

# Groups and Semigroups Defined by Colorings of Synchronizing Automata

Daniele D'Angeli

Institut für Mathematische Strukturtheorie (Math C)

Technische Universität Graz

Steyrergasse 30, 8010 Graz, Austria.

`dangeli@math.tugraz.at`

Emanuele Rodaro

Department of Mathematics, University of Porto

Rua do Campo Alegre, 687, Porto, 4169-007, Portugal.

`emanuele.rodaro@fc.up.pt`

September 8, 2018

## Abstract

In this paper we combine the algebraic properties of Mealy machines generating self-similar groups and the combinatorial properties of the corresponding deterministic finite automata (DFA). In particular, we relate bounded automata to finitely generated synchronizing automata and characterize finite automata groups in terms of nilpotency of the corresponding DFA. Moreover, we present a decidable sufficient condition to have free semigroups in an automaton group. A series of examples and applications is widely discussed, in particular we show a way to color the De Bruijn automata into Mealy automata whose associated semigroups are free, and we present some structural results related to the associated groups.

## 1 Introduction

This paper deals with different aspects concerning automata, semigroups and groups. In this context, groups generated by finite automata, naturally appear. Given a deterministic finite automaton (DFA) on the alphabet  $A$ , one can introduce an output function (or coloring) on each arrow in

such a way that the states of the automaton are identified with the generators of a subgroup of the permutation groups over  $A^*$ , these automata are particular kind of simple Mealy machines, also known as Mealy automata, with the same input and output alphabets [13, 27]. In this way automata groups belong to the class of self-similar groups, which act by automorphisms (isometries) on a rooted regular tree. Such class of groups contains remarkable examples of groups with intermediate growth, amenable groups, infinite finitely generated torsion groups, groups with exponential but non-uniform exponential growth and it has been proved to have deep connections with the theory of profinite groups, combinatorics and with complex dynamics. In particular, groups of this type satisfy a property of self-similarity which reflects on the fractalness of some limit objects associated with them via the notion of limit space and Schreier graphs [5, 7, 10, 14, 19]. In this context the class of groups generated by bounded automata, i.e. automata with a finite number of infinite paths avoiding the sink is of special interest and presents important properties [4, 8, 28]. In this spirit, here, we relate the structure of a bounded automaton regarded as a DFA to the combinatorial properties of the sets of its synchronizing words, connecting the algebraic and the combinatorial aspects of automata theory. The study of groups and semigroups generated by automata usually starts with a specific simple Mealy machine, here instead we address the problem of studying the groups (semigroups) that can arise from the possible “colorings” of a deterministic finite automaton into simple Mealy machines, and how combinatorial properties on the underlying DFA can reflect into structural properties of the corresponding groups (semigroups) generated. This paper focuses on a particular class of DFAs called synchronizing, i.e. the automata for which there is a word  $w$ , called reset word, and a state  $q$  such that  $w$  applied to an arbitrary state  $p$  leads to  $q$ . This class has received a great deal of attention in the last fifty years both in computer science being a suitable model of error resistant systems, and in mathematics mainly motivated by the Černý conjecture, i.e. every synchronizing DFA with  $n$  states has a reset word of length at most  $(n - 1)^2$ . By now this simply looking conjecture is arguably the most longstanding open problem in the combinatorial theory of finite automata. Other mathematical motivations for the study of this kind of automata come from semigroup theory [1, 2], theory of codes [6], multiple-valued logic and symbolic dynamics [18]. The latter connection is especially interesting in view of the Road Coloring Problem which has recently been solved positively [31]. For a general introduction on synchronizing automata and the Černý conjecture we refer to Volkov’s survey [32].

The paper is organized as follows. In Section 2 we give some basic notions

useful later in the paper. In Section 3 we extend the main result of [29] considering the natural class of reset Mealy automata and proving that for automata in this class with distinct modified state functions the associated semigroups are free. In Section 4 we study group colorings, in particular we present a gap theorem for reset group colorings of synchronizing DFAs which are simple, we also frame the class of bounded synchronizing automata in the more general class of finitely generated synchronizing automata, and we finally characterize the synchronizing DFAs with a sink state for which all the group colorings generate finite groups. In Section 5 we give some sufficient conditions on some particular synchronizing automata to have a weakly reset group colorings for which the associated semigroups are free. Furthermore, we show group colorings on the De Bruijn automata for which the associated semigroups are also free.

## 2 Preliminaries

In the sequel  $A$  denotes a finite set, called *alphabet*,  $A^*$  ( $A^+$ ) is the free monoid (semigroup) on  $A$ . By  $A^{\leq n}$  ( $A^{\geq n}$ ,  $A^n$ ) we denote the set of words of length less or equal (greater or equal, equal) to  $n$ .  $A^\omega$  is the set of right infinite words in  $A$ . In our context a directed graph (for short *digraph*) is a graph in the sense of Serre. Thus, it is a tuple  $(V, E, \iota, \tau)$ , where  $V$  is the set of vertices,  $E$  is the set of edges, and  $\iota, \tau$  are functions from  $E$  into  $V$  giving the initial and terminal vertices, respectively. Therefore, we can depict an edge  $e \in E$  as  $q \rightarrow q'$  where  $q = \iota(e)$ ,  $q' = \tau(e)$ . We allow multiple edges and for  $q \in V$ , we denote by  $\partial^+(q)$  the set of outgoing edges, i.e. the collection of  $e \in E$  with  $\iota(e) = q$ . In this paper we are interested in the particular class of *out-regular* digraphs (for short *or-digraph*). These are digraphs such that every vertex  $q$  has the same number  $k$  of edges leaving it, or equivalently there is an integer  $k \geq 1$  with  $|\partial^+(q)| = k$ , the integer  $k$  is called the *out-degree*. The interest in *or-digraphs* derives from the connection with deterministic finite automata since their underlying digraphs are out-regular. A *deterministic finite automaton* (for short DFA) is a 3-tuple  $\mathcal{A} = (Q, A, \delta)$  where  $Q$  is a finite set of states,  $A$  is a finite alphabet,  $\delta : Q \times A \rightarrow Q$  is the *transition function*. Note that traditionally, in literature, these objects are often referred as semiautomata [17] since they are not seen as languages recognizers. However, we still call a DFA a tuple  $\mathcal{A} = (Q, A, \delta, q_0, F)$ , where  $q_0 \in Q$  is the initial state,  $F \subseteq Q$  is the set of final states and the *language recognized* by  $\mathcal{A}$  is given by

$$L[\mathcal{A}] = \{u \in A^* : \delta(q_0, u) \in F\}$$

When the transition function is clear from the context we use the simple notation  $q \cdot a$  to denote  $\delta(q, a)$ . This action of the alphabet  $A$  on the states can be naturally extended to an action of  $A^*$  on  $Q$  and this action can be further extended to subsets  $Q$  by putting  $H \cdot u = \{q \cdot u : q \in H\}$  for any  $H \subseteq Q$ ,  $u \in A^*$ . The underlying digraph of  $\mathcal{A}$  is defined as  $D(\mathcal{A}) = (Q, E, \iota, \tau)$  where

$$E = \{e = q \longrightarrow q' : \exists a \in A, \delta(q, a) = q'\}$$

Notice that  $D(\mathcal{A})$  is an *or*-digraph. Conversely, given an *or*-digraph  $G = (V, E, \iota, \tau)$  it is possible to define DFAs via certain “edge colorings”. Indeed, if  $G$  has out-degree  $k$ , a *DFA-coloring* is a map  $\chi : E \rightarrow A$ , where  $|A| = k$ , such that  $\chi : \partial^+(v) \rightarrow A$  is a bijection for any  $v \in V$ . It is evident that  $\chi$  gives rise to the DFA  $\mathcal{A}(G, \chi) = (V, A, \delta)$ , where  $\delta(v, a) = v'$  such that  $e = v \longrightarrow v'$  and  $\chi(e) = a$ .

In this paper we deal mostly with *synchronizing automata*. A synchronizing DFA  $\mathcal{A} = (Q, A, \delta)$  has the property that there is a word  $u \in A^*$ , called *synchronizing* (or *reset*) *word* such that  $q \cdot u = q' \cdot u$  for any  $q, q' \in Q$ , or equivalently  $|Q \cdot u| = 1$ . We use  $\text{Syn}(\mathcal{A})$  to denote the set of all the reset words of  $\mathcal{A}$ . The set  $\text{Syn}(\mathcal{A})$  has a natural structure of two-sided ideal (for short ideal) of the free monoid  $A^*$ , i.e.  $A^* \text{Syn}(\mathcal{A}) A^* \subseteq \text{Syn}(\mathcal{A})$ . In general an ideal  $I$  is said to be *finitely generated* whenever there is a finite set  $U$  such that  $A^* U A^* = I$  or equivalently the bifix code generated by  $I$  is finite [22]. We say that  $\mathcal{A}$  has a *sink* state whenever there is a state  $s \in Q$  such that  $s \cdot a = s$  for all  $a \in A$ . It is an easy exercise to check that every synchronizing automaton has at most one sink state. Note that a DFA  $\mathcal{A} = (Q, A, \delta)$  with a unique sink  $s$ , such that any state  $q \in Q$  is co-accessible from  $s$ , i.e. there is a word  $u \in A^*$  with  $q \cdot u = s$ , is actually synchronizing. An *automata congruence* (for short congruence) on  $\mathcal{A} = (Q, A, \delta)$  is an equivalence relation  $\rho \subseteq Q \times Q$  which is compatible with the action  $\delta$ , i.e.  $q \rho p \Rightarrow (q \cdot a) \rho (p \cdot a)$  for all  $a \in A$ .

