

# The finiteness of a group generated by a 2-letter invertible-reversible Mealy automaton is decidable

Ines Klimann

► **To cite this version:**

Ines Klimann. The finiteness of a group generated by a 2-letter invertible-reversible Mealy automaton is decidable. Natacha Portier and Thomas Wilke. 30th International Symposium on Theoretical Aspects of Computer Science (STACS 2013), Feb 2013, Kiel, Germany. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 20, pp.502–513, 2013, <10.4230/LIPIcs.STACS.2013.502>. <hal-00875177>

**HAL Id: hal-00875177**

**<https://hal-univ-diderot.archives-ouvertes.fr/hal-00875177>**

Submitted on 21 Oct 2013

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# The finiteness of a group generated by a 2-letter invertible-reversible Mealy automaton is decidable

Ines Klimann\*

Univ Paris Diderot, Sorbonne Paris Cité, LIAFA,  
UMR 7089 CNRS, F-75013 Paris, France  
klimann@liafa.univ-paris-diderot.fr

---

## Abstract

We prove that a semigroup generated by a reversible two-state Mealy automaton is either finite or free of rank 2. This fact leads to the decidability of finiteness for groups generated by two-state or two-letter invertible-reversible Mealy automata and to the decidability of freeness for semigroups generated by two-state invertible-reversible Mealy automata.

**1998 ACM Subject Classification** F.4.3

**Keywords and phrases** Mealy automata, automaton semigroups, decidability of finiteness, decidability of freeness, Nerode equivalence

**Digital Object Identifier** 10.4230/LIPIcs.xxx.yyy.p

## 1 Introduction

*Automaton (semi)groups* — short for semigroups generated by Mealy automata and groups generated by invertible Mealy automata — were formally introduced half a century ago (for details, see [14, 9] and references therein). Over the years, important results have started revealing their full potential, by contributing to important conjectures in group theory, as Milnor problem (first example of a group of intermediate growth) or Burnside problem (example of a very simple Mealy automaton generating an infinite torsion group).

In a way, semigroups can be classified according to their growth function: at one end stand finite semigroups and at the other one free semigroups. Several sufficient or necessary criteria for finiteness of automaton semigroups exist [2, 15, 9, 16, 17, 22, 4, 8, 21], but deciding finiteness of such semigroups is still an open problem. As to freeness, it has been and it is still a challenge: only some particular invertible Mealy automata, possibly parametrized, have been shown to generate free groups [23, 11, 19, 24, 25]; and some Cayley automaton semigroups have been shown to be free [22].

In this paper, we link both issues for semigroups generated by reversible two-state Mealy automata: we prove that such semigroups are either finite or free, in this latter case the states of the generating Mealy automaton being free generators of the semigroup, answering a conjecture stated in [15]. On the basis of this dichotomy between finite and free semigroups, we prove that finiteness and freeness of the semigroup are decidable if the generating reversible two-state Mealy automaton is also invertible. Decidability of finiteness extends by duality to groups generated by two-letter invertible-reversible Mealy automata. The problems of deciding finiteness or freeness of automaton semigroups was raised by Grigorchuk, Nekrashevych, and Sushchanskii [14, Problem 7.2.1(b)].

---

\* The author is partially supported by ANR Project MealyM ANR-JCJC-12-JS02-012-01.

Specializing to two letters or states may seem to be a strong restriction, but most of the significant examples in literature have faced this restriction: the first example of a finitely generated group of intermediate growth, the Grigorchuk group [13, 14], is generated by a two-letter Mealy automaton while the very smallest Mealy automaton with intermediate growth [6] has two letters and two states; the lamplighter group [12] is generated by a two-letter and two-state Mealy automaton; the Aleshin automaton [3, 24] gives the simplest example of a free automaton group and has two letters. The article [7] is entirely devoted to the study of groups generated by 3-state 2-letter invertible Mealy automata.

This paper is organized as follows. In Section 2 we define Mealy automata and automaton (semi)groups. Basic tools to manipulate them are introduced in Section 3. Section 4 is devoted to the dichotomy between free and finite semigroups. The decidability results are proved in Section 5. The cornerstone of our proofs and constructions is the very classical Nerode equivalence used to minimize automata.

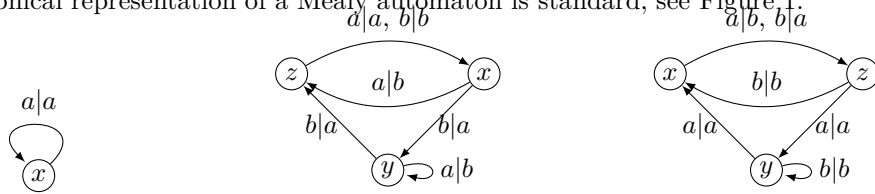
## 2 (Semi)groups generated by Mealy automata

### 2.1 Mealy automata

If one forgets initial and final states, a (*finite, deterministic, and complete*) automaton  $\mathcal{A}$  is a triple  $(A, \Sigma, \delta = (\delta_i : A \rightarrow A)_{i \in \Sigma})$ , where the *stateset*  $A$  and the *alphabet*  $\Sigma$  are non-empty finite sets, and where the  $\delta_i$  are functions.

A *Mealy automaton* is a quadruple  $(A, \Sigma, \delta = (\delta_i : A \rightarrow A)_{i \in \Sigma}, \rho = (\rho_x : \Sigma \rightarrow \Sigma)_{x \in A})$ , such that both  $(A, \Sigma, \delta)$  and  $(\Sigma, A, \rho)$  are automata. In other terms, a Mealy automaton is a letter-to-letter transducer with the same input and output alphabet.

The graphical representation of a Mealy automaton is standard, see Figure 1.



(a) The trivial aut.

(b) The Aleshin automaton.

(c) The Baby-Aleshin aut.

■ **Figure 1** Examples of Mealy automata: the Aleshin automaton generates the rank 3 free group [3, 24], the Baby-Aleshin automaton generates the free product  $\mathbb{Z}_2^{*3} = \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$  [19].

A Mealy automaton  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  is *invertible* if the functions  $\rho_x$  are permutations of  $\Sigma$  and *reversible* if the functions  $\delta_i$  are permutations of  $A$ .

In a Mealy automaton  $\mathcal{A} = (A, \Sigma, \delta, \rho)$ , the sets  $A$  and  $\Sigma$  play dual roles. So we may consider the *dual (Mealy) automaton* defined by  $\mathfrak{d}(\mathcal{A}) = (\Sigma, A, \rho, \delta)$ . Obviously, a Mealy automaton is reversible if and only if its dual is invertible.

Considering the underlying graph of a Mealy automaton, it makes sense to look at the connected components of a Mealy automaton. Note that a connected component of a reversible Mealy automaton is always strongly connected: its  $(\delta_i : A \rightarrow A)_{i \in \Sigma}$  are permutations of a finite set and in particular they are surjective.

### 2.2 Automaton (semi)groups

Let  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  be a Mealy automaton. We view  $\mathcal{A}$  as an automaton with an input and an output tape, thus defining mappings from input words over  $\Sigma$  to output words over  $\Sigma$ .

