbf{L^c}$ *are closed under inverse morphisms and word quotients. Furthermore, the class* $\mathbf{L}$ *is closed under finite union and the class* $\mathbf{L^c}$ *under finite intersection.*

Theorem 4.2. *A language of* Σ^* *is in* $\mathbf{L}$ *if and only if it is of the form* $L_0 \cup \left(\bigcup_{\sigma\in\Sigma} L_\sigma \sigma \Sigma^*\right)$*, where* L_0 *and the* L_σ *are group languages.*

Proof. First, if $L \subset \Sigma^*$ is a group-language and $\sigma \in \Sigma$, the languages L and $L\sigma\Sigma^*$ are recognized by IFA-A and therefore are in $\mathbf{L}$. Since by Theorem 4.1, $\mathbf{L}$ is closed under finite union, the languages described in the statement are in $\mathbf{L}$.

Consider now a language L recognized by an IFA-A $\mathcal{A} = (Q, \Sigma, q_0, F, \cdot)$ having an absorbing state h. Let $P = Q \setminus \{h\}$. Each letter of Σ induces an injective partial map on P. Completing these partial maps to bijections in an arbitrary way, we obtain a bijective automaton $\mathcal{B} = (Q, \Sigma, \cdot_{\mathcal{B}})$. Let L_0 be the language recognized by the automaton $\mathcal{A}_0 = (Q, \Sigma, q_0, F \setminus \{h\}, \cdot_{\mathcal{B}})$ and, for each letter $\sigma \in \Sigma$, let L_σ be the language recognized by the automaton $\mathcal{A}_\sigma = (Q, \Sigma, q_0, F_\sigma, \cdot_{\mathcal{B}})$, where $F_\sigma = \{q \in P \mid q \cdot \sigma = h\}$. If L is the language recognized by the IFA-A represented in Figure 3, the three automata $\mathcal{A}_0$, $\mathcal{A}_\sigma$ and $\mathcal{A}_\tau$ are pictured in Figure 4. Then by construction, $L = L_0 \cup \bigcup_{\sigma\in\Sigma^*} L_\sigma \sigma \Sigma^*$. $\square$

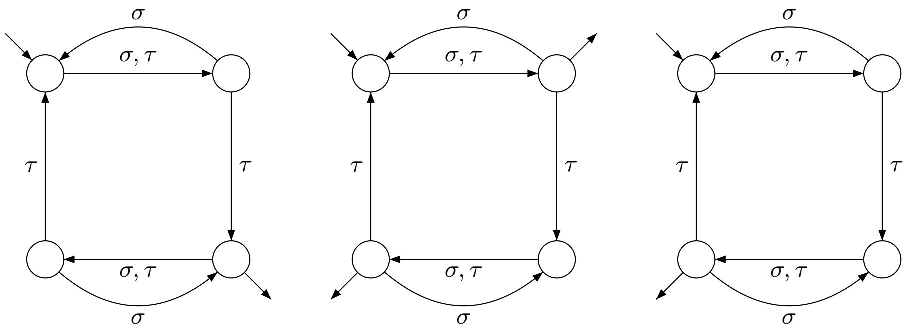

Fig. 4. The automata $\mathcal{A}_0$, $\mathcal{A}_\sigma$ and $\mathcal{A}_\tau$, respectively.

Corollary 4.3. *A language of* Σ^* *is recognized by an IFA-R if and only if it can be written as* $L_0 \cap \left(\bigcap_{\sigma\in\Sigma} (L_\sigma\sigma\Sigma^*)^c\right)$*, where* L_0 *and the* L_σ *are group languages.*

So the class of languages recognized by IFA is characterized by Theorem 4.2 and Corollary 4.3.

By Theorem 4.1, $\mathbf{L}$ ($\mathbf{L^c}$, respectively) is closed under finite union (finite intersection), inverse morphisms and word quotients. Nevertheless, one can show that $\mathbf{L}$ ($\mathbf{L^c}$, respectively) does not form a disjunctive (conjunctive) variety in the sense of Polák [22], since it is not closed under inverse free semiring morphisms $\psi^{(-1)}$ ($\psi^{[-1]}$) defined there.