A *finite state Mealy automaton* is a 4-tuple  $\mathcal{M} = (Q, A, \delta, \lambda)$  where  $Q$  is a finite set of states,  $A$  is a finite alphabet,  $\delta : Q \times A \rightarrow Q$  is the transition function, while  $\lambda : Q \times A \rightarrow A$  is called the *output function*. The tuple  $(Q, A, \delta)$  is called the *associated DFA* of  $\mathcal{M}$ . In case both the transition function and the output function are clear from the context we also use the shorter notation

$$\delta(q, a) = q \cdot a, \quad \lambda(q, a) = q \circ a$$

for any  $q \in Q$ ,  $a \in A$ . These maps also extend naturally on  $A^*$  by  $q \cdot (ua) = (q \cdot u) \cdot a$ , and  $(q \circ ua) = (q \circ u)((q \cdot u) \circ a)$  with  $q \in Q$ ,  $u \in A^*$ ,  $a \in A$ . For  $q \in Q$ , the function  $\lambda_q : A \rightarrow A$  defined by  $\lambda_q(a) = \lambda(q, a)$  for  $a \in A$  is called

the *state function*. One can depict a Mealy automata as an *or*-digraph with edges labelled as  $q \xrightarrow{a|b} q'$  whenever  $q \cdot a = q'$  and  $q \circ a = b$ . We call a Mealy automaton  $\mathcal{A}$  is called *invertible* if for any  $q \in Q$ ,  $\lambda_q$  is a permutation on  $A$ , and it is called *synchronizing* whenever the associated DFA is synchronizing, in this case we denote  $\text{Syn}(\mathcal{A})$  the set of reset words of the associated DFA. Given any state  $q \in Q$ , with a slight abuse of notation we consider the (sequential) functions  $\mathcal{A}_q : A^* \rightarrow A^*$  and  $\mathcal{A}_q : A^\omega \rightarrow A^\omega$  defined by:

$$\mathcal{A}_q(1) = 1, \quad \mathcal{A}_q(a_0 \dots a_n) = \lambda_q(a_0) \mathcal{A}_{q \cdot a_0}(a_1 \dots a_n)$$

$$\mathcal{A}_q(a_0 a_1 \dots) = \lim_{n \rightarrow \infty} \mathcal{A}_q(a_0 \dots a_n)$$

This action extends to subsets of  $A^*, A^\omega$  in the obvious way. Note that if  $\mathcal{A}$  is invertible, then  $\mathcal{A}_q$  is also invertible and the inverse is denote by  $\mathcal{A}_q^{-1}$ . The action of  $\mathcal{A}_q^{-1}$  on  $A^*, A^\omega$  is uniquely determined. The automaton  $\mathcal{A}$  is called *reduced* if the functions  $\mathcal{A}_q$ ,  $q \in Q$ , are distinct. The semigroup of automatic transformations generated by the automaton  $\mathcal{A}$ , which we refer to as *automata semigroup* of  $\mathcal{A}$ , is the semigroup  $\mathcal{S}(\mathcal{A})$  generated by  $\{\mathcal{A}_q : q \in Q\}$ . If  $\mathcal{A}$  is invertible, then the group  $\mathcal{G}(\mathcal{A})$  generated by  $\{\mathcal{A}_q : q \in Q\}$  is called the *automata group* of  $\mathcal{A}$ . Recall that, in this case, we denote by  $\mathcal{A}_q^{-1}$  the inverse of the generator  $\mathcal{A}_q$ .

The following lemma is a straightforward consequence of the previous definitions.

**Lemma 1.** *Let  $\mathcal{A} = (Q, A, \delta, \lambda)$ , then, for any  $q \in Q$  and  $u \in A^*$ ,  $\mathcal{A}_q(u) = (q \circ u) \mathcal{A}_{q \cdot u}$ .*

The group  $\mathcal{G}(\mathcal{A})$  naturally acts on the space of finite and infinite words  $A^* \sqcup A^\omega$  in the alphabet  $A$ . The set  $A^* \sqcup A^\omega$  can be identified with a rooted regular tree  $T_{|A|}$ , i.e. a simple graph which is a tree and the root  $r$  is the only vertex of degree  $|A|$ , instead the other vertices have degree  $|A| + 1$ . Denote by  $\emptyset$  the empty word of the set  $A^*$  and  $\sim$  the adjacency relation in  $T_{|A|}$ . A labeling  $\Lambda$  of the vertices of such tree is a bijective map

$$\Lambda : A^* \longrightarrow V(T_{|A|})$$

such that  $\Lambda(\emptyset) = r$  and  $\Lambda(v) \sim \Lambda(w)$  if and only if either  $v = wa$  or  $w = va$ , for  $a \in A$ . The  $n$ -th level of  $T_{|A|}$  is identified with the set  $A^n$ . The group  $\mathcal{G}(\mathcal{A})$  acts on  $A^n$ , for every  $n$  and fixes the root. It is easy to prove that, if  $d$  is the discrete distance in the graph  $T_{|A|}$ , then  $d(v, w) = d(gv, gw)$ . Hence  $\mathcal{G}(\mathcal{A})$  is a subgroup of the full automorphism (isometry) group  $\text{Aut}(T_{|A|})$  of  $T_{|A|}$ . Every  $g \in \mathcal{G}(\mathcal{A})$  can be written as a product  $\prod_i \mathcal{A}_{q_i}^{\epsilon_i}$ ,  $\epsilon_i \in \{-1, +1\}$

of the generators and their inverses. This implies that  $g \cdot a \in \mathcal{G}(\mathcal{A})$  for every  $a \in A$  and the action of  $g$  on  $A$  is a permutation  $\sigma_g$  of the symmetric group  $Sym(|A|)$  such that  $\sigma(a) = g \circ a$ . From this it follows that  $g$  can be represented by the element  $(g_0, \dots, g_{|A|-1})\sigma_g$  and this is called the *self-similar representation* of  $g$ . More precisely  $g$  can be regarded as an element of the wreath product  $Sym(|A|) \wr \mathcal{G}(\mathcal{A})$  and this gives an embedding of  $\mathcal{G}(\mathcal{A})$  into the iterated wreath product  $Sym(|A|) \wr (Sym(|A|) \wr \dots)$  [19]. The simplest infinite group that we can obtain by this construction is the (binary) Adding Machine isomorphic to  $\mathbb{Z}$ . It corresponds to  $\mathcal{A} = (Q, A, \delta, \lambda)$  where  $Q = \{q, s\}$ ,  $A = \{0, 1\}$ ,  $\delta(q, 0) = s$ ,  $\delta(q, 1) = q$ ,  $\delta(s, a) = s$  and  $\lambda(q, a) = 1 - a$ ,  $\lambda(s, a) = a$  for  $a \in A$ . The name is motivated by the fact the this group acts by adding 1 in the binary expansion of a positive integer. In this paper we consider groups (semigroups) that can arise from colorings that give rise to invertible Mealy automata. Therefore, given an *or*-digraph  $G = (V, E, \iota, \tau)$ , a *group coloring* is a pair  $(\chi_1, \chi_2)$  consisting of two DFA-colorings on  $G$  on the set  $A$  of cardinality equal to the out-degree of  $G$ . Thus, from  $(\chi_1, \chi_2)$  and  $G$  we can build the associated invertible Mealy automaton

$$\mathcal{M}(G, \chi_1, \chi_2) = (V, A, \delta, \lambda)$$

where  $\delta(v, a) = v'$  and  $\lambda(v, a) = b$  whenever there is an edge  $e = v \rightarrow v'$  such that  $\chi_1(e) = a$ ,  $\chi_2(e) = b$ . If  $\mathcal{A} = (Q, A, \delta)$  is a DFA, then we still call a group coloring of  $\mathcal{A}$  a DFA-coloring  $\chi$  on  $A$  of the underlying digraph  $D(\mathcal{A})$ . Hence the associated invertible Mealy automaton is clearly given by

$$\mathcal{M}(\mathcal{A}, \chi) = (Q, A, \delta, \lambda)$$

where  $\lambda(v, a) = b$  whenever  $v \xrightarrow{a} v'$  is a transition in  $\mathcal{A}$  corresponding to an edge  $e$  in  $D(\mathcal{A})$  colored by  $\chi(e) = b$ .

### 3 Reset Mealy automata

We generalize the definition of *reset* Mealy automaton given in [29].

**Definition 1.** A Mealy automaton  $\mathcal{A}$  is called *reset* if the following conditions are satisfied

- i)  $\mathcal{A}$  is synchronizing;
- ii)  $\mathcal{A}_q(\text{Syn}(\mathcal{A})) \subseteq \text{Syn}(\mathcal{A})$  for any  $q \in Q$ ;

For a given reset Mealy automaton  $\mathcal{A} = (Q, A, \delta, \lambda)$  we can also generalize the *modified state functions* introduced in [29] in the following way. For a given  $q \in Q$  the *modified state function* is the map

$$\widetilde{\lambda}_q : \text{Syn}(\mathcal{A}) \rightarrow Q$$

defined by  $\widetilde{\lambda}_q(u) = Q \cdot (q \circ u)$  for any  $u \in \text{Syn}(\mathcal{A})$ . Note that the definitions ensure the function to be well defined. We have the following theorem.