Formally, for  $x \in A$ , the map  $\rho_x : \Sigma^* \rightarrow \Sigma^*$ , extending  $\rho_x : \Sigma \rightarrow \Sigma$ , is defined by:

$$\forall i \in \Sigma, \forall \mathbf{s} \in \Sigma^*, \quad \rho_x(i\mathbf{s}) = \rho_x(i)\rho_{\delta_i(x)}(\mathbf{s}).$$

By convention, the image of the empty word is itself. The mapping  $\rho_x$  is length-preserving and prefix-preserving. We say that  $\rho_x$  is the *production function* associated with  $(\mathcal{A}, x)$  or more briefly, if there is no ambiguity, the *production function* of  $x$ . For  $\mathbf{x} = x_1 \cdots x_n \in A^n$  with  $n > 0$ , set  $\rho_{\mathbf{x}} : \Sigma^* \rightarrow \Sigma^*$ ,  $\rho_{\mathbf{x}} = \rho_{x_n} \circ \cdots \circ \rho_{x_1}$ .

Denote dually by  $\delta_i : A^* \rightarrow A^*$ ,  $i \in \Sigma$ , the production functions associated with the dual automaton  $\mathfrak{d}(\mathcal{A})$ . For  $\mathbf{s} = s_1 \cdots s_n \in \Sigma^n$  with  $n > 0$ , set  $\delta_{\mathbf{s}} : A^* \rightarrow A^*$ ,  $\delta_{\mathbf{s}} = \delta_{s_n} \circ \cdots \circ \delta_{s_1}$ .

The semigroup of mappings from  $\Sigma^*$  to  $\Sigma^*$  generated by  $\rho_x, x \in A$ , is called the *semigroup generated by  $\mathcal{A}$*  and is denoted by  $\langle \mathcal{A} \rangle_+$ . When  $\mathcal{A}$  is invertible, its production functions are permutations on words of the same length and thus we may consider the group of mappings from  $\Sigma^*$  to  $\Sigma^*$  generated by  $\rho_x, x \in A$ ; it is called the *group generated by  $\mathcal{A}$*  and is denoted by  $\langle \mathcal{A} \rangle$ .

An invertible Mealy automaton generates a finite group if and only if it generates a finite semigroup [2]. A Mealy automaton generates a finite semigroup if and only if so does its dual [19, 20, 2].

### 3 Basic tools

In this section, we present basic tools to manipulate Mealy automata: Nerode equivalence and minimization of automata (§ 3.1) are classic constructions from automata theory,  $\mathfrak{m}\mathfrak{d}$ -reduction and  $\mathfrak{m}\mathfrak{d}$ -triviality (§ 3.2) have been introduced in [2] to give a sufficient condition for finiteness, portraits of automorphisms on a regular rooted tree (§ 3.3) come from geometric group theory and tensor closures (§ 3.4) are newly introduced in order to better control the structure of a Mealy automaton.

Let  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  be a Mealy automaton. A convenient and natural operation is to raise  $\mathcal{A}$  to the power  $n$ , for some  $n > 0$ : its  *$n$ -th power* is the Mealy automaton

$$\mathcal{A}^n = (A^n, \Sigma, (\delta_i : A^n \rightarrow A^n)_{i \in \Sigma}, (\rho_{\mathbf{u}} : \Sigma \rightarrow \Sigma)_{\mathbf{u} \in A^n}).$$

Note that the powers of a reversible Mealy automaton are reversible.

#### 3.1 Nerode equivalence and minimization of a Mealy automaton

**Throughout this subsection,  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  denotes a Mealy automaton.**

The *Nerode equivalence*  $\equiv$  on  $A$  is the limit of the sequence of increasingly finer equivalences  $(\equiv_k)$  recursively defined by:

$$\begin{aligned} \forall x, y \in A, \quad x \equiv_0 y &\iff \rho_x = \rho_y, \\ \forall k \geq 0, x \equiv_{k+1} y &\iff (x \equiv_k y \quad \wedge \quad \forall i \in \Sigma, \delta_i(x) \equiv_k \delta_i(y)). \end{aligned}$$

Since the set  $A$  is finite, this sequence is ultimately constant; moreover if two consecutive equivalences are equal, the sequence remains constant from this point on. The limit is therefore computable. For every element  $x$  in  $A$ , we denote by  $[x]$  (*resp.*  $[x]_k$ ) the class of  $x$  w.r.t. the Nerode equivalence (*resp.* the  $\equiv_k$  equivalence), called the *Nerode class* (*resp.* the  *$k$ -class*) of  $x$ . Extending to the  $n$ -th power of  $\mathcal{A}$ , we denote by  $[\mathbf{x}]$  the Nerode class in  $A^n$  of  $\mathbf{x} \in A^n$ .

The *minimization* of  $\mathcal{A}$  is the Mealy automaton  $\mathfrak{m}(\mathcal{A}) = (A/\equiv, \Sigma, \tilde{\delta}, \tilde{\rho})$ , where for every  $(x, i)$  in  $A \times \Sigma$ ,  $\tilde{\delta}_i([x]) = [\delta_i(x)]$  and  $\tilde{\rho}_{[x]} = \rho_x$ . This definition is consistent with the

standard minimization of “deterministic finite automata” where instead of considering the mappings  $(\rho_x : \Sigma \rightarrow \Sigma)_x$ , the computation is initiated by the separation between terminal and non-terminal states. Using the Hopcroft algorithm, the time complexity of minimization is  $\mathcal{O}(\Sigma A \log A)$ , see [1] –  $E$  being used here instead of  $\#E$ , for a set  $E$ , to simplify notations.

Two states of a Mealy automaton belong to the same Nerode class if and only if they represent the same element in the generated semigroup, i.e. if and only if they have the same production function  $\Sigma^* \rightarrow \Sigma^*$ . Two words on  $A$  of the same length  $n$  are *equivalent* if they belong to the same Nerode class in  $A^n$ . By extension, any two words on  $A$  are *equivalent* if they have the same production function. The set of all words equivalent to  $\mathbf{x} \in A^*$ , regardless of their length, is denoted by  $[\mathbf{x}]$ .

Two states of a Mealy automaton belong to the same  $k$ -class if and only if the restrictions of their production functions to  $\Sigma^k \rightarrow \Sigma^k$  are equal.

The following remarks will be useful for the rest of the paper:

► **Remark 1.** *Let  $n$  be an integer. If each word of  $A^n$  is equivalent to a strictly shorter word, then the semigroup  $\langle \mathcal{A} \rangle_+$  is finite, its set of elements being  $\{\rho_{\mathbf{u}}, \mathbf{u} \in A^{\leq n-1}\}$ .*

► **Remark 2.** *If two words of  $A^*$  are equivalent, so are their images under the action of each element of  $\langle \mathcal{A} \rangle_+$ .*

### 3.2 $\mathfrak{m}\mathfrak{d}$ -reduction and $\mathfrak{m}\mathfrak{d}$ -triviality

The  $\mathfrak{m}\mathfrak{d}$ -reduction and the  $\mathfrak{m}\mathfrak{d}$ -triviality were introduced in [2] to give a sufficient but not necessary condition of finiteness. We show in Section 5 that, in the case of a two-state or two-letter invertible-reversible Mealy automaton, this condition is actually necessary.

A pair of dual Mealy automata is *reduced* if both automata are minimal. The  $\mathfrak{m}\mathfrak{d}$ -reduction of a Mealy automaton consists in minimizing the automaton or its dual until the resulting pair of dual Mealy automata is reduced. It is well-defined: if both a Mealy automaton and its dual automaton are non-minimal, the reduction is confluent [2].