Consider the closure of $\mathbf{L}$ under finite intersection. The resulting class of languages is a positive variety of languages. By [21, Theorem 4.4], the corresponding variety of ordered monoids is $\mathbf{J_1^+} * \mathbf{G} = \mathbf{ECom}^+$. Combining this result with the description of the languages of $\mathbf{L}$ given by Theorem 4.2, we obtain the following result:

Proposition 4.4. *Let Z be a language of Σ^*. The following conditions are equivalent:*

(1) *Z belongs to the closure of $\mathbf{L}$ under finite intersection,*

(2) *Z is a positive boolean combination of languages of the form L or $L\sigma\Sigma^*$, where L is a group language,*

(3) *The syntactic ordered monoid of Z belongs to the variety $\mathbf{ECom}^+$.*

Similarly, the closure of $\mathbf{L^c}$ under finite union is exactly the class of languages recognized by Pin's reversible automata and the corresponding variety of ordered monoids is $\mathbf{ECom}^- = [\![x^\omega y^\omega = y^\omega x^\omega,\ x^\omega \geq 1]\!]$ [16, 17].

Finally, by [12], the closure of $\mathbf{L}$ or $\mathbf{L^c}$ under boolean operations corresponds to the monoid variety $\mathbf{ECom}$, defined by the identity $x^\omega y^\omega = y^\omega x^\omega$.

5 Reversible Finite Automata

The class of languages recognized by CRFA (which, by Proposition 2.3, is also the class of languages recognized by RFA) will be denoted by $\mathbf{K}$.

In this section give a necessary condition for membership in $\mathbf{K}$, as well as an algebraic characterization of the boolean closure $\overline{\mathbf{K}}$ of this class of languages.

Theorem 5.1. *Any language of Σ^* recognized by a CRFA can be written as $K_0 \cup K_1\sigma_1\Sigma^* \cup \cdots \cup K_k\sigma_k\Sigma^*$, where $K_0, \ldots, K_k \in \mathbf{L^c}$ and $\sigma_1, \ldots, \sigma_k$ are letters.*

Proof. Consider a language Z recognized by a CRFA $\mathcal{A} = (Q, \Sigma, q_0, F, \cdot)$. If $\mathcal{A}$ has less than two absorbing states, the result follows from Theorem 4.2. Hence assume that $\mathcal{A}$ has two absorbing states: a non-final state g and a final state h. Let $J = Q \setminus \{h\}$. We first decompose Z as the union of two languages K_0 and Z_1. The language K_0 is recognized by the automaton $\mathcal{A}_0 = (J, \Sigma, q_0, F \setminus \{h\}, \cdot')$, where

$$q \cdot' \sigma = \begin{cases} q\cdot\sigma & \text{if } q\cdot\sigma \in J, \\ g & \text{otherwise.} \end{cases}$$

Then $\mathcal{A}_0$ is an IFA-R and thus $K \in \mathbf{L^c}$. The language Z_1 is recognized by the automaton $\mathcal{A}_1 = (Q, \Sigma, q_0, \{h\}, \cdot)$. For each transition in

$$T = \{(q, \sigma) \in J \times \Sigma \mid q\cdot\sigma = h\}$$

create an automaton $\mathcal{A}_{q,\sigma} = (Q, \Sigma, q_0, \{h\}, \cdot_{q,\sigma})$, where

$$p \cdot_{q,\sigma} \tau = \begin{cases} p\cdot\tau & \text{if } (p,\tau) \notin T \text{ or } (p,\tau) = (q,\sigma) \\ g & \text{otherwise.} \end{cases}$$

Denoting by $Z_{(q,\sigma)}$ the language recognized by $\mathcal{A}_{(q,\sigma)}$, we obtain $Z = \bigcup_{(q,\sigma)\in T} Z_{(q,\sigma)}$. Further, $Z_{(q,\sigma)} = K_{q,\sigma}\sigma\Sigma^*$, where $K_{q,\sigma}$ is the language in $\mathbf{L^c}$ that is recognized by the automaton $(J, \Sigma, q_0, \{q\}, \cdot'_{q,\sigma})$, where $\cdot'_{q,\sigma}$ is the restriction of $\cdot_{q,\sigma}$ to J, completed by the transition $q \cdot'_{q,\sigma} \sigma = g$. Hence $Z = K_0 \cup \big(\bigcup_{(q,\sigma)\in T} K_{q,\sigma}\sigma\Sigma^*\big)$. $\square$

Note that given a language $K \subseteq \Sigma^*$ of $\mathbf{L^c}$ and $\sigma \in \Sigma$, the language $K\sigma\Sigma^*$ is recognized by a CRFA.