**Theorem 1.** *If  $\mathcal{A} = (Q, A, \delta, \lambda)$  is an invertible reset Mealy automaton with distinct modified state functions, then  $\mathcal{S}(\mathcal{A})$  is a free semigroup on  $\{\mathcal{A}_q : q \in Q\}$ .*

*Proof.* Suppose that  $\mathcal{S}(\mathcal{A})$  is not free on  $\{\mathcal{A}_q : q \in Q\}$ . By [29, Lemma 2.7], there must be a non-trivial relation of the form

$$\mathcal{A}_{p_n} \dots \mathcal{A}_{p_1} = \mathcal{A}_{q_n} \dots \mathcal{A}_{q_1} \quad (1)$$

for some  $n$ , and let us assume that  $n$  is the smallest integer for which a relation like (1) holds in  $\mathcal{S}(\mathcal{A})$ . Since  $\mathcal{A}$  has distinct modified state functions, then  $\mathcal{A}$  is also reduced, and so  $n \geq 2$ . Furthermore, there is a  $u \in \text{Syn}(\mathcal{A})$  such that  $\widetilde{\lambda}_{p_1}(u) \neq \widetilde{\lambda}_{q_1}(u)$ , hence  $Q \cdot (q_1 \circ u) \neq Q \cdot (p_1 \circ u)$ . In particular by condition ii) we have  $p_1 \circ u, q_1 \circ u \in \text{Syn}(\mathcal{A})$ , hence

$$q_2 \cdot (q_1 \circ u) \neq p_2 \cdot (p_1 \circ u) \quad (2)$$

If we apply both sides of (1) to  $uv$  for any  $v \in A^*$ , by Lemma 1 we get

$$\begin{aligned} \mathcal{A}_{p_n} \dots \mathcal{A}_{p_2} \mathcal{A}_{p_1}(uv) &= \mathcal{A}_{p_n} \dots \mathcal{A}_{p_2}(p_1 \circ u) \mathcal{A}_{p_1 \cdot u}(v) = \\ &= \mathcal{A}_{p_n} \dots (p_2 \circ (p_1 \circ u)) \mathcal{A}_{p_2 \cdot (p_1 \circ u)} \mathcal{A}_{p_1 \cdot u}(v) = \dots \\ &= (p_n \circ (\dots \circ (p_2 \circ (p_1 \circ u)))) \mathcal{A}_{t_n} \dots \mathcal{A}_{p_2 \cdot (p_1 \circ u)} \mathcal{A}_{p_1 \cdot u}(v) \\ \mathcal{A}_{q_n} \dots \mathcal{A}_{q_2} \mathcal{A}_{q_1}(uv) &= \mathcal{A}_{q_n} \dots \mathcal{A}_{q_2}(q_1 \circ u) \mathcal{A}_{q_1 \cdot u}(v) = \\ &= \mathcal{A}_{q_n} \dots (q_2 \circ (q_1 \circ u)) \mathcal{A}_{q_2 \cdot (q_1 \circ u)} \mathcal{A}_{q_1 \cdot u}(v) = \dots \\ &= (q_n \circ (\dots \circ (q_2 \circ (q_1 \circ u)))) \mathcal{A}_{s_n} \dots \mathcal{A}_{q_2 \cdot (q_1 \circ u)} \mathcal{A}_{q_1 \cdot u}(v) \end{aligned}$$

where  $t_i = p_i \cdot (p_{i-1} \circ (\dots \circ p_2 \circ (p_1 \circ u)))$  and  $s_i = q_i \cdot (q_{i-1} \circ (\dots \circ q_2 \circ (q_1 \circ u)))$ . Therefore, since (1) holds, we have

$$(q_n \circ (\dots \circ (q_2 \circ (q_1 \circ u)))) = (p_n \circ (\dots \circ (p_2 \circ (p_1 \circ u))))$$

and so we get

$$\mathcal{A}_{t_n} \dots \mathcal{A}_{p_2 \cdot (p_1 \circ u)} \mathcal{A}_{p_1 \cdot u}(v) = \mathcal{A}_{s_n} \dots \mathcal{A}_{q_2 \cdot (q_1 \circ u)} \mathcal{A}_{q_1 \cdot u}(v)$$

for any  $v \in A^*$ . Since  $u \in \text{Syn}(\mathcal{A})$ , then  $q_1 \cdot u = p_1 \cdot u$ , whence  $\mathcal{A}_{q_1 \cdot u} = \mathcal{A}_{p_1 \cdot u}$ , and since  $\mathcal{A}$  is invertible, we get

$$\mathcal{A}_{t_n} \dots \mathcal{A}_{p_2 \cdot (p_1 \circ u)}(v) = \mathcal{A}_{s_n} \dots \mathcal{A}_{q_2 \cdot (q_1 \circ u)}(v)$$

for any  $v \in A^*$ . However, by (2) and the fact that  $\mathcal{A}$  is reduced, we get  $\mathcal{A}_{p_2 \cdot (p_1 \circ u)} \neq \mathcal{A}_{q_2 \cdot (q_1 \circ u)}$ , whence

$$\mathcal{A}_{t_n} \dots \mathcal{A}_{p_2 \cdot (p_1 \circ u)} = \mathcal{A}_{s_n} \dots \mathcal{A}_{q_2 \cdot (q_1 \circ u)}$$

is a non-trivial relation with a number of elements  $n - 1$ , against the minimality of (1), a contradiction.  $\square$

**Remark 1.** Note that an analogous of Theorem 1 holds if we consider a larger class of Mealy automata, which we can call weakly reset. For an element  $\mathcal{A}$  in this class, we request that  $\mathcal{A}$  is synchronizing, and that there is a non-empty ideal  $H \subseteq \text{Syn}(\mathcal{A})$  such that  $\mathcal{A}_q(H) \subseteq H$  for any  $q \in Q$ . Note that with this last condition we need to modify also the definition of modified state function and consider these functions restricted to  $H$  instead of the whole set  $\text{Syn}(\mathcal{A})$ .

The notion of weakly reset Mealy automaton apparently depends on the sub-ideal  $H$  chosen. However, the following proposition shows that it is not the case and we can always choose a canonical sub-ideal.

**Proposition 1.** Let  $\mathcal{A} = (Q, A, \delta, \lambda)$  be a weakly reset Mealy automaton with respect to some ideal  $H$ , and let

$$\mathcal{I}(\mathcal{A}) = \text{Syn}(\mathcal{A}) \setminus \bigcup_{g \in \mathcal{S}(\mathcal{A})} g^{-1}(A^* \setminus \text{Syn}(\mathcal{A}))$$

Then  $\mathcal{I}(\mathcal{A})$  is the maximal two-sided ideal for which  $\mathcal{A}$  is weakly reset. In particular  $\mathcal{A}$  is weakly reset if and only if  $\mathcal{I}(\mathcal{A}) \neq \emptyset$ .

*Proof.* It is evident that  $\mathcal{I}(\mathcal{A})$  is fixed by  $\mathcal{S}(\mathcal{A})$  and it is the maximal set with respect to this property. It remains to prove that it is an ideal. Indeed, if  $u \in \mathcal{I}(\mathcal{A})$ , then for any  $v, v' \in A^*$  and  $g \in \mathcal{S}(\mathcal{A})$ , it is straightforward to check that the elements  $g(uv'), g(vu) \in \text{Syn}(\mathcal{A})$ , i.e.  $vu v' \in \mathcal{I}(\mathcal{A})$ .  $\square$

Recall that, any finitely generated group that contains a free semigroup (over at least two letters) is of exponential growth (see, for example [12]). From this and Theorem 1 we get the following



**Corollary 1.** *Let  $\mathcal{A}$  be an invertible (weakly) reset Mealy automaton on an alphabet  $A$ ,  $|A| \geq 2$ , and with distinct modified state functions, then  $\mathcal{G}(\mathcal{A})$  has exponential growth.*

We end this section with some algorithmic considerations, we prove that checking whether an invertible synchronizing Mealy automaton is reset is a decidable task, first we need to recall some basic facts on automata, and transducers theory (see for instance [17, 27]). We recall that a regular (rational) language is a subset  $L \subseteq A^*$  which is recognized by some finite automaton  $\mathcal{A} = (Q, A, \delta, q_0, F)$  where  $\delta \subseteq Q \times A \times Q$ . Using the usual subset construction we can always assume  $\mathcal{A}$  to be a DFA, furthermore the class of these languages are closed by the usual boolean operations which can be effectively implemented as well as checking if for two regular languages  $L_1, L_2$  it holds  $L_1 \subseteq L_2$ . We also recall the following lemma regarding the image of a regular languages by transducers, we present here with a proof for the sake of completeness.

**Lemma 2.** *Let  $\mathcal{A} = (Q, A, \delta, \lambda)$  be a Mealy machines and  $L \subseteq A^*$  be a regular language, then for any  $q \in Q$  the language  $\mathcal{A}_q(L)$  is regular.*

*Proof.* Suppose that  $L$  is recognized by the DFA  $\mathcal{A} = (P, A, \phi, p_0, F)$ . Therefore using the usual product construction consider the finite automaton

$$\mathcal{C} = (Q \times P, A, \eta, (q, p_0), Q \times F)$$

where

$$\eta((q_1, p_1), a) = \{(q_2, p_2) : \delta(q_1, a) = q_2, \lambda(q_1, a) = a, \phi(p_1, a) = p_2\}$$

it is straightforward to check that  $L[\mathcal{C}] = \mathcal{A}_q(L)$ , hence regular.  $\square$

We have the following decidability result regarding reset Mealy automata.

**Proposition 2.** *Let  $\mathcal{A} = (Q, A, \delta, \lambda)$  be an invertible synchronizing Mealy automaton, then the two following properties are decidable:*

- checking if  $\mathcal{A}$  is a reset Mealy automaton;
- for  $q \neq p$  checking whether or not  $\widetilde{\lambda}_q = \widetilde{\lambda}_p$ .