The trivial Mealy automaton (see Figure 1(a)) generates the trivial (semi)group. If the  $\mathfrak{m}\mathfrak{d}$ -reduction of a Mealy automaton  $\mathcal{A}$  leads to the trivial Mealy automaton,  $\mathcal{A}$  is said to be  *$\mathfrak{m}\mathfrak{d}$ -trivial*. It is decidable whether a Mealy automaton is  $\mathfrak{m}\mathfrak{d}$ -trivial. An  $\mathfrak{m}\mathfrak{d}$ -trivial Mealy automaton generates a finite semigroup, but in general the converse is false [2].

A priori the sequence of minimization-dualization can be arbitrarily long: the minimization of a Mealy automaton with a minimal dual can make the dual automaton non-minimal. Nevertheless, if the automaton has two states, the  $\mathfrak{m}\mathfrak{d}$ -reduction can be shortened to  $\mathfrak{m}\mathfrak{d}\mathfrak{m}\mathfrak{d}$ . Hence, in this particular case, the time complexity of the  $\mathfrak{m}\mathfrak{d}$ -reduction is  $\mathcal{O}(\Sigma \log \Sigma)$ .

### 3.3 Portrait of a word

**Throughout this subsection,  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  denotes an invertible Mealy automaton.**

The set  $\Sigma^*$  can naturally be thought of as a regular rooted tree; its root is the empty word and two words are connected if and only if they are of the form  $\mathbf{s}$  and  $\mathbf{s}i$ , with  $\mathbf{s} \in \Sigma^*$ ,  $i \in \Sigma$ . The set  $\Sigma^n$  is the  $n$ th level of  $\Sigma^*$ . A *branch* of the tree  $\Sigma^*$  is a sequence of words  $(\mathbf{s}_k)_{k \in \mathbb{N}}$  such that, for each  $k \in \mathbb{N}$ ,  $\mathbf{s}_k$  is of length  $k$  and is a prefix of  $\mathbf{s}_{k+1}$ .

An *automorphism* of  $\Sigma^*$  is a bijective map  $\Sigma^* \rightarrow \Sigma^*$  preserving the root and the adjacency of the vertices. Each state  $x$  of the automaton  $\mathcal{A}$  acts on the regular rooted tree  $\Sigma^*$  by the production rule  $\rho_x$ . The constructions of this subsection are directly inspired by this view

(see [19] and references therein for more details on automorphisms acting on regular rooted trees). Denote by  $Aut(\Sigma^*)$  the set of automorphisms of  $\Sigma^*$ .

Let  $g$  be an automorphism on the regular rooted tree  $\Sigma^*$ . For any word  $\mathbf{s} \in \Sigma^*$ , there exists a unique automorphism  $g_{|\mathbf{s}} : \Sigma^* \rightarrow \Sigma^*$  called a *section* of  $g$  and defined, for all word  $\mathbf{t} \in \Sigma^*$ , by  $g(\mathbf{st}) = g(\mathbf{s})g_{|\mathbf{s}}(\mathbf{t})$ , see [19] for more details. The *portrait* of  $g$  is the tree  $\Sigma^*$  in which each vertex  $\mathbf{s} \in \Sigma^*$  is labeled by  $g_{|\mathbf{s}} : \Sigma \rightarrow \Sigma$ . It is denoted by  $\mathbf{p}_\infty(g)$ . The permutation of  $\Sigma$  associated to the empty word is the *root permutation* of  $g$ . A level (*resp.* branch) of a portrait is the labeled level (*resp.* branch) of the tree.

For a given integer  $k$ , the *k-portrait* of  $g$  is the restriction of  $\mathbf{p}_\infty(g)$  to levels 0 to  $k - 1$  and is denoted by  $\mathbf{p}_k(g)$ , it represents the action of  $g$  on the partial regular rooted tree  $\Sigma^{\leq k}$ .

Let  $\mathbf{u} \in A^*$ . The *portrait* (or  $\infty$ -*portrait* — *resp.* the *k-portrait*) of  $\mathbf{u}$  is the portrait (*resp.* the *k-portrait*) of  $\rho_{\mathbf{u}}$ : each vertex  $\mathbf{s} \in \Sigma^*$  is labeled by  $\rho_{\delta_{\mathbf{s}}(\mathbf{u})} : \Sigma \rightarrow \Sigma$ . It is denoted by  $\mathbf{p}_\infty[\mathbf{u}]$  (*resp.*  $\mathbf{p}_k[\mathbf{u}]$ ). This notation is completely justified by the fact that two equivalent words have the same  $\mathbf{p}_{i|j}$  function. An example is given in Figure 2

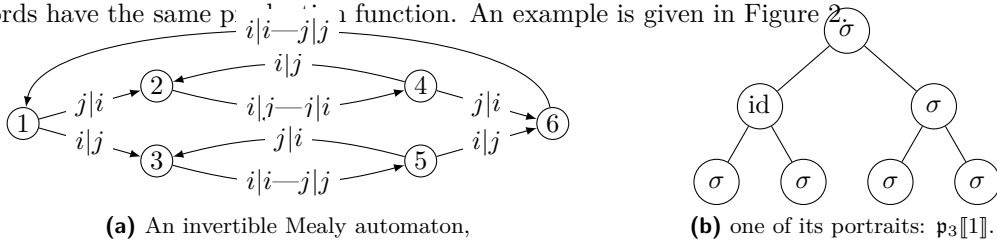


Figure 2 Some portrait of a two-letter Mealy automaton;  $\text{id} = \text{id}_\Sigma$  and  $\sigma$  permutes  $i$  and  $j$ .

The map from  $Aut(\Sigma^*)$  to the set of portraits induces a monoid structure on the set of portraits. The neutral element of the product of portraits is the *identity portrait*:  $\mathcal{I}_\infty = \mathbf{p}_\infty(\text{id}_{\Sigma^*})$ . The *portraits of the automaton*  $\mathcal{A}$  are the portraits of the elements of  $\langle \mathcal{A} \rangle_+$ . The product of two  $k$ -portraits of  $\mathcal{A}$  can be expressed in terms of words:  $\mathbf{p}_k[\mathbf{u}]\mathbf{p}_k[\mathbf{v}] = \mathbf{p}_k[\mathbf{uv}]$ . It provides a monoid structure to the set of  $k$ -portraits of  $\mathcal{A}$ , whose neutral element is the *identity k-portrait*  $\mathcal{I}_k = \mathbf{p}_k(\text{id}_{\Sigma^*})$ .

A level of a portrait is *homogeneous* if all its vertices have the same label; a portrait is *homogeneous* if all its levels are homogeneous: the portrait  $\mathbf{p}_3[1]$  of Figure 2(b) has homogeneous levels 0 and 2, but is not homogeneous. For any integer  $k \geq 1$ , the  $k$ -portrait  $\mathbf{p}_k(g)$  is *almost homogeneous* if  $\mathbf{p}_{k-1}(g)$  and all the  $(\mathbf{p}_{k-1}(g_{|i}))_{i \in \Sigma}$  are homogeneous.

An almost homogeneous  $(k + 1)$ -portrait  $\mathcal{K}$  is built in the following way from a homogeneous  $k$ -portrait  $\mathcal{J}$  and a sequence  $\tau = (\tau_i)_{i \in \Sigma}$  of permutations of  $\Sigma$ : the restriction of  $\mathcal{K}$  to levels 0 to  $k - 1$  is  $\mathcal{J}$  and the leaves of the subtree of the root corresponding to the letter  $i \in \Sigma$  have all label  $\tau_i$ . This portrait is denoted by  $\mathcal{J}[\tau]$ , see Figure 3.