Theorem 5.2. *The class* $\mathbf{K}$ *is closed under complement, inverse of morphisms between free monoids and word quotients.*

Corollary 5.3. *If a language of* Σ^* *is recognized by a CRFA, then it can be written as* $K_0^c \cap (K_1\sigma_1\Sigma^*)^c \cap \cdots \cap (K_k\sigma_k\Sigma^*)^c$*, where* $k \geq 0$*,* $K_0, \ldots, K_k \in \mathbf{L^c}$ *and* $\sigma_1, \ldots, \sigma_k \in \Sigma$*.*

Since $\mathbf{K}$ is closed under complement, its closure under positive boolean operations (finite unions and intersections) is equal to its boolean closure $\overline{\mathbf{K}}$.

Theorem 5.4. *A language belongs to* $\overline{\mathbf{K}}$ *if and only if its syntactic ordered monoid belongs to* $\mathbf{J_1^+} * (\mathbf{J_1^-} * \mathbf{G})$*.*

Proof. Let L be a regular language and let $M(L)$ be its syntactic ordered monoid. If $L \in \overline{\mathbf{K}}$, then it is by Theorem 5.1 a positive boolean combination of languages of the form K or $K\sigma\Sigma^*$, where $K \in \mathbf{L^c}$. Thus by the [16, 17], $M(K) \in \mathbf{ECom}^- = \mathbf{J_1^-} * \mathbf{G}$. Therefore by [21, Theorem 4.4], $M(L) \in \mathbf{J_1^+} * (\mathbf{J_1^-} * \mathbf{G})$.

Suppose now that $M(L) \in \mathbf{J_1^+} * (\mathbf{J_1^-} * \mathbf{G})$. Then by [21, Theorem 4.4], L is a positive boolean combination of languages of the form Z or $Z\sigma\Sigma^*$, where $M(Z) \in \mathbf{J_1^-} * \mathbf{G}$. Further, Z is a positive boolean combination of languages of the form Y_i and $(Y_j\sigma\Sigma^*)^c$, where Y_i, Y_j are group languages. So $Z = \bigcup_i K_i$, where $K_i \in \mathbf{L^c}$. Now $Z\sigma\Sigma^* = (\bigcup_i K_i)\sigma\Sigma^* = \bigcup_i (K_i\sigma\Sigma^*)$. Hence $L \in \overline{\mathbf{K}}$. □

By associativity, $\mathbf{J_1^+} * (\mathbf{J_1^-} * \mathbf{G}) = (\mathbf{J_1^+} * \mathbf{J_1^-}) * \mathbf{G}$, hence it is of interest to describe the variety $\mathbf{J_1^+} * \mathbf{J_1^-}$. Due to the lack of space, we omit the proof of this semigroup theoretic result.

Theorem 5.5. *The following equality holds:* $\mathbf{J_1^+} * \mathbf{J_1^-} = \mathbf{J_1^-} * \mathbf{J_1^+} = \mathbf{R_1}$*.*

The variety of monoids $\mathbf{R_1}$ is defined by the identity $xyx = xy$. Hence by [2], Corollary 4.3 and [1], p. 276, $\mathbf{R_1} * \mathbf{G} = [\![x^\omega y^\omega x^\omega = x^\omega y^\omega]\!]$.

The facts exposed above yield the following theorem, which essentially says that the languages recognized by RFA generate the variety $\mathbf{R_1} * \mathbf{G}$:

Theorem 5.6. *A language is in* $\overline{\mathbf{K}}$ *if and only if its syntactic monoid belongs to the variety* $\mathbf{R_1} * \mathbf{G} = [\![x^\omega y^\omega x^\omega = x^\omega y^\omega]\!]$*.*

6 Algebraic Conditions

Let us note that Ambainis and Freivalds have proved ([5], theorems 2 and 3) the following characterization for the class of languages recognized by RFA:

Theorem 6.1. [5] *Let* $\mathcal{A}$ *be the minimal automaton of a regular language* L*. Then* L *is recognized by a reversible finite automaton if and only if for any states* q_1, q_2, q_3 *of* $\mathcal{A}$*,* $q_1 \neq q_2$*,* $q_2 \neq q_3$*, and for any input words* x, y*,* $\mathcal{A}$ *does not contain the following configuration:* $q_1 \cdot x = q_2$*,* $q_2 \cdot x = q_2$*,* $q_2 \cdot y = q_3$*.*

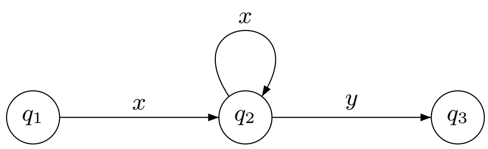

Fig. 5. The forbidden configuration in a RFA.