*Proof.* For the reset condition it is enough to check if the stability condition ii) in Definition 1 is decidable. It is sufficient to prove that for a fixed  $q \in Q$ ,  $\mathcal{A}_q(\text{Syn}(\mathcal{A})) \subseteq \text{Syn}(\mathcal{A})$  is decidable. Consider the associated DFA  $\mathcal{A} = (Q, A, \delta)$ , it is a well known fact that the power automaton  $\mathcal{P}(\mathcal{A}) =$

$(2^Q, A, \delta, Q, \{\{q\} : q \in Q\})$  recognizes  $\text{Syn}(\mathcal{A})$ . By Lemma 2  $\mathcal{A}_q(\text{Syn}(\mathcal{A}))$  is a regular language, therefore we can decide whether or not  $\mathcal{A}_q(\text{Syn}(\mathcal{A})) \subseteq \text{Syn}(\mathcal{A})$ .

We now prove that it is decidable to check whether or not  $\widetilde{\lambda}_q = \widetilde{\lambda}_p$ . For an  $s \in Q$ , consider the set

$$R(s) = \{u \in \text{Syn}(\mathcal{B}) : Q \cdot u = \{s\}\}$$

Note that

$$\mathcal{A}_q^{-1}(R(s)) \cap \text{Syn}(\mathcal{B}) = \{u \in \text{Syn}(\mathcal{B}) : \widetilde{\lambda}_q(u) = s\}$$

Therefore, to check if  $\widetilde{\lambda}_q = \widetilde{\lambda}_p$  it is enough to verify if

$$\mathcal{A}_q^{-1}(R(s)) \cap \text{Syn}(\mathcal{B}) = \mathcal{A}_p^{-1}(R(s)) \cap \text{Syn}(\mathcal{B}) \quad (3)$$

holds for any  $s \in Q$ . Since  $\text{Syn}(\mathcal{B})$  is regular, and the equality of two regular languages is decidable, then by Lemma 2 it is enough to prove that  $R(s)$  is regular. Indeed, if we consider the power automaton restricting the set of final states we get the DFA  $(2^Q, A, \delta, Q, \{s\})$  which recognizes  $R(s)$ .  $\square$

## 4 Group colorings of synchronizing DFA

In this section we consider group colorings on synchronizing DFAs. In view of Theorem 1, among the group colorings, we can consider the class of (*weakly*) *reset group colorings*. A (weakly) reset group coloring of a synchronizing DFA  $\mathcal{A}$  is a group coloring  $\chi$  of  $\mathcal{A}$  with the property that the associated Mealy automaton  $\mathcal{M}(\mathcal{A}, \chi)$  is (weakly) reset. We call a (weakly) reset Mealy automaton  $\mathcal{A}$  *singular* whenever all the modified state functions of  $\mathcal{A}$  are equal. For instance all the reset Mealy automata whose associated DFAs have a sink state are singular.

The first result we present is a gap theorem for (weakly) reset group colorings of simple synchronizing automata. We recall that a DFA  $\mathcal{A}$  is called *simple* whenever the set of (automata) congruences consists only of the identity  $1_{\mathcal{A}}$ , and the universal relation  $\omega_{\mathcal{A}}$  (see for instance [3, 30]). We have the following theorem.

**Theorem 2.** *Let  $\mathcal{A}$  be a simple synchronizing automaton, then for any (weakly) reset group coloring  $\chi$ , either  $\mathcal{S}(\mathcal{M}(\mathcal{A}, \chi))$  is a free semigroup or  $\mathcal{M}(\mathcal{A}, \chi)$  is singular.*

*Proof.* We consider the case of a group coloring, the weakly group coloring case is analogous and it is left to the reader. Let us prove that for any reset group coloring  $\chi$ , for the invertible Mealy automaton  $\mathcal{A}_\chi = \mathcal{M}(\mathcal{A}, \chi) = (Q, A, \delta, \lambda)$ , either the modified state functions  $\widetilde{\lambda}_q$ ,  $q \in Q$ , are all distinct, and so by Theorem 1  $\mathcal{S}(\mathcal{M}(\mathcal{A}, \chi))$  is free, or all the modified state functions are equal. Since  $\mathcal{A}$  is simple, it is sufficient to prove that the relation  $\sigma$  defined on  $Q$  by  $p\sigma q$  if  $\widetilde{\lambda}_p = \widetilde{\lambda}_q$  is a congruence on  $\mathcal{A}$ . It is straightforward to check that  $\sigma$  is an equivalence relation. Thus, we have to prove that if  $p\sigma q$ , then  $(p \cdot v)\sigma(q \cdot v)$  for any  $v \in A^*$ . Suppose, contrary to our statement, that there are distinct states  $p, q \in Q$  such that  $\widetilde{\lambda}_p = \widetilde{\lambda}_q$ , but  $\widetilde{\lambda}_{p \cdot v}(u) \neq \widetilde{\lambda}_{q \cdot v}(u)$  for some  $v \in A^*$  and  $u \in \text{Syn}(\mathcal{A})$ . Hence

$$Q \cdot ((p \cdot v) \circ u) \neq Q \cdot ((q \cdot v) \circ u)$$

In particular, since  $u \in \text{Syn}(\mathcal{A})$  and  $Q \cdot (p \circ v) \subseteq Q$ ,  $Q \cdot (q \circ v) \subseteq Q$ , we get

$$(Q \cdot (p \circ v)) \cdot ((p \cdot v) \circ u) \neq (Q \cdot (q \circ v)) \cdot ((q \cdot v) \circ u) \quad (4)$$

Using an induction on the length of the words, it is straightforward to check that  $Q \cdot (p \circ (vu)) = (Q \cdot (p \circ v)) \cdot ((p \cdot v) \circ u)$ . Hence by (4) we have  $Q \cdot (p \circ (vu)) \neq Q \cdot (q \circ (vu))$ , or equivalently  $\widetilde{\lambda}_p(vu) \neq \widetilde{\lambda}_q(vu)$  since  $\text{Syn}(\mathcal{A})$  is a two-sided ideal. Hence we get  $\widetilde{\lambda}_p \neq \widetilde{\lambda}_q$ , a contradiction.  $\square$

We say that a DFA  $\mathcal{A} = (Q, A, \delta)$  with a unique sink  $s$  is *bounded* if the set  $\{u = u_1 u_2 \dots \in A^\omega : q \cdot (u_1 \dots u_i) \neq s \ \forall i \in \mathbb{N}\}$  is finite, or equivalently, there are finitely many right infinite paths avoiding the sink. The definition of this class of DFA is motivated by the theory of automata groups [28]. In what follows, we frame the bounded automata in the more general class of *finitely generated synchronizing automata*. This class consists of the synchronizing automata whose language of synchronizing words is a finitely generated ideal [21, 23]. These automata have a combinatorial characterization in term of their power automata. First we need to recall some definitions from [23]. For a DFA  $\mathcal{A} = (Q, A, \delta)$ , a subset  $S \subseteq Q$  is called *reachable* if  $Q \cdot u = S$  for some  $u \in A^*$ , we put  $\text{Syn}(S) = \{u \in A^* : |S \cdot u| = 1\}$  and  $\text{Fix}(S) = \{u \in A^+ : S \cdot u = S\}$ . For a word  $w \in A^*$ ,  $m(w)$  denotes the maximum (with respect to the inclusion order) subset of  $Q$  fixed by  $w$ , i.e.  $m(w) \cdot w = m(w)$ . It is an easy exercise to prove that this set always exists, it is unique, and  $m(u) = Q \cdot u^k$  for some integer  $k$  with  $k \leq |Q| - |m(u)|$ . We have the following characterization.

**Theorem 3.** [23, Theorem 1] *A synchronizing automaton  $\mathcal{A} = (Q, A, \delta)$  is finitely generated if and only if for any reachable subset  $S \subseteq Q$  with  $1 < |S| < |Q|$  and for any  $u \in \text{Fix}(S)$ ,  $\text{Syn}(S) = \text{Syn}(m(u))$  holds.*

The following proposition places the class of bounded automata inside the class of finitely generated synchronizing automata.

**Proposition 3.** *Let  $\mathcal{A} = (Q, A, \delta)$  be a bounded DFA with sink  $s$  and  $|A| > 1$ , then  $\text{Syn}(\mathcal{A})$  is a finitely generated ideal.*

*Proof.* We first prove that  $\mathcal{A}$  is synchronizing. For this purpose, by the remark in Section 2 regarding automata with a unique sink state, it is sufficient to prove that for any state  $q \in Q$  there is a word  $u \in A^*$  such that  $q \cdot u = s$ . Let us assume, contrary to our claim, that there is a state  $p \in Q$  such that  $p \cdot u \neq s$  for all  $u \in A^*$ . Therefore, since  $|A| > 1$ , it is straightforward to verify that the set

$$\{u \in A^\omega : p \cdot u \neq s\}$$

is infinite, a contradiction.