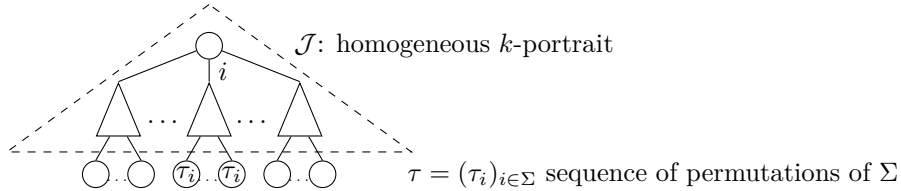


Figure 3 The almost homogeneous  $(k + 1)$ -portrait  $\mathcal{J}[\tau]$ ,  $\tau = (\tau_i)_{i \in \Sigma}$ .

- ▶ **Remark 3.** The product of two homogeneous  $k$ -portraits is a homogeneous  $k$ -portrait. Furthermore, if  $\Sigma = \{i, j\}$ :
  - the square of a homogeneous  $k$ -portrait is the identity  $k$ -portrait  $\mathcal{I}_k$ ;
  - the square of an almost homogeneous  $k$ -portrait whose root permutation is the identity on  $\Sigma$  is the identity  $k$ -portrait;

- *the square of an almost homogeneous  $k$ -portrait  $\mathcal{J}[\tau_i, \tau_j]$  whose root permutation is the permutation of  $i$  and  $j$  is the identity  $k$ -portrait if and only if  $\tau_i = \tau_j$ .*

### 3.4 Tensor closure

When a Mealy automaton generates a finite semigroup, we may augment the alphabet on which it acts to gain a better control over its structure.

Let  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  be a Mealy automaton which generates a finite semigroup. Its *tensor closure* is the Mealy automaton  $\mathfrak{c}(\mathcal{A}) = (A, \Xi, \bar{\delta}, \bar{\rho})$ , where  $\Xi = \{\llbracket \mathbf{s} \rrbracket \mid \mathbf{s} \in \Sigma^*\} = \langle \mathfrak{d}(\mathcal{A}) \rangle_+$  and  $\bar{\delta}$  and  $\bar{\rho}$  are the natural extensions of  $\delta$  and  $\rho$ :

$$\forall x \in A, \forall \mathbf{s} \in \Sigma^*, \bar{\delta}_{\llbracket \mathbf{s} \rrbracket}(x) = \delta_{\mathbf{s}}(x) \text{ and } \bar{\rho}_x(\llbracket \mathbf{s} \rrbracket) = \llbracket \rho_x(\mathbf{s}) \rrbracket.$$

A Mealy automaton is *tensor closed* if it is isomorphic to its tensor closure. Its dual is then minimal.

The following remark justifies the introduction of the tensor closures:

- **Remark 4.** *Let  $\mathcal{A}$  be a two-state Mealy automaton which generates a finite semigroup. Then the automaton  $\mathfrak{c}(\mathcal{A})$  generates a finite semigroup. If  $\mathfrak{c}(\mathcal{A})$  is  $\mathfrak{m}\mathfrak{d}$ -trivial, then so is  $\mathcal{A}$ .*

The first result is obtained by looking at the respective dual automata which generates the same semigroup. The second result is immediate since a two-state Mealy automaton  $\mathcal{A}$  is  $\mathfrak{m}\mathfrak{d}$ -trivial if and only if  $\mathfrak{m}\mathfrak{d}\mathfrak{m}\mathfrak{d}(\mathcal{A})$  is trivial and the alphabet of  $\mathfrak{d}\mathfrak{m}\mathfrak{d}(\mathcal{A})$  can be injected into the alphabet of  $\mathfrak{c}(\mathcal{A})$ .

- **Lemma 5.** *Let  $\mathcal{A} = (A, \Xi, \delta, \rho)$  be a two-state invertible-reversible tensor closed Mealy automaton. The connected components of the powers of  $\mathcal{A}$  are complete graphs.*

**Proof.** Let  $k$  be an integer. The connected components of  $\mathcal{A}^k$  are strongly connected by reversibility. Hence any two words  $\mathbf{u}$  and  $\mathbf{v}$  in the same connected component are connected by a path with input label in  $\Xi^*$ . The automaton  $\mathcal{A}$  being tensor closed, any word over  $\Xi$  is equivalent to a one-length word over  $\Xi$  and so the connected component of  $\mathbf{u}$  and  $\mathbf{v}$  is a complete graph: any two states are connected by a transition. ◀

## 4 The semigroup is either free or finite

Recall that a semigroup  $S$  is *free* if there exists a subset  $X$  of  $S$  such that every element of  $S$  can be written uniquely as a word over  $X$ , its *rank* is then the cardinality of  $X$ .

- **Remark.** On the other hand, a group  $G$  is free if there exists a subset  $X$  of  $G$  such that every element of  $G$  can be written uniquely as an irreducible word over  $X \sqcup X^{-1}$ . An invertible automaton can generate a free semigroup and a non-free group; for example, the dual of Aleshin automaton (see Figure 1(b)) generates a free semigroup, by Theorems 6 and 19, but not a free group:  $ba^{-1}ba^{-1} = 1$ .

- **Theorem 6.** *Let  $\mathcal{A}$  be a reversible two-state Mealy automaton. If  $\mathcal{A}$  admits a disconnected power, then it generates a finite semigroup, otherwise it generates a free semigroup of rank 2 with the states of  $\mathcal{A}$  being free generators.*

Theorem 6 is a corollary of Proposition 10 and the case  $p = 2$  in Proposition 14 below.

Let us look at the connected components of the powers of a Mealy automaton  $\mathcal{A}$ . For  $m > 0$ ,  $\mathbf{u}, \mathbf{v} \in A^m$ , and  $x, y \in A$ , if there exists a path from  $\mathbf{u}x$  to  $\mathbf{v}y$  in  $\mathcal{A}^{m+1}$ , then there is a path from  $\mathbf{u}$  to  $\mathbf{v}$  in  $\mathcal{A}^m$ . Hence if  $\mathcal{A}^n$  is disconnected, so are the  $\mathcal{A}^k$ , for all  $k > n$ . Thus

there exists at most one integer  $n$  such that  $\mathcal{A}^n$  is connected and  $\mathcal{A}^{n+1}$  is disconnected. This integer is called the *connection degree* of  $\mathcal{A}$ . By convention, if  $\mathcal{A}$  is disconnected, its connection degree is 0, and it has an infinite connection degree if no power of  $\mathcal{A}$  is disconnected. For a Mealy automaton, having infinite connection degree coincides with the very classical notion of level transitivity (or spherical transitivity) for its dual [19, 14].

Note that the Baby Aleshin automaton (see Figure 1(c)) is reversible, has a connection degree of 2, three states, and generates an infinite non-free semigroup (its generators have order 2). So Theorem 6 and Proposition 10 do not extend to bigger stateset. However, we conjecture that Proposition 14 extends to any stateset for invertible automata.

## 4.1 Finite connection degree

In this section, we prove that a reversible two-state Mealy automaton has a finite connection degree if and only if it generates a finite semigroup. This result is already known [7, Lemma 3], but we present here a new proof; its main idea is to bound the sizes of the connected components of the powers of  $\mathcal{A}$  once the connection degree has passed.

► **Lemma 7.** *Let  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  be a reversible Mealy automaton with at least two states, which generates a semigroup with torsion elements. Then its connection degree is finite.*

**Proof.** Since  $\langle \mathcal{A} \rangle_+$  has torsion elements, there exist a word  $\mathbf{u} \in A^+$  and two integers  $n \geq 0$  and  $k > 0$  such that  $\mathbf{u}^n$  and  $\mathbf{u}^{n+k}$  are equivalent:  $\rho_{\mathbf{u}^n} = \rho_{\mathbf{u}^{n+k}}$ .