The Ambainis-Freivalds condition can be translated into an algebraic condition. Let L a regular language of Σ^*. We denote by $M(L)$ its syntactic monoid, by $\varphi : \Sigma^* \longrightarrow M(L)$ its syntactic morphism and by $P = \varphi(L)$ the syntactic image of L. Let $\sim_r$ be the right congruence on $M(L)$ defined by $s \sim_r t$ if and only if, for all $u \in M(L)$, $su \in P$ is equivalent to $tu \in P$.

Corollary 6.2. *L is recognized by a reversible finite automaton if and only if for all $s, t, u \in M(L)$, $st^\omega \sim_r s$ or $st^\omega u \sim_r st^\omega$.*

Proof. Consider the minimal automaton $(Q, \Sigma, q_0, F, \cdot)$ of a language L. Due to Ambainis-Freivalds condition, a language is recognized by a reversible finite automaton if and only if for all $q_1, q_2, q_3 \in Q$ and $x, y \in \Sigma^*$,

$$q_1 \cdot x = q_2,\ q_2 \cdot x = q_2 \text{ and } q_2 \cdot y = q_3 \text{ imply } q_1 = q_2 \text{ or } q_2 = q_3$$

or, equivalently, for all $q \in Q$, for all $x, y \in \Sigma^*$,

$$q \cdot x = q \cdot x^2 \text{ implies } q = q \cdot x \text{ or } q \cdot x = q \cdot xy.$$

Now, choose $v \in \Sigma^*$ such that $q = q_0 \cdot v$ and let $s = \varphi(v)$ and $t = \varphi(x)$. We claim that the condition $q \cdot x = q \cdot x^2$ is equivalent to $st \sim_r st^2$. Indeed, by the definition of the Nerode equivalence, the first condition means that, for every $y \in \Sigma^*$, $q_0 \cdot vxy \in F$ if and only if $q_0 \cdot vx^2y \in F$, or, equivalently, for all $u \in M(L)$, $stu \in P$ if and only if $st^2u \in P$.

Therefore, Formula (6) can be rewritten as follows: for all $s, t, u \in M(L)$,

$$st \sim_r st^2 \text{ implies } s \sim_r st \text{ or } st \sim_r stu,$$

which is in turn equivalent to: for all $s, t, u \in M(L)$,

$$s \sim_r st^\omega \text{ or } st^\omega \sim_r st^\omega u.$$

□

Consider an injective automaton $\mathcal{A}$, which is not a group automaton, i.e., has one absorbing state. We assume that $\mathcal{A}$ is accessible. Then for any state q and any word w, exists $k > 0$ such that $q \cdot w^k = q$ or $q \cdot w^k = h$, where h is the absorbing state. Therefore we deduce that the absorbing state is accessible from any state. So the transition monoid $M(\mathcal{A})$ has a zero element ([15, Exercise 2.7]). Since $M(L)$ divides $M(\mathcal{A})$, $M(L)$ also has a zero element. One can view the syntactic monoid $M(L)$ as an automaton $(M(L), \Sigma, 1, P, \cdot)$, which recognizes L. Any of its states is accessible from the initial state 1. The right equivalence class containing 0 corresponds to the absorbing state in the minimal automaton of L. All the absorbing states of $M(L)$ are in this class. Hence if for every u $st^\omega \sim_r st^\omega u$, then $st^\omega \sim_r 0$. So in the case of DBPA, Corollary 6.2 may be rewritten as follows:

Corollary 6.3. *A language L is recognized by a deterministic Brodsky-Pippenger automaton if and only if, for all $s, t \in M(L)$, $st^\omega \sim_r s$ or $st^\omega \sim_r 0$.*

If L is a group language, $M(L)$ does not have a zero, so this condition reduces to: for all $s, t \in M(L)$, $st^\omega \sim_r s$, which is turn equivalent to $t^\omega = 1$.