We now prove that if  $S \subseteq Q$  is reachable and  $w \in \text{Fix}(S)$ , then  $S = m(w)$ , and so by Theorem 3  $\mathcal{A}$  is finitely generated. Suppose, contrary to our claim, that there is a reachable subset  $S \subseteq Q$  and  $w \in \text{Fix}(S)$  such that  $S \subsetneq m(w) \subseteq Q$ . Let  $u \in A^+$  such that  $Q \cdot u = S$ , and let  $q \in m(w) \setminus S$ . Since  $Q \cdot u = S$ , the vertex  $p = q \cdot u \in S$ . Since  $w$  acts like a permutation on  $m(w)$ , and  $S \subseteq m(w)$ , then there is an integer  $m > 0$  such that  $p \cdot w^m = p$ ,  $q \cdot w^m = q$ . Therefore, for any  $k, h \geq 1$  we have paths

$$q \xrightarrow{w^{km}u(w^m)^h} p$$

avoiding the sink  $s$ . Hence, we have distinct right infinite paths labeled by  $w^{km}u(w^m)^\omega$  for any  $k \geq 1$ . Thus, by the boundedness hypothesis, and by simple considerations on the combinatorics of words, we necessarily have  $w = uw' = w'u$  for some  $w' \in A^*$ . Therefore, there is an integer  $\ell \geq 1$  such that

$$m(w) = Q \cdot w^\ell = S \cdot w^{\ell-1}w' = S \cdot w'$$

Hence,  $|m(w)| \leq |S|$ , and since  $S \subseteq m(w)$ , we get  $m(w) = S$ , a contradiction.  $\square$

In the class of synchronizing DFA with a sink state we now consider the more general case of group colorings. We characterize the class of synchronizing DFAs with sink for which any group coloring (not just reset group coloring) gives rise to an invertible Mealy automaton whose associated group is finite. Before proving the characterization, we define the notion of *nilpotent* automata. This particular class of synchronizing automata has been introduced by Perles et al. in 1962 under the name of definite table [20].

Later, such automata were studied by Rystsov in [26] in view of Černý's conjecture. In the present paper we use the definition from [26]. Namely, we say that a DFA  $\mathcal{A} = (Q, A, \delta)$  is nilpotent if there is a state  $s \in Q$  and a positive integer  $n \geq 1$  such for any word  $w \in A^*$  of length at least  $n$  it holds  $Q \cdot w = \{s\}$ . Obviously, any nilpotent automaton is a finitely generated synchronizing automaton with a sink state  $s$ . This automata also represent, in some sense, the worst case from the computational complexity theory point of view, since they are fundamental in proving the co- $NP$ -hardness of the problem of recognizing finitely generated synchronizing automata [23, Theorem 6]. It is an easy exercise to prove that a DFA  $\mathcal{A}$  with a unique sink state is nilpotent if and only if there are no cycles or loops passing through non-sink states. Therefore, nilpotent automata are also bounded. The next result establishes a connection between automata groups theory and nilpotent DFA. Put

$$GC(\mathcal{A}) = \{\mathcal{G}(\mathcal{M}(\mathcal{A}, \chi)) : \chi \text{ is a group coloring on } \mathcal{A}\}$$

**Proposition 4.** *Let  $\mathcal{A} = (Q, A, \delta)$  be a synchronizing automaton with a sink  $s$  and  $|A| > 1$ . If  $\mathcal{A}$  is not nilpotent then there exists a group coloring  $\chi$  such that  $\mathcal{G}(\mathcal{M}(\mathcal{A}, \chi))$  contains a subgroup isomorphic to  $\mathbb{Z}$ .*

*Proof.* We can suppose that there exists at least one cycle in  $\mathcal{A}$

$$q_0 \xrightarrow{x_0} q_1 \xrightarrow{x_1} \dots \xrightarrow{x_{k-2}} q_{k-1} \xrightarrow{x_{k-1}} q_k = q_0 \quad (5)$$

avoiding the sink state  $s$ , which is labeled by  $v = x_0 \dots x_{k-1} \in A^k$ , and a path

$$q_0 = p_0 \xrightarrow{y_0} p_1 \xrightarrow{y_1} \dots \xrightarrow{y_{d-2}} p_{d-1} \xrightarrow{y_{d-1}} p_d = s \quad (6)$$

labelled by the word  $y = y_0 \dots y_{d-1} \in A^d$  such that  $q_0 \cdot y = s$  and no state of  $\{p_0, \dots, p_d\}$  belongs to any cycle with the same properties. We consider the following two cases:

- Assume  $d \leq k$ . Consider the group coloring  $\chi$  defined by

$$q_0 \xrightarrow{x_0|y_0} q_1 \xrightarrow{x_1|y_1} \dots q_{d-1} \xrightarrow{x_{d-1}|y_{d-1}} q_d \xrightarrow{x_d|x_d} q_{d+1} \dots q_{k-1} \xrightarrow{x_{k-1}|x_{k-1}} q_k$$

and

$$p_0 \xrightarrow{y_0|x_0} p_1 \xrightarrow{y_1|x_1} \dots p_{d-1} \xrightarrow{y_{d-1}|x_{d-1}} p_d$$

while for the other edges is defined in such a way that  $\chi$  is a group coloring (this can be always done since there is no common edge between the two paths (5) and (6)) and with identity on the sink, i.e.  $s \xrightarrow{a|a} s$  for  $a \in A$ . Putting  $y_i = x_i$  for  $d \leq i \leq k-1$ , notice that

$$q_0 \circ (x_0 \dots x_{k-1}) = y_0 \dots y_{k-1}, \quad q_0 \cdot (x_0 \dots x_{k-1}) = q_0$$

and

$$q_0 \circ (y_0 \cdots y_{k-1}) = x_0 \cdots x_{k-1}, \quad q_0 \cdot (y_0 \cdots y_{k-1}) = s,$$

After passing to a new alphabet  $Y = A^k$ , in such a way that  $\bar{0} \in Y$  corresponds to  $x_0 \cdots x_{k-1} \in A^k$  and  $\bar{1} \in Y$  corresponds to  $y_0 \cdots y_{k-1} \in A^k$ , we get that  $q_0 \cdot \bar{0} = q_0$ ,  $q_0 \cdot \bar{1} = s$ ,  $q_0 \circ \bar{x} = \overline{1-x}$ , for  $x \in \{0, 1\}$ . This means that its self-similar representation is  $q_0 = (q_0, s, \dots)(\bar{0}\bar{1})\sigma$ , for some  $\sigma \in \text{Sym}(Y \setminus \{\bar{0}, \bar{1}\})$  and so it generates a group acting as the Adding machine on the subtree  $\{\bar{0}, \bar{1}\}^*$ . Hence  $\mathcal{G}(\mathcal{M}(\mathcal{A}, \chi))$  contains a subgroup isomorphic to  $\mathbb{Z}$ .

- If  $d > k$ , let  $y_0 \cdots y_{k-1} \in A^k$  such that  $q_0 \cdot (y_0 \cdots y_{k-1}) = q_1$ . Note that by the choice of the path (6),  $q_1$  does not belong to any other cycle. This implies that  $q_1 \cdot (y_0 \cdots y_{k-1})^t y_0 \cdots y_i \neq q_0$  for any  $t \geq 0$  and  $i \leq k-1$ . Define  $\chi$  in such a way that

$$q_0 \circ (x_0 \cdots x_{k-1}) = y_0 \cdots y_{k-1}, \quad q_0 \cdot (x_0 \cdots x_{k-1}) = q_0$$

and

$$q_0 \circ (y_0 \cdots y_{k-1}) = x_0 \cdots x_{k-1}, \quad q_0 \cdot (y_0 \cdots y_{k-1}) = q_1.$$

Moreover impose that  $q_1 \circ (y_0 \cdots y_{k-1})^t y_0 \cdots y_i = (y_0 \cdots y_{k-1})^t y_0 \cdots y_i$ . Consider the alphabet  $Y = A^k$  and let  $\bar{0}$  and  $\bar{1}$  correspond to  $x_0 \cdots x_{k-1}$  and  $y_0 \cdots y_{k-1}$  respectively. The action of  $q_0$  on the infinite word  $\bar{0}^\infty$  is such that

$$q_0 \circ \bar{0}^\infty = \bar{1}^\infty, \quad q_0^{1+n} \circ \bar{0}^\infty = \bar{1}^n \bar{0} \bar{1}^\infty.$$

Since  $q_0$  is invertible and  $q_0^n \neq id$  for every  $n$ , we get that the subgroup of  $\mathcal{G}(\mathcal{M}(\mathcal{A}, \chi))$  generated by  $q_0$  is isomorphic to  $\mathbb{Z}$ .

□

The following theorem shows an algebraic characterization of nilpotent DFAs inside the class of synchronizing automata with sink.

**Theorem 4.** *Let  $\mathcal{A} = (Q, A, \delta)$  be a synchronizing automaton with a sink  $s$  and  $|A| > 1$ . Then any group in  $GC(\mathcal{A})$  has finite order if and only if  $\mathcal{A}$  is nilpotent.*

*Proof.* First suppose that the DFA  $\mathcal{A}$  is nilpotent, then for every right infinite word  $w = w_1 w_2 \cdots \in A^\omega$ , and for every state  $q \in Q$  there is  $n$  such that  $q \cdot w_1 \cdots w_n = s$ . Let  $\chi$  be a group coloring of  $\mathcal{A}$ , and consider the associated

Mealy automaton  $\mathcal{A} = \mathcal{M}(\mathcal{A}, \chi)$ . Consider the action of  $\mathcal{M}$  on  $w$ . Every generators  $\mathcal{A}_q$  acts non trivially on  $w_1 \dots w_n$ , and acts as a permutation  $\sigma \in \text{Sym}(|A|)$  (induced by the action of  $s$  on  $A$ ) on every symbol  $w_i$ , with  $i > n$ . This implies that  $\mathcal{A}_q$  can be identified with the pair  $(g', \sigma)$ , where  $g'$  is an element of the wreath product  $\text{Sym}(|A|) \wr \dots \wr \text{Sym}(|A|)$  of  $n$  copies of  $\text{Sym}(|A|)$ . This implies that the associated group  $\mathcal{G}(\mathcal{A})$  is finite.