Let  $\mathbf{s} \in \Sigma^*$ , we have:  $\delta_{\mathbf{s}}(\mathbf{u}^{n+2k}) = \delta_{\mathbf{s}}(\mathbf{u}^n)\delta_{\rho_{\mathbf{u}^n}(\mathbf{s})}(\mathbf{u}^k)\delta_{\rho_{\mathbf{u}^{n+k}}(\mathbf{s})}(\mathbf{u}^k) = \delta_{\mathbf{s}}(\mathbf{u}^n)(\delta_{\rho_{\mathbf{u}^n}(\mathbf{s})}(\mathbf{u}^k))^2$ . Hence all the states of the connected component of  $\mathbf{u}^{n+2k}$  have form  $\mathbf{v}\mathbf{w}^2$  and  $\mathcal{A}^{(n+2k)|\mathbf{u}|}$  is disconnected. ◀

**In the reminder of this subsection,  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  denotes a reversible two-state Mealy automaton ( $A = \{x, y\}$ ) with finite connection degree  $n$ .** If  $z \in A$  is a state of  $\mathcal{A}$ ,  $\bar{z} \in A$  denotes the other state:  $z \neq \bar{z}$ .

► **Lemma 8.** *Let  $\mathcal{C}$  be a connected component of  $\mathcal{A}^m$  for some  $m$ , and let  $\mathbf{u} \in A^m$  be a state of  $\mathcal{C}$ . The connected component (in  $\mathcal{A}^{m+1}$ ) of  $\mathbf{u}x$  has size  $\#\mathcal{C}$  if it does not contain  $\mathbf{u}y$ , and  $2\#\mathcal{C}$  if it does contain  $\mathbf{u}y$ .*

**Proof.** Let  $\mathcal{D}$  be the connected component of  $\mathbf{u}x$ :  $\mathbf{v} \in A^m$  is a state of  $\mathcal{C}$  if and only if there exists  $z \in A$  such that  $\mathbf{v}z$  is a state of  $\mathcal{D}$ , hence:  $N \leq \#\mathcal{D} \leq 2N$ . Let  $\mathbf{v}$  be a state of  $\mathcal{C}$  and  $z \in A$ :  $\mathbf{u}x$  and  $\mathbf{v}z$  are in the same connected component if and only if so are  $\mathbf{u}y$  and  $\mathbf{v}\bar{z}$ . The result follows. ◀

Recall that  $n$  is the connection degree of  $\mathcal{A}$ .

► **Lemma 9.** *For each  $m \geq n$ , the connected components of  $\mathcal{A}^m$  have size exactly  $2^n$ .*

**Proof.** By induction on  $m \geq n$ . For  $m \in \{n, n+1\}$ , the property is true (using Lemma 8 for  $m = n+1$ ).

Assume  $m > n+1$ . Suppose that the connected components of  $\mathcal{A}^{m-1}$  and  $\mathcal{A}^m$  have size  $2^n$ . Then let  $\mathcal{C}$  be a connected component of  $\mathcal{A}^{m+1}$  and  $\mathbf{u} = u_1 \cdots u_{m+1}$  a state of  $\mathcal{C}$ . The word  $\mathbf{u}^\bullet = u_1 \cdots u_m$  belongs to a connected component  $\mathcal{D}$  of  $\mathcal{A}^m$ , of size  $2^n$  by the induction hypothesis. Hence  $\mathcal{C}$  has size  $2^n$  or  $2^{n+1}$  according to Lemma 8.

Suppose that  $\mathcal{C}$  has size  $2^{n+1}$ : it means by Lemma 8 that both  $\mathbf{u}$  and  $\mathbf{u}^\bullet \overline{u_{m+1}}$  belong to  $\mathcal{C}$ . It follows that  $u_2 \cdots u_m u_{m+1}$  and  $u_2 \cdots u_m \overline{u_{m+1}}$  belong to the same connected component  $\mathcal{E}$  of  $\mathcal{A}^m$ , of size  $2^n$  by the induction hypothesis. Hence Lemma 8 ensures the existence of a connected component of  $\mathcal{A}^{m-1}$  of size  $2^{n-1}$ , contradicting the induction hypothesis. ◀



► **Proposition 10.** *The connection degree of a reversible two-state Mealy automaton is finite if and only if it generates a finite semigroup.*

**Proof.** Let  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  be a reversible two-state Mealy automaton. If the connection degree of  $\mathcal{A}$  is 0,  $\langle \mathfrak{d}(\mathcal{A}) \rangle_+$  is the trivial semigroup and  $\langle \mathcal{A} \rangle_+$  is finite [2].

Otherwise, let  $n \geq 1$  be the connection degree of  $\mathcal{A}$ : by Lemma 9, for  $m \geq n$ , the connected components of  $\mathcal{A}^m$  have size  $2^n$ . These connected components are reversible Mealy automata on the alphabet  $\Sigma$ . Up to state numbering, there are only a finite number of such automata and thus there exist  $p < q$  such that  $\mathfrak{m}(\mathcal{A}^p) = \mathfrak{m}(\mathcal{A}^q)$ . It follows by Remark 1 that  $\langle \mathcal{A} \rangle_+$  is finite.

The reciprocal property is a particular case of Lemma 7. ◀

## 4.2 Infinite connection degree

Here we prove that if a reversible  $p$ -state Mealy automaton,  $p$  prime, has infinite connection degree, then it generates a free semigroup, the states of the automaton being free generators. The idea is to bound the sizes of the Nerode classes in the powers of  $\mathcal{A}$ .

For the next three lemmas, let  $\mathcal{A} = (A, \Sigma, \delta, \rho)$  be a reversible  $p$ -state Mealy automaton,  $p$  prime, with infinite connection degree ( $A = \{x_1, \dots, x_p\}$ ). By Lemma 7,  $\mathcal{A}$  generates an infinite semigroup.

► **Lemma 11.** *There cannot exist two equivalent words of different length in  $A^*$ .*

**Proof.** For each  $m$ ,  $\mathcal{A}^m$  is connected, and so any two words of length  $m$  are mapped one onto the other by an element of  $\langle \mathfrak{d}(\mathcal{A}) \rangle_+$ .

Let  $\mathbf{u}$  and  $\mathbf{v}$  be two equivalent words of different lengths, say  $|\mathbf{u}| < |\mathbf{v}|$ . Every word of length  $|\mathbf{v}|$  is then equivalent to a word of length  $|\mathbf{u}|$ : if  $\mathbf{w}$  is of length  $|\mathbf{v}|$ , then  $\mathbf{w} = \delta_{\mathbf{t}}(\mathbf{v})$  for some  $\mathbf{t} \in \Sigma^*$ , and, by Remark 2,  $\mathbf{w}$  is equivalent to  $\delta_{\mathbf{t}}(\mathbf{u})$  of length  $|\mathbf{u}|$ . By Remark 1, the semigroup  $\langle \mathcal{A} \rangle_+$  is finite, which is impossible. ◀

► **Lemma 12.** *All the Nerode classes of a given power  $A^m$  have the same size, which happens to be a power of  $p$ .*

**Proof.** Let  $\mathbf{u} \in A^m$ :  $[\mathbf{u}] \subseteq A^m$  by definition. If  $[\mathbf{u}] = A^m$ , the result is clear. Otherwise, let  $\mathbf{v} \in A^m - [\mathbf{u}]$ . Since  $\mathcal{A}^m$  is connected,  $\mathbf{u}$  is mapped onto  $\mathbf{v}$  by an element of  $\langle \mathfrak{d}(\mathcal{A}) \rangle_+$ ; that is there exists  $\mathbf{r} \in \Sigma^*$  such that  $\mathbf{v} = \delta_{\mathbf{r}}(\mathbf{u})$ .