References

1. J. Almeida. Finite Semigroups and Universal Algebra. *World Scientific*, Singapore, 1994.
2. J. Almeida, J.E. Pin, P. Weil. Semigroups whose Idempotents Form a Subsemigroup. *Math. Proc. Camb. Phil. Soc.*, Vol. 111, pp. 241-253, 1992.
3. A. Ambainis, M. Beaudry, M. Golovkins, A. Ķikusts, M. Mercer, D. Thérien. Algebraic Results on Quantum Automata. *STACS 2004, LNCS*, Vol. 2996, pp. 93-104, 2004.
4. A. Ambainis, R.F. Bonner, R. Freivalds, A. Ķikusts. Probabilities to Accept Languages by Quantum Finite Automata. *COCOON 1999, LNCS*, Vol. 1627, pp. 174-183, 1999.
5. A. Ambainis, R. Freivalds. 1-Way Quantum Finite Automata: Strengths, Weaknesses and Generalizations. *Proc. 39th FOCS*, pp. 332-341, 1998.
6. A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani. Dense Quantum Coding and Quantum Finite Automata. *Journal of the ACM*, Vol. 49(4), pp. 496-511, 2002.
7. C.J. Ash. Finite Semigroups with Commuting Idempotents. *J. Austral. Math. Soc. (Series A)*, Vol. 43, pp. 81-90, 1987.
8. A. Bertoni, C. Mereghetti, B. Palano. Quantum Computing: 1-Way Quantum Finite Automata. *DLT 2003, LNCS*, Vol. 2710, pp. 1-20, 2003.
9. A. Brodsky, N. Pippenger. Characterizations of 1-Way Quantum Finite Automata. *SIAM Journal on Computing*, Vol. 31(5), pp. 1456-1478, 2002.
10. M. Golovkins, M. Kravtsev. Probabilistic Reversible Automata and Quantum Automata. *COCOON 2002, LNCS*, Vol. 2387, pp. 574-583, 2002.
11. A. Kondacs, J. Watrous. On The Power of Quantum Finite State Automata. *Proc. 38th FOCS*, pp. 66-75, 1997.
12. S.W. Margolis, J.E. Pin. Inverse Semigroups and Varieties of Finite Semigroups. *Journal of Algebra*, Vol. 110, pp. 306-323, 1987.
13. C. Moore, J.P. Crutchfield. Quantum Automata and Quantum Grammars. *Theoretical Computer Science*, Vol. 237(1-2), pp. 275-306, 2000.
14. A. Nayak. Optimal Lower Bounds for Quantum Automata and Random Access Codes. *Proc. 40th FOCS*, pp. 369-377, 1999.
15. J.E. Pin. Varieties of Formal Langages, North Oxford, London and Plenum, New-York, 1986.
16. J.E. Pin. On the Languages Accepted by Finite Reversible Automata. *ICALP 1987, LNCS*, Vol. 267, pp. 237-249, 1987.
17. J.E. Pin. On Reversible Automata. *LATIN 1992, LNCS*, Vol. 583, pp. 401-416, 1992.
18. J.E. Pin. Eilenberg's Theorem for Positive Varieties of Languages. *Russian Mathematics (Iz. VUZ)*, Vol. 39(1), pp. 80-90, 1995.
19. J.E. Pin, H. Straubing, D. Thérien. Small Varieties of Finite Semigroups and Extensions. *J. Austral. Math. Soc. (Series A)*, Vol. 37, pp. 269-281, 1984.
20. J.E. Pin, P. Weil. Semidirect Products of Ordered Semigroups. *Communications in Algebra*, Vol. 30(1), pp. 149-169, 2002.
21. J.E. Pin, P. Weil. The Wreath Product Principle for Ordered Semigroups. *Communications in Algebra*, Vol. 30(12), pp. 5677-5713, 2002.
22. L. Polák. Syntactic Semiring of a Language. *MFCS 2001, LNCS*, Vol. 2136, pp. 611-620, 2001.
23. G.B. Preston. Inverse Semi-groups with Minimal Right Ideals. *J. London Math. Soc.*, Vol. 29, pp. 404-411, 1954.
24. V.V. Vagner. Generalized Groups. *Dokl. Akad. Nauk SSSR*, Vol. 84(6), pp. 1119-1122, 1952.