On the other hand suppose that  $\mathcal{A}$  is not nilpotent, then Proposition 4 says that there exists a group coloring  $\chi$  such that  $\mathcal{G}(\mathcal{M}(\mathcal{A}, \chi))$  contains a subgroup isomorphic to  $\mathbb{Z}$ . In particular  $\mathcal{G}(\mathcal{M}(\mathcal{A}, \chi))$  is infinite.  $\square$

Note that Proposition 4 is constructive. Therefore, by the above theorem, for any given synchronizing automaton which is not nilpotent, there is always a constructive way to color it in an invertible Mealy automaton such that the resulting associated group is infinite. Furthermore, note that each group coloring  $\chi$  of a nilpotent automaton is also a reset group coloring. Indeed, for a nilpotent automaton  $\mathcal{A}$ ,  $\text{Syn}(\mathcal{A}) = A^{\geq k}$  for some positive integer  $k$ , and  $\mathcal{A}_q = \mathcal{M}(\mathcal{A}, \chi)_q$ , for any state  $q$  and any group coloring  $\chi$ , is a transformation on the rooted regular tree  $T_{|A|}$ , hence  $\mathcal{A}_q(\text{Syn}(\mathcal{A})) \subseteq \text{Syn}(\mathcal{A})$  clearly holds.

## 5 Examples of reset Mealy automata

So far we have generalized the concept of reset automaton presented in [29] without presenting any example of automaton satisfying the conditions of Definition 1 but which is different from the kind of reset automata considered in [29]. Note that, by [25], for any regular ideal language  $I \subseteq A^*$  on an alphabet with  $|A| > 1$  there is a strongly connected<sup>1</sup> synchronizing automaton whose set of reset words is exactly  $I$ . We have already noted at the end of Section 4 that any group coloring of a nilpotent automaton gives rise to a reset Mealy automaton. Not all the synchronizing automata having  $A^{\geq k}$ , for some  $k > 0$ , as set of reset words are nilpotent. However, the same argument at the end of Section 4 holds, thus any group coloring gives rise to a reset Mealy automaton. We record this fact in the following

**Proposition 5.** *Let  $\mathcal{A}$  be a synchronizing automaton such that  $\text{Syn}(\mathcal{A}) = A^{\geq k}$ , for some  $k > 0$ . Then for any group coloring  $\chi$ , the associated Mealy automaton  $\mathcal{M}(\mathcal{A}, \chi)$  is reset.*

---

<sup>1</sup>A DFA  $\mathcal{A} = (Q, A, \delta)$  is called strongly connected whenever for any  $q, q' \in Q$  there is a word  $u \in A^*$  such that  $\delta(q, u) = q'$ .

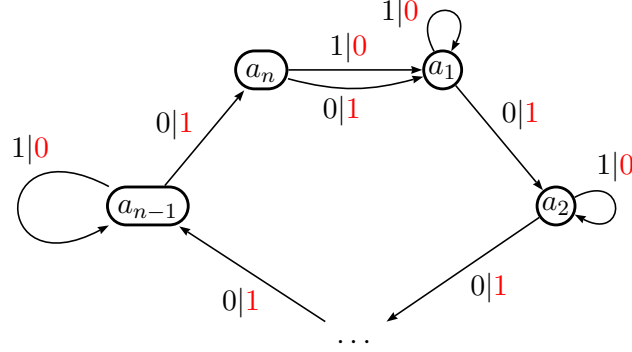


Figure 1: A weakly reset group coloring of the Černý's automaton  $\mathcal{C}_n$ .

When dealing with synchronization, the Černý's series is a fundamental example of synchronizing automata since it is the only infinite series reaching the bound  $(n-1)^2$  for the minimal synchronizing words. In Figure 1 it is depicted a group coloring of the Černý's automaton  $\mathcal{C}_n$  which gives rise to a weakly reset Mealy automaton  $\mathcal{C}_n$ . The group coloring is defined by coloring each transition  $q_1 \xrightarrow{x} q_2$  by  $q_1 \xrightarrow{x|1-x} q_2$ , for  $x \in \{0, 1\}$ . The automaton  $\mathcal{C}_n$  is weakly reset by taking the two sided ideal  $I$  generated by the two synchronizing words  $w_1 = 1^{n-1}(0^{n-1}1^{n-1})^{n-2}0^{n-1}$ ,  $w_2 = 0^{n-1}(1^{n-1}0^{n-1})^{n-2}1^{n-1}$ . It is routine to check that each  $(\mathcal{C}_n)_q$ , for each state  $q$ , transforms  $w_1$  into  $w_2$  and vice versa. It is also not hard to see that the group  $\mathcal{G}(\mathcal{C}_n)$  generated is isomorphic to  $(\mathbb{Z}/(2\mathbb{Z}))^n$ . This coloring generates a weakly reset Mealy automaton which is not reduced and, in particular, it is singular, i.e. all the modified state functions are equal. The next natural step is to produce examples of reset coloring for which Theorem 1 can be applied, hence we are seeking for reset group colorings for which the modified state functions are all distinct. In this case it comes in handy Theorem 2 since if the underlying DFA is simple, then we just have to exclude the singularity condition.

The following lemma provides some natural sufficient conditions on a DFA to be simple.

**Lemma 3.** *Let  $\mathcal{A} = (Q, A, \delta)$  be a synchronizing automaton with  $|Q|$  prime and having a subset  $B \subseteq A$  such that  $B^*$  acts transitively on  $Q$  like a permutation group. Then  $\mathcal{A}$  is simple.*

*Proof.* If  $\mathcal{A}$  is not simple, then there is an automata congruence  $\sigma$  with  $\sigma \neq 1_{\mathcal{A}}, \omega_{\mathcal{A}}$ . Thus there is an equivalence class  $[q]_{\sigma}$  of  $Q/\sigma$  with  $1 < |[q]_{\sigma}| < |Q|$ . Since  $\sigma$  is a congruence, and  $B^*$  acts like a permutation group transitively on  $Q$ , then  $|[q']_{\sigma} \cdot u| = |[q']_{\sigma}|$  for any  $q' \in Q$  and  $u \in B^*$ . Thus by the transitivity



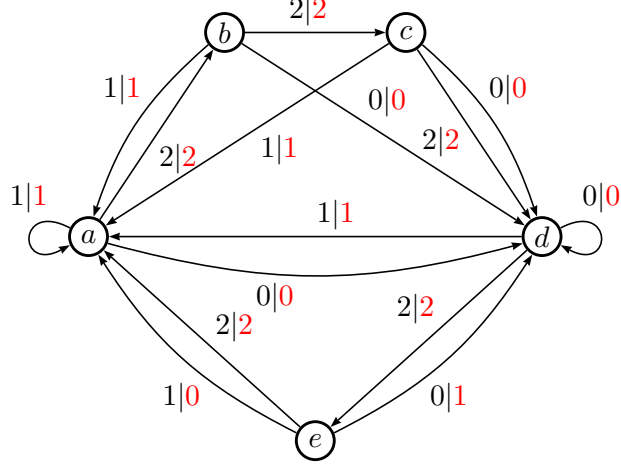


Figure 2: An example of a group coloring of a DFA described in the proof of Proposition 6 where the chosen state is  $e$

we get  $|Q| = |Q/\sigma||[q]_\sigma|$  with  $1 < |[q]_\sigma| < |Q|$ , a contradiction.  $\square$

For instance all the Černý's automata  $\mathcal{C}_n$ , with  $n$  prime, are simple. The following proposition provides a way to color particular simple synchronizing automata in such a way that the resulting associated monoid is free.

**Proposition 6.** *Let  $\mathcal{A} = (Q, A, \delta)$  be a synchronizing automaton such that  $|Q| > 1$  is prime, there is a  $B \subseteq A$  for which  $B^*$  acts transitively on  $Q$ , and with two elements  $a, b \in A \cap \text{Syn}(\mathcal{A})$  such that  $Q \cdot a \neq Q \cdot b$ . Then there is a weakly reset group coloring  $\chi$ , such that  $\mathcal{S}(\mathcal{M}(\mathcal{A}, \chi))$  is free.*

*Proof.* Choose a state  $q$ , and consider the group coloring  $\chi$  defined by

$$q \xrightarrow{a|b} v, \quad q \xrightarrow{b|a} v', \quad q \xrightarrow{s|s} v'', \quad s \in A \setminus \{a, b\}$$

while  $p \xrightarrow{s|s} p'$  for any  $p \in Q \setminus \{q\}$ ,  $s \in A$ . Put  $\mathcal{B} = \mathcal{M}(\mathcal{A}, \chi)$ . Note that  $\chi$  is a weakly reset group coloring such that  $\mathcal{B}_q(I) \subseteq I$  for any  $q \in Q$ , and  $I = A^*\{a, b\}A^*$ . Since by Lemma 3  $\mathcal{A}$  is simple, then by Theorem 2 we get that either  $\mathcal{B}$  is singular, or  $\mathcal{S}(\mathcal{B})$  is free. We prove that the singular condition does not occurs. Indeed, since  $|Q| > 1$  consider any  $p \in Q \setminus \{q\}$ , then by the definition of  $\chi$  we get

$$\widetilde{\lambda}_q(a) = Q \cdot b \neq Q \cdot a = \widetilde{\lambda}_p(a)$$

Therefore,  $\mathcal{B}$  can not be singular, and so  $\mathcal{S}(\mathcal{M}(\mathcal{A}, \chi))$  is free.  $\square$