By Remark 2, any word equivalent to  $\mathbf{u}$  is mapped by  $\delta_{\mathbf{r}}$  onto a word equivalent to  $\mathbf{v}$ . Since the automaton  $\mathcal{A}^m$  is reversible,  $\delta_{\mathbf{r}}$  is a permutation of  $A^m$ , hence we find  $\#[\mathbf{u}] = \#[\mathbf{v}]$ .

The stateset of  $\mathcal{A}^m$  has size a power of  $p$ , where  $p$  is a prime number, and so has any Nerode equivalence class. ◀

► **Lemma 13.** *There cannot exist two equivalent words of the same length in  $A^*$ .*

**Proof.** Let  $\mathbf{u}$  and  $\mathbf{v}$  be two different equivalent words of the same length  $n + 1$ . Let us prove by induction on  $m > n$  that  $\mathfrak{m}(\mathcal{A}^m)$  has at most  $p^n$  states.

The automaton  $\mathcal{A}^{n+1}$  has  $p^{n+1}$  states. The words  $\mathbf{u}$  and  $\mathbf{v}$  are in the same Nerode class: by Lemma 12, all Nerode classes of  $A^{n+1}$  have at least  $p$  elements and  $\mathfrak{m}(\mathcal{A}^{n+1})$  has at most  $p^n$  states.

Suppose that  $\mathfrak{m}(\mathcal{A}^m)$  has at most  $p^n$  states. Then, since all Nerode classes have the same size by Lemma 12, the induction hypothesis implies that they have at least  $p^{m-n}$  elements. Let us look at  $[x_1^m]$ : it contains

$$x_1^m, \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{p^{m-n}-1},$$

which are pairwise distinct. Among these words, there is at least one whose suffix in  $x_1$  is the shortest, say  $\mathbf{u}_1$  without loss of generality:  $p^{m-n} > 1$  and  $x_1^m$  has the longest possible suffix in  $x_1$ . Hence  $[x_1^{m+1}]$  contains the following pairwise distinct  $p^{m-n} + 1$  words

$$x_1^{m+1}, \mathbf{u}_1 x_1, \mathbf{u}_2 x_1, \dots, \mathbf{u}_{p^{m-n}-1} x_1, x_1 \mathbf{u}_1.$$

By Lemma 12,  $\#[x_1^{m+1}]$  is a power of  $p$ , so  $\#[x_1^{m+1}] \geq p^{m+1-n}$ . As all Nerode classes of  $A^{m+1}$  have the same cardinality, we can conclude that  $\mathfrak{m}(A^{m+1})$  has at most  $p^{m+1}/p^{m+1-n} = p^n$  elements, ending the induction.

Consequently, since there is only a finite number of different Mealy automata with up to  $p^n$  states, there exist  $k < \ell$  such that  $\mathfrak{m}(A^k)$  and  $\mathfrak{m}(A^\ell)$  are equal up to state numbering. By Remark 1, the semigroup  $\langle A \rangle_+$  is finite, which is impossible. ◀

As a corollary of Lemmas 7, 11 and 13 we can state the following proposition.

► **Proposition 14.** *Let  $A$  be a reversible  $p$ -state Mealy automaton,  $p$  prime. If the automaton  $A$  has infinite connection degree, then it generates a free semigroup of rank  $p$  with the states of  $A$  being free generators of the semigroup. The converse holds for  $p = 2$ .*

## 5 Decidability of finiteness and of freeness

This section is devoted to the decidability of finiteness and of freeness for semigroups generated by two-state invertible-reversible Mealy automata by linking Theorem 6 and the possible  $\mathfrak{m}\mathfrak{d}$ -triviality of such an automaton.

► **Lemma 15.** *Let  $A = (A, \Sigma, \delta, \rho)$  be a two-state invertible-reversible automaton of finite connection degree  $n$ . Two elements of  $\Sigma^*$  which have the same action on a word of  $A^n$  are equivalent.*

**Proof.** It is sufficient to prove that  $\text{id}_{A^*}$  is the only element of  $\langle \mathfrak{d}(A) \rangle_+$  which fixes a word of  $A^n$ .

If  $n = 0$ ,  $\langle \mathfrak{d}(A) \rangle_+$  is the trivial semigroup and the result is true. Otherwise, let  $\mathbf{u} \in A^n$  and  $\mathbf{s} \in \Sigma^*$  such that  $\mathbf{u}$  is stable by  $\delta_{\mathbf{s}}$ :  $\delta_{\mathbf{s}}(\mathbf{u}) = \mathbf{u}$ .

By Lemma 8,  $A^{n+1}$  has two connected components:  $\mathbf{u}x$  belongs to one of them and  $\mathbf{u}y$  to the other one. Looking forward, a connected component  $\mathcal{C}$  of  $A^m$ , for  $m \geq n$ , originates two connected components of  $A^{m+1}$ :  $\{\mathbf{v}z_{\mathbf{v}} \mid \mathbf{v} \in \mathcal{C}, z_{\mathbf{v}} \in A\}$  and  $\{\mathbf{v}\bar{z}_{\mathbf{v}} \mid \mathbf{v} \in \mathcal{C}\}$ . And all connected component of  $A^{m+1}$  are built this way. Hence if two different words of the same length  $m > n$  have the same prefix of length  $n$ , they belong to different connected components of  $A^m$ .

Let  $\mathbf{t} \in \Sigma^*$  satisfy  $\rho_{\mathbf{u}}(\mathbf{s}) = \mathbf{t}$ , and let  $\mathbf{v}, \mathbf{w} \in A^*$  such that  $\mathbf{t}$  maps  $\mathbf{v}$  onto  $\mathbf{w}$ :  $\delta_{\mathbf{t}}(\mathbf{v}) = \mathbf{w}$ .

The words  $\mathbf{u}\mathbf{v}$  and  $\mathbf{u}\mathbf{w}$  belong to the same connected component:

$$\delta_{\mathbf{s}}(\mathbf{u}\mathbf{v}) = \delta_{\mathbf{s}}(\mathbf{u})\delta_{\rho_{\mathbf{u}}(\mathbf{s})}(\mathbf{v}) = \mathbf{u}\delta_{\mathbf{t}}(\mathbf{v}) = \mathbf{u}\mathbf{w},$$

and have a common prefix of length  $n$ , so they are equal. Hence:  $\delta_{\mathbf{t}} = \text{id}_{A^*}$ . As  $\mathfrak{d}(A)$  is reversible,  $\mathbf{t}$  is mapped onto  $\mathbf{s}$  by an element of  $\langle A \rangle_+$  and  $\delta_{\mathbf{s}} = \text{id}_{A^*}$ . ◀

We have a similar (but weaker) result on shorter words for tensor closed Mealy automata. **In the next three lemmas of this section,  $A = (A, \Xi, \delta, \rho)$  denotes a tensor closed two-state invertible-reversible automaton of finite connection degree  $n$ :  $A = \{x, y\}$ .** By Lemma 5,  $A^n$  is complete as a graph. Furthermore, a transition has a unique label: if a transition had several labels, they would coincide on a word of  $A^n$  and by Lemma 15 they actually would be the same letter of  $\Xi$ .