This last proposition shows examples of synchronizing automata which can be colored in such a way that the associated semigroup is free. However, the synchronization is quite trivial being these automata synchronized by a one letter of the alphabet. We now present a way to color a particular class of finitely generated synchronizing automata having non-trivial reset words in such a way that the associated semigroup is free. These automata are the De Bruijn automata and they are built from the De Bruijn graphs of the words  $A^k$ . These graphs were first defined by N. G. de Bruijn [11] and they are connected to symbolic systems. Indeed, given a subshift  $(X, S)$  it is possible to associate to the language  $L_k(X)$  of all the factors of  $X$  of length  $k$ , some graphs, called Rauzy graphs [9, 24]. De Bruijn graphs are Rauzy graphs when  $L_k(X) = A^k$ , or equivalently when  $X$  is a full shift. We now introduce the De Bruijn automata in a slightly more general form, indeed we assume that the finite alphabet  $A$  is endowed with a structure of group  $(A, \star)$ . This condition is not required for the definition of these automata, however it is used in the definition of the group coloring presented later. The De Bruijn automata  $\mathcal{B}_k(A) = (Q, A, \delta)$ , for  $k > 1$ , is the DFA whose set of states is given by  $Q = A^k$  and there is a transition  $u \xrightarrow{x} v$  if  $u = ys$ ,  $v = sx$  for some  $s \in A^{k-1}$ . It is evident that the underlying graph of  $\mathcal{B}_k(A)$  is the De Bruijn graph of order  $k$  with respect to the alphabet  $A$ . Moreover, it is not difficult to check that this automaton is a finitely generated synchronizing automaton which is also strongly connected. Another interesting feature of these automata is that  $\mathcal{B}_k(A)$  is the only strongly connected (finitely generated) synchronizing automata (up to isomorphisms) whose set of reset words is  $A^{\geq k}$  [16, Theorem 1]. Since  $\text{Syn}(\mathcal{B}_k(A)) = A^{\geq k}$ , then by Proposition 5 a group coloring for a De Bruijn automaton is necessarily a reset group coloring. For a word  $u = u_1 \dots u_k \in A^k$ , let  $u[i] = u_i$ , for  $1 \leq i \leq k$ , denote the  $i$ -th component of  $u$ , and for  $i \geq 0$  we denote by  $u[0, i] = u_1 \dots u_i$  with the convention that  $u[0, 0]$  is the empty word. Without loss of generality we can view  $u$  as an element  $(u_1, \dots, u_k) \in A^k$  in the direct product  $(A^k, \star)$ . Consider the group coloring  $\chi_k(A)$  on  $\mathcal{B}_k(A)$  defined on the transitions by the following rule. If we have the transition  $u \xrightarrow{a} u'$  with  $u = ys$ ,  $u' = sx$  for some  $s \in A^{k-1}$ ,  $x, y \in A$ , then we color this transition as:

$$u \xrightarrow{x|xy^{-1}} u'$$

Using the fact that  $(A, \star)$  is a group, it is straightforward to see that  $\chi_k(A)$  is actually a group coloring. In Figure 3 it is depicted the reset Mealy automaton  $\mathcal{M}(\mathcal{B}_k(A), \chi_k(A))$  in the case  $k = 3$  and  $(A, +) = (\mathbb{Z}_2, +)$  with the usual operation of sum modulo two. Note that the Mealy automaton  $\mathcal{M}(\mathcal{B}_1(\mathbb{Z}_2), \chi_1(\mathbb{Z}_2))$  is the automaton given by Grigorchuk and Żuk, whose

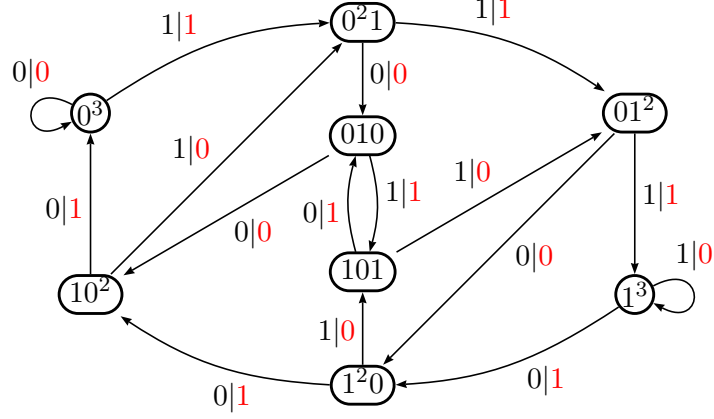


Figure 3: A reset group coloring for the De Bruijn automaton  $\mathcal{B}_3(\mathbb{Z}_2)$  whose associated semigroup is free. Note that for any  $u, v \in A^3$ ,  $u \circ v = u + v \pmod 2$ .

associated group is the lamplighter group  $\mathbb{Z}_2 \wr \mathbb{Z}$  [15].

The following proposition shows that the semigroup associated to all the De Bruijn automata with this coloring are free.

**Proposition 7.** *With the above notation  $\mathcal{M}(\mathcal{B}_k(A), \chi_k(A))$  is a reset Mealy automaton with all different modified state functions. In particular, the associated semigroup  $\mathcal{S}(\mathcal{M}(\mathcal{B}_k(A), \chi_k(A)))$  is free.*

*Proof.* We have already remarked that  $\mathcal{B}_k(A)$  is reset invertible Mealy automaton. It is not hard to check, by the definition of the action  $\delta$ , that for a word  $u \in A^k$ ,  $Q \cdot u = \{u\}$ . We claim that for any pair  $q \neq q'$  of states, and for any element  $u \in A^k$ , we have

$$\lambda_q(u) = Q \cdot (q \circ u) \neq Q \cdot (q' \circ u) = \lambda_{q'}(u)$$

By the previous remark, since  $Q \cdot u = \{u\}$ , it is enough to show that for  $q \neq q'$ ,  $q \circ u \neq q' \circ u$ . To prove this fact consider the functions  $\zeta : A^k \times A^\ell \rightarrow A^\ell$ ,  $\ell \geq 1$ , defined componentwise by

$$\zeta(q, v)_i = (q \cdot v[0, i-1])[1], \text{ for } 1 \leq i \leq \ell$$

Starting from the state  $q$  and applying the word  $v$ , this function takes trace of the elements that are multiplied in the output function. Therefore, using

an induction on the length of  $v$ , it is easy to prove that

$$q \circ v = v \star \zeta(q, v)^{-1} \quad (7)$$

holds. We claim that for any  $v \in A^k$ , we have

$$\zeta(q, v) = q \quad (8)$$

Indeed, let  $q = q_1 \dots q_k$ , we prove by induction on the index  $1 \leq i \leq k$ , that  $q[i] = \zeta(q, v)_i$ . It is evident that the base of the induction holds since  $q[1] = (q \cdot v[0, 0])[1]$ . Thus, assume the statement true for  $i - 1 \geq 1$ . It is straightforward to check, using the definition of the action  $\delta$ , that

$$q \cdot v[0, i - 1] = q_i \dots q_k v[0, i - 1]$$

Hence,

$$\zeta(q, v)_i = (q \cdot v[0, i - 1])[1] = (q_i \dots q_k v[0, i - 1])[1] = q_i$$

and so claim (8) holds. Let  $q, q'$  be two different states, and let  $v \in A^k$ . Assume, contrary to our claim, that  $q \circ v = q' \circ v$ , whence by (7) and (8) we obtain:

$$v \star q^{-1} = q \circ v = q' \circ v = v \star (q')^{-1}$$

Thus, since  $(A, \star)$  is a group, we get  $q = q'$ , a contradiction.  $\square$

Let  $\mathcal{B}(k, A) = \mathcal{G}(\mathcal{M}(\mathcal{B}_k(A), \chi_k(A)))$ , if we assume  $(A, +)$  to be a non-trivial abelian group, by using similar techniques involved in [29, Theorem 3.1], we obtain the following analogous structural result.

**Theorem 5.** *If  $(A, +)$  is a non-trivial finite abelian group, then*

$$\mathcal{B}(k, A) = A^k \wr \mathbb{Z}$$

As in [29] we consider the ring  $G[[t]]$  of formal power series with coefficients in  $G$ , we may identify all the words in  $G^\omega$  as elements in  $G[[t]]$  via the correspondence:

$$g = g_0 g_1 g_2 \dots \longleftrightarrow F_g(t) = \sum_{i=0}^{\infty} g_i t^i$$

The following lemma shows how the action of the elements in  $\mathcal{B}(k, A)$  on  $A^\omega$  is reflected in the formal power series.

**Lemma 4.** Let  $(A, +)$  be a non-trivial finite abelian group, and let  $\mathcal{B} = \mathcal{M}(\mathcal{B}_k(A), \chi_k(A))$ . Therefore, for any state  $q$  of  $\mathcal{B}$  we have:

$$F_{\mathcal{B}_q(g)}(t) = (1 - t^k)F_g(t) - F_q(t), \quad F_{\mathcal{B}_q^{-1}(g)}(t) = (F_g(t) + F_q(t)) \frac{1}{(1 - t^k)} \quad (9)$$

Moreover, if  $e = 0^k$ , where  $0$  is the neutral element of  $A$ , then for any  $q \in Q$  and  $\ell \neq 0$  we have:

$$F_{\mathcal{B}_e^\ell \mathcal{B}_q \mathcal{B}_e^{-\ell}(g)}(t) = F_g(t) - (1 - t^k)^\ell F_q(t) \quad (10)$$

*Proof.* Let  $q = q_1 \dots q_k \in A^k$ . An element  $g \in A^\omega$  can be (uniquely) factorized as a product of words in  $A^k$ . Therefore, using equations (8), (7) in the proof of Proposition 7, it is not difficult to check that

$$F_{\mathcal{B}_q(g)}(t) = F_g(t) - F_{qg}(t)$$

with  $qg = q_1 \dots q_k g_1 g_2 \dots$ . Since  $F_{qg}(t) = F_q(t) + t^k F_g(t)$ , we obtain the first claim of the lemma, the other equality follows from the first one and the equality:

$$\sum_{i=0}^{\infty} t^{ki} = \frac{1}{(1 - t^k)}$$

Equality (10) can be proved by a straightforward induction using equations (9).  $\square$

**Lemma 5.** With the above notation, if:

$$P = \sum_{i=0}^N (1 - t^k)^{\ell_i} c_i = 0 \quad (11)$$

where  $\ell_i \in \mathbb{Z}$  and  $c_i$  are polynomial of degree at most  $k - 1$ , then  $c_i = 0$ .

*Proof.* Suppose, contrary to the claim, that not all of the  $c_1, \dots, c_N$  are zero. Let  $\ell = \max\{|\ell_i|, i = 1, \dots, N\}$ , multiplying by  $(1 - t^k)^\ell$  on the both sides of equality (11), we can suppose, without loss of generality, that  $0 \leq \ell_i < \ell_{i+1}$  for  $0 \leq i \leq N - 1$ , and  $c_i \neq 0$  for  $0 \leq i \leq N$ . It is straightforward to check that  $P - t^{k\ell_N} c_N$  is a polynomial of degree at most  $k\ell_N - 1$ . Hence if (11) holds, then  $t^{k\ell_N} c_N = 0$ , i.e  $c_N = 0$ , contradiction.  $\square$

*Proof of Theorem 5.* By (10) of Lemma 4 the mapping in  $A^k \rightarrow \mathcal{B}(k, A)$  defined by  $h \mapsto \mathcal{B}_h \mathcal{B}_e$ , where  $e$  is the neutral element of  $A^k$ , is injective.

If  $a = \mathcal{B}_e^{-1}$ , then  $\mathcal{B}(k, A) = \langle A^k, a \rangle$ . Moreover, by (10) of Lemma 4 and Lemma 5 we have that the subgroup  $H = \langle a^\ell q a^{-\ell} : q \in A^k, \ell \in \mathbb{Z} \rangle$  is isomorphic to  $\bigoplus_{\mathbb{Z}} A^k$ . Therefore, since  $\mathcal{B}(k, A) = H \langle a \rangle$  with  $H$  and  $\langle a \rangle$  intersecting trivially, having  $a$  infinite order and  $H$  being of torsion, and since  $a$  acts on  $H$  by conjugation as the shift on  $\mathbb{Z}$ , we get

$$\mathcal{B}(k, A) \simeq \bigoplus_{\mathbb{Z}} A^k \rtimes \mathbb{Z} = A^k \wr \mathbb{Z}$$

□

## 6 Open Problems

We give a list of natural open problems originated by the previous results.

**Problem 1.** *In Proposition 2 we prove that checking whether a Mealy automaton is reset or not is a decidable problem. However, unlike the conditions of [29] which can be checked in linear time for a particular subclass of reset Mealy automata, the algorithm proposed here is not polynomial. The natural question is to find the computational class where this problem lies. By far it is not even known if this problem is in the class **NP** or not. Things become even more unclear in the case of checking the weakly reset condition. This problem is clearly equivalent to checking whether or not  $\mathcal{I}(\mathcal{A}) \neq \emptyset$ , which is not known whether or not it is decidable.*

**Problem 2.** *Is there any combinatorial characterization of the synchronizing automata possessing a (weakly) reset group coloring. In particular, are there examples of synchronizing automata which do not have any (weakly) reset group coloring?*

**Problem 3.** *Theorem 2 gives a gap result for (weakly) reset group colorings of simple synchronizing automata. It would be interesting to give structural results for the groups (semigroups) associated to singular (weakly) reset Mealy automata.*

**Problem 4.** *It would be interesting to explore the algebraic properties of the groups obtained by (some) colorings of the Černý's series  $\mathcal{C}_n$  or the De Bruijn groups  $\mathcal{B}(A, k)$  in case  $(A, \star)$  is not abelian.*

**Problem 5.** *Can we say more about the structure of the groups defined by a reset Mealy automata with distinct modified state functions?*

## Acknowledgments

The first author was supported by Austrian Science Fund project FWF P24028-N18.

The second author acknowledges support from the European Regional Development Fund through the programme COMPETE and by the Portuguese Government through the FCT – Fundação para a Ciência e a Tecnologia under the project PEst-C/MAT/UI0144/2011 and the support of the FCT project SFRH/BPD/65428/2009.

## References

- [1] J. Almeida, S. Margolis, B. Steinberg, and M. Volkov. Representation theory of finite semigroups radical and formal language theory. *Trans. Amer. Math. Soc.*, 361:1429–1461, 2009.
- [2] D.S. Ananichev and M.V. Volkov. *Some results on Černý type problems for transformation semigroups*. World Scientific, 2002.
- [3] I. Babcsányi. Automata with finite congruence lattices. *Acta Cybernetica*, 18(1):155–165, 2007.
- [4] L. Bartholdi, V. Kaimanovich, and V. Nekrashevych. On amenability of automata groups. *Duke Math. J.*, 154(3):575–598, 2010.
- [5] L. Bartholdi and V. Nekrashevych. Thurston equivalence of topological polynomials. *Act Math*, 197:1–51, 2006.
- [6] J. Berstel, D. Perrin, and C. Reutenauer. *Codes and Automata*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010.
- [7] I. Bondarenko, T. Ceccherini-Silberstein, A. Donno, and V. Nekrashevych. On a family of Schreier graphs of intermediate growth associated with a self-similar group. *European Journal of Combinatorics*, 33:1408–1421, 2012.
- [8] I. Bondarenko, D. D’Angeli, and T. Nagnibeda. Ends of Schreier graphs of self-similar groups. *In preparation*.
- [9] M. Boshernitzan. A condition for minimal interval exchange maps to be uniquely ergodic. *Duke Math. J.*, 53(3):723–752, 1985.

- [10] D. D’Angeli, A. Donno, M. Matter, and T. Nagnibeda. Infinite Schreier graphs of the Basilica group. *Journal of Modern Dynamics*, 2(24):153–194, 2010.
- [11] N. G. de Bruijn. A combinatorial problem. *Proc. Konin. Neder. Akad. Wet.*, 49:83–96, 1946.
- [12] P. de la Harpe. *Topics in geometric group theory*. University of Chicago Press., 2000.
- [13] S. Eilenberg. *Automata, Languages, and Machines*, volume A of *Pure and Applied Mathematics*. Academic Press, 1974.
- [14] R. Grigorchuk. Some topics of dynamics of group actions on rooted trees. *The Proceedings of the Steklov Institute of Math.*, 273:1–118, 2011.
- [15] R. Grigorchuk and A. Zuk. The lamplighter group as a group generated by a 2-state automaton, and its spectrum. *Geom. Dedicata*, 87:209–244, 2001.
- [16] V.V. Gusev, M.I. Maslennikova, and E.V. Pribavkina. Finitely generated ideal languages and synchronizing automata. In *WORDS 2013*, volume 8079 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2013.
- [17] J. M. Howie. *Automata and Languages*. Clarendon Press, 1991.
- [18] A. Mateescu and A. Salomaa. Many-valued truth functions, Černý’s conjecture and road coloring. *EATCS Bull*, 68:134–150, 1999.
- [19] V. Nekrashevych. Self-similar groups. *Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI*, 117, 2005.
- [20] M. Perles, M.O. Rabin, and E. Shamir. The theory of definite automata. *IEEE Trans. Electr. Comp*, 12(3):233–243, 1962.
- [21] E.V. Pribavkina and E. Rodaro. Finitely generated synchronizing automata. In *Language and Automata Theory and Applications*, volume 5457 of *Lecture Notes in Computer Science*, pages 672–683. Springer Berlin / Heidelberg, 2009.
- [22] E.V. Pribavkina and E. Rodaro. State complexity of code operators. *International Journal of Foundations of Computer Science*, 22(07):1669–1681, 2011.



- [23] E.V. Pribavkina and E. Rodaro. Synchronizing automata with finitely many minimal synchronizing words. *Information and Computation*, 209(3):568 – 579, 2011.
- [24] G. Rauzy. Suites à termes dans un alphabet fini. In *Séminaire de Théorie des Nombres de Bordeaux*, pages 25.01–25.16, 1982/83.
- [25] R. Reis and E. Rodaro. Regular ideal languages and synchronizing automata. In *WORDS 2013*, volume 8079 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2013.
- [26] I. K. Rystsov. Resetting words for decidable automata. *Cybernetics and Systems analysis*, 30, No. 6:807–811, 1994.
- [27] J. Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009.
- [28] S. Sidki. Automorphisms of one-rooted trees: growth, circuit structure and acyclicity. *J. Math. Sci. (New York)*, 100(1):1925–1943, 2000.
- [29] P. V.. Silva and B. Steinberg. On a class of automata groups generalizing lamplighter groups. *International Journal of Algebra and Computation*, 15(05n06):1213–1234, 2005.
- [30] G. Thierrin. Simple automata. *Kybernetika*, 6(5):343–350, 1970.
- [31] A.N. Trahtman. The road coloring problem. *Israel Journal of Mathematics*, 172(1):51–60, 2009.
- [32] M. V. Volkov. Synchronizing automata and the Černý conjecture. In *C. Martín-Vide, F. Otto, H. Fernau (eds.), Languages and Automata: Theory and Applications. LATA 2008, Lect. Notes Comp. Sci, Berlin, Springer*, 5196:11–27, 2008.