► **Lemma 16.** *Let  $k$  be an integer,  $1 \leq k \leq n$ . Two elements of  $\Xi^*$  which map a given word of  $A^k$  into the same word have the same action on  $A^k$ .*

**Proof.** Each word of  $\Xi^*$  is equivalent to a letter of  $\Xi$ , hence it is sufficient to prove the result for letters.

The Mealy automaton  $\mathcal{A}^n$  has  $2^n$  states, is complete as a graph and each transition has a unique label, so  $\#\Xi = 2^n$ . By hypothesis,  $\Xi$  is the set of elements of  $\langle \mathfrak{d}(\mathcal{A}) \rangle_+$ , so  $\#\langle \mathfrak{d}(\mathcal{A}) \rangle_+ = 2^n$ .

Let us consider the minimization of  $\mathfrak{d}(\mathcal{A})$ , using the sequence of increasingly finer equivalences  $(\equiv_k)$  introduced in Section 3.1. Each  $n$ -class of  $\Xi$  is a singleton by Lemma 15, hence the sequence  $(\equiv_k)$  remains constant at least from  $n$  on. So the Nerode equivalence produces  $2^n$  equivalence classes formed uniquely by singletons, by partitioning the stateset of  $\mathfrak{d}(\mathcal{A})$  of cardinality  $2^n$  in  $n$  steps, each step cutting each class of the previous one into at most two subsets as  $\#A = 2$ . Hence the equivalence  $\equiv_k$  cuts each  $(k-1)$ -class into two sets of the same cardinality:  $\forall k, 0 \leq k \leq n, \forall s \in \Xi, \#[s]_k = \#[s]_{k-1}/2 = 2^{n-k}$ .

Let  $k, 1 \leq k \leq n, \mathbf{u} \in A^k$ , and  $s \in \Xi$ . We have:

$$[s]_k \subseteq \{t \in \Xi \mid t(\mathbf{u}) = s(\mathbf{u})\}. \quad (1)$$

The left set in Equation (1) has cardinality  $2^{n-k}$ , it is the set of elements of  $\Xi$  which coincide with  $s$  on  $A^k$ . Since two elements of  $\Xi$  whose actions coincide on a word of  $A^n$  are equivalent, the right set of Equation (1) has cardinality at most  $\#A^{n-k} = 2^{n-k}$ , and so the two sets of Equation (1) are equal, leading to the result. ◀

One consequence of Lemma 16 is that an element of  $\Xi^*$  which fixes a word of length  $k$  on  $A$  fixes completely  $A^k$ .

Denote by  $\text{id}$  the identity of  $A$  and by  $\sigma$  the permutation of  $x$  and  $y$ . We can translate Lemma 16 in terms of portraits of  $\mathfrak{d}(\mathcal{A})$ : whenever two  $k$ -portraits of  $\mathfrak{d}(\mathcal{A})$  have an identical branch, they are equal. In particular,  $\mathcal{I}_k$  being a portrait of  $\mathfrak{d}(\mathcal{A})$ , if a whole branch of a  $k$ -portrait of  $\mathfrak{d}(\mathcal{A})$  is labeled by  $\text{id}$ , this portrait is  $\mathcal{I}_k$ . Hence if in a  $k$ -portrait of  $\mathfrak{d}(\mathcal{A})$ , all vertices at level less than  $k-1$  are labeled by  $\text{id}$ , this portrait is either  $\mathcal{I}_k$  or  $\mathcal{I}_{k-1}[\sigma, \sigma]$ . Note that for  $k \leq n$ , both  $\mathcal{I}_k$  and  $\mathcal{I}_{k-1}[\sigma, \sigma]$  are portraits of  $\mathfrak{d}(\mathcal{A})$ .

By Lemma 15, any element of  $\langle \mathfrak{d}(\mathcal{A}) \rangle_+$  whose  $n$ -portrait is  $\mathcal{I}_n$  acts trivially on  $A^*$ .

What are the possible portraits of  $\mathfrak{d}(\mathcal{A})$ ? Since  $\mathcal{A}^n$  is connected and  $\mathcal{A}$  is tensor closed, it is immediate that each finite sequence  $(\pi_i)_{1 \leq i \leq n} \in \{\text{id}, \sigma\}^n$  labels a branch of an  $n$ -portrait of  $\mathfrak{d}(\mathcal{A})$ : in  $\mathcal{A}^n$ , there is a transition with input  $s \in \Xi$  from  $x^n$  to  $\pi_1(x) \cdots \pi_n(x)$  and the leftmost branch of  $\mathfrak{p}_n \llbracket s \rrbracket$  is labeled by  $\pi$ .

► **Lemma 17.** *The portraits of  $\mathfrak{d}(\mathcal{A})$  are homogeneous.*

**Proof.** Let us prove the result for  $k \leq n$ , by induction on  $k \geq 1$ . A 1-portrait has a unique element, its root, and so is homogeneous.

Suppose that the  $\ell$ -portraits of  $\mathfrak{d}(\mathcal{A})$  are all homogeneous, for  $\ell \leq k < n$ . Let us consider a letter  $s \in \Xi$  and  $\mathcal{S} = \mathfrak{p}_{k+1} \llbracket s \rrbracket$ : it is almost homogeneous by the induction hypothesis. More precisely:  $\mathcal{S} = \mathfrak{p}_k \llbracket s \rrbracket [\tau_1, \tau_2]$  for  $\tau_1, \tau_2$ , some permutations of  $A$ .

**First case:  $\delta_s$  permutes  $x$  and  $y$ .** We consider the following  $(n+1)$ -portrait  $\mathcal{K}$ :

- the restriction of  $\mathcal{K}$  to levels 0 to  $(n-k-1)$  is  $\mathcal{I}_{n-k}$ ,
- in bottom-left of  $\mathcal{I}_{n-k}$ , we put  $\mathfrak{p}_{k+1} \llbracket s \rrbracket$ : the root of  $\mathfrak{p}_{k+1} \llbracket s \rrbracket$  is the left child of the bottom-left leaf of  $\mathcal{I}_{n-k}$  (it is possible since we can choose the left branch of a portrait, applying Lemma 16 and  $\mathfrak{p}_{k+1} \llbracket s \rrbracket$  is actually a portrait of  $\mathfrak{d}(\mathcal{A})$ ),

■ it is completed to be a portrait of  $\mathfrak{d}(\mathcal{A})$ .

The leftmost branch of  $\mathcal{K}^2$  starts with  $\text{id}^n$ . Hence by Lemma 15,  $\mathcal{K}^2$  is the identity  $(n+1)$ -portrait, which implies  $\tau_1 = \tau_2$  by Remark 3 and Lemma 15, that is  $\mathcal{S}$  is homogeneous.

**Second case:  $\delta_s$  stabilizes  $A$ .** Let  $\mathcal{L}$  be the  $(k+1)$ -portrait whose root permutation is  $\sigma$  and all other vertices are labeled by  $\text{id}$ : it is a portrait of  $\mathfrak{d}(\mathcal{A})$  since so are all homogeneous  $(k+1)$ -portraits with root permutation  $\sigma$  from first case. Then by multiplying  $\mathcal{S}$  by  $\mathcal{L}$ , we obtain a non-homogeneous  $(k+1)$ -portrait with root permutation  $\sigma$  which has to be a portrait of  $\mathfrak{d}(\mathcal{A})$ . That is impossible.

The proof is similar for  $k > n$ , considering the portrait  $\mathfrak{p}_k[[s]]$ . ◀

► **Lemma 18.** *The states of  $\mathcal{A}$  are equivalent.*

**Proof.** By Lemma 17, all the portraits of  $\mathfrak{d}(\mathcal{A})$  are homogeneous. For any letter  $s \in \Xi$ , since its portrait is homogeneous,  $\rho_x(s)$  and  $\rho_y(s)$  are equivalent. The automaton being tensor closed, they are equal, and so  $\rho_x = \rho_y$ . ◀

► **Theorem 19.** *Let  $\mathcal{A}$  be a two-state invertible-reversible Mealy automaton. It generates a finite group if and only if it is  $\mathfrak{m}\mathfrak{d}$ -trivial.*

**Proof.** By [2], if  $\mathcal{A}$  is  $\mathfrak{m}\mathfrak{d}$ -trivial, it generates a finite group.

Suppose that  $\mathcal{A}$  generates a finite group and consider its tensor closure  $\mathfrak{c}(\mathcal{A})$ :  $\mathfrak{c}(\mathcal{A})$  generates a finite group by Remark 4. The connection degree of  $\mathfrak{c}(\mathcal{A})$  is finite by Proposition 10 and so  $\mathfrak{c}(\mathcal{A})$  is  $\mathfrak{m}\mathfrak{d}$ -trivial by Lemma 18. Hence  $\mathcal{A}$  is  $\mathfrak{m}\mathfrak{d}$ -trivial by Remark 4. ◀

The last theorem summarizes all the decidability results arising from this article.

► **Theorem 20.** *It is decidable whether a two-state invertible-reversible Mealy automaton with alphabet  $\Sigma$  generates a finite group, in time  $\mathcal{O}(\Sigma \log \Sigma)$ . It is decidable whether it generates a free semigroup, in time  $\mathcal{O}(\Sigma \log \Sigma)$ .*

*It is decidable whether a two-letter invertible-reversible Mealy automaton with stateset  $A$  generates a finite group, in time  $\mathcal{O}(A \log A)$ .*

Up to now, the only methods to conclude infiniteness of automaton groups were to prove the existence of an element of infinite order [18, FindElementOfInfiniteOrder][5, SIZE\_FR], using Sidki's fundamental work [8, 21], or to test level transitivity [5, IsLevelTransitive]. All these methods give sufficient but not necessary conditions.

To illustrate the actual efficiency of the  $\mathfrak{m}\mathfrak{d}$ -triviality as an algorithm to test finiteness, let us consider the 2-letter 6-state invertible-reversible Mealy automata. Bireversible Mealy automata are particular invertible-reversible Mealy automata and an invertible-reversible automaton generates a finite group only if it is bireversible [2]. Testing the  $\mathfrak{m}\mathfrak{d}$ -triviality of the 3446 bireversible 2-letter 6-states Mealy automata takes 751ms<sup>1</sup>, while applying FindElementOfInfiniteOrder, SIZE\_FR or IsLevelTransitive to determine the infinity of the group generated by the particular bireversible 2-letter 6-state Mealy automaton of Figure 2(a) is unsuccessful after three weeks of computation.

**Acknowledgments** I would like to thank Jean Mairesse and Matthieu Picantin for numerous discussions around this topic.

---

<sup>1</sup> Timings obtained on an Intel Xeon computer with clock speed 2.13GHz; programs written in GAP [10].

## References

- 1 A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, 1974.
- 2 A. Akhavi, I. Klimann, S. Lombardy, J. Mairesse, and M. Picantin. On the finiteness problem for automaton (semi)groups. *Int. J. Algebra Comput.*, 22(6):26p., 2012.
- 3 S.V. Alešin. Finite automata and the Burnside problem for periodic groups. *Mat. Zametki*, 11:319–328, 1972.
- 4 A.S. Antonenko. On transition functions of Mealy automata of finite growth. *Matematychni Studii.*, 29(1):3–17, 2008.
- 5 L. Bartholdi. FR *Functionally recursive groups – a GAP package, v.1.2.4.2*, 2011.
- 6 L. Bartholdi, I.I. Reznikov, and V.I. Sushchanskiĭ. The smallest Mealy automaton of intermediate growth. *J. Algebra*, 295(2):387–414, 2006.
- 7 I. Bondarenko, R.I. Grigorchuk, R. Kravchenko, Y. Muntyan, V. Nekrashevych, D. Savchuk, and Z. Šunić. On classification of groups generated by 3-state automata over a 2-letter alphabet. *Algebra Discrete Math.*, 1:1–163, 2008.
- 8 I.V. Bondarenko, N.V. Bondarenko, S.N. Sidki, and F.R. Zapata. On the conjugacy problem for finite-state automorphisms of regular rooted trees. *Groups, Geometry, and Dynamics*, in press. arXiv:math.GR/1011.2227.
- 9 A.J. Cain. Automaton semigroups. *Theor. Comput. Sci.*, 410:5022–5038, 2009.
- 10 The GAP Group. *GAP – Groups, Algorithms, and Programming, v.4.4.12*, 2008.
- 11 Y. Glasner and Sh. Mozes. Automata and square complexes. *Geom. Dedicata*, 111(1):43–6, 2005.
- 12 R. Grigorchuk and A. Żuk. The lamplighter group as a group generated by a 2-state automaton, and its spectrum. *Geom. Dedicata*, 87:209–244, 2001.
- 13 R.I. Grigorchuk. On Burnside’s problem on periodic groups. *Funktsional. Anal. i Prilozhen.*, 14(1):53–54, 1980.
- 14 R.I. Grigorchuk, V.V. Nekrashevich, and V.I. Sushchanskiĭ. Automata, dynamical systems, and groups. *Tr. Mat. Inst. Steklova*, 231:134–214, 2000.
- 15 I. Klimann, J. Mairesse, and M. Picantin. Implementing computations in automaton (semi)groups. In *Proc. 17th CIAA*, volume 7381 of *LNCS*, pages 240–252, 2012. DOI No: 10.1142/S021819671250052X.
- 16 V. Maltcev. Cayley automaton semigroups. *Int. J. Algebra Comput.*, 19(1):79–95, 2009.
- 17 A. Mintz. On the Cayley semigroup of a finite aperiodic semigroup. *Int. J. Algebra Comput.*, 19(6):723–746, 2009.
- 18 Y. Muntyan and D. Savchuk. *automgrp Automata Groups – a GAP package, v.1.1.4.1*, 2008.
- 19 V. Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.
- 20 D.M. Savchuk and Y. Vorobets. Automata generating free products of groups of order 2. *J. Algebra*, 336(1):53–66, 2011.
- 21 S.N. Sidki. Automorphisms of one-rooted trees: growth, circuit structure, and acyclicity. *J. Math. Sci. (New York)*, 100(1):1925–1943, 2000. *Algebra*, 12.
- 22 P.V. Silva and B. Steinberg. On a class of automata groups generalizing lamplighter groups. *Int. J. Algebra Comput.*, 15(5-6):1213–1234, 2005.
- 23 B. Steinberg, M. Vorobets, and Y. Vorobets. Automata over a binary alphabet generating free groups of even rank. *Int. J. Algebra Comput.*, 21(1-2):329–354, 2011.
- 24 M. Vorobets and Y. Vorobets. On a free group of transformations defined by an automaton. *Geom. Dedicata*, 124:237–249, 2007.
- 25 M. Vorobets and Y. Vorobets. On a series of finite automata defining free transformation groups. *Groups Geometry and Dynamics*, 4:377–405, 2010.