

**Citation for published version:**

Attila Egri-Nagy and Chrystopher L. Nehaniv, 'Symmetries of automata', *Algebra and Discrete Mathematics*, Vol. 19 (1): 48-57, March 2015.

**DOI:**

[Link to published paper in publisher's website](#)

**Document Version:**

This is the Published Version.

**Copyright and Reuse:**

© 2015 *Algebra and Discrete Mathematics*.

Content in the UH Research Archive is made available for personal research, educational, and non-commercial purposes only. Unless otherwise stated, all content is protected by copyright, and in the absence of an open license, permissions for further re-use should be sought from the publisher, the author, or other copyright holder.

**Enquiries**

If you believe this document infringes copyright, please contact Research & Scholarly Communications at [rsc@herts.ac.uk](mailto:rsc@herts.ac.uk)

# Symmetries of automata<sup>1</sup>

Attila Egri-Nagy and Chrystopher L. Nehaniv

Communicated by V. I. Sushchansky

**ABSTRACT.** For a given reachable automaton  $\mathcal{A}$ , we prove that the (state-) endomorphism monoid  $End(\mathcal{A})$  divides its characteristic monoid  $M(\mathcal{A})$ . Hence so does its (state-)automorphism group  $Aut(\mathcal{A})$ , and, for finite  $\mathcal{A}$ ,  $Aut(\mathcal{A})$  is a homomorphic image of a subgroup of the characteristic monoid. It follows that in the presence of a (state-) automorphism group  $G$  of  $\mathcal{A}$ , a finite automaton  $\mathcal{A}$  (and its transformation monoid) always has a decomposition as a divisor of the wreath product of two transformation semigroups whose semigroups are divisors of  $M(\mathcal{A})$ , namely the symmetry group  $G$  and the quotient of  $M(\mathcal{A})$  induced by the action of  $G$ . Moreover, this division is an embedding if  $M(\mathcal{A})$  is transitive on states of  $\mathcal{A}$ . For more general automorphisms, which may be non-trivial on input letters, counterexamples show that they need not be induced by any corresponding characteristic monoid element.

## 1. Preliminaries

An *automaton* is a 3-tuple  $\mathcal{A} = (X, \Sigma, \delta : X \times \Sigma \rightarrow X)$ , with state set  $X$ , input alphabet  $\Sigma$ , and state-transition function  $\delta$ , which given a state and input letter returns the next state. This action on  $X$  by symbols  $\Sigma$  naturally extends to words, i.e. sequences of symbols, by applying the symbols sequentially from left to right. An automaton is said to be *finite* if its state and input set are finite. Write  $x \cdot a$  for  $\delta(x, a)$  for  $x \in X, a \in \Sigma$ , and extend this inductively to words  $w \in \Sigma^*$  by  $x \cdot aw = (x \cdot a) \cdot w$ , where

---

<sup>1</sup>This work was in part supported by the EU FP6 Project OPAALS (Contract No IST-034824) and the FP7 EU Project BIOMICS (contract number CNECT-318202). This support is gratefully acknowledged.

**2010 MSC:** 20B25, 20E22, 20M20, 20M35, 68Q70.

the empty word acts as the identity. (NB:  $\Sigma^*$  is the free monoid on the alphabet  $\Sigma$ , consisting of finite words over  $\Sigma$  under concatenation, while  $\Sigma^+$  is the free semigroup consisting of non-empty words.) The *transition monoid* (or *characteristic monoid*) of  $\mathcal{A}$  is  $M(\mathcal{A}) = \Sigma^*/\equiv$ , where  $w \equiv w'$  if  $x \cdot w = x \cdot w'$  for all  $x \in X$ ,  $w, w' \in \Sigma^*$ . A state  $y$  is *reachable* (or *accessible*) from a state  $x$  if there exists a word  $w \in \Sigma^*$  such that  $x \cdot w = y$ . We say  $\mathcal{A}$  is *generated by* a state  $x_0$  if each state of  $\mathcal{A}$  can be reached from  $x_0$ . We then say  $x_0$  is an ‘initial state’ from which all other states are reachable. We sometimes then say that (all of)  $\mathcal{A}$  is ‘reachable’ from  $x_0$ . If each state of  $\mathcal{A}$  has this property, the automaton is said to be *strongly connected*. In this paper, we shall henceforth restrict attention to automata all of whose states are reachable from some initial state.

Let  $\mathcal{A} = (X, \Sigma, \delta)$  and  $\mathcal{B} = (Y, \Sigma', \delta')$  be automata with characteristic monoids  $M$  and  $M'$ . A pair of functions  $(\pi, \theta)$  with  $\pi : X \rightarrow Y$  and  $\theta : \Sigma \rightarrow \Sigma'$  is a *homomorphism of automata* if  $\pi(x \cdot s) = \pi(x) \cdot \theta(s)$  holds for all  $x \in X$  and  $s \in \Sigma$ . It is an *endomorphism* of  $\mathcal{A}$  if it maps  $\mathcal{A}$  to itself, i.e.  $\mathcal{B} = \mathcal{A}$ . If  $\pi$  and  $\theta$  are bijective, then it is an *isomorphism*. An endomorphism which is also an isomorphism is called an *automorphism*. A morphism of automata is called a *state-morphism* (state-endomorphism, state-automorphism, etc.) if  $\Sigma = \Sigma'$  and  $\theta$  is the identity function; that is, all input letters are fixed under the morphism. Let  $End^*(\mathcal{A})$  denote the monoid of endomorphisms of  $\mathcal{A}$ . Let  $Aut^*(\mathcal{A})$  denote the group of automorphisms of  $\mathcal{A}$ . Let  $End(\mathcal{A})$  and  $Aut(\mathcal{A})$  be their submonoid and subgroup, respectively, consisting just of state-morphisms.

A *transformation semigroup*  $(X, S)$  is a set  $X$  and subsemigroup  $S$  of the semigroup  $X^X$  of all functions from  $X$  under function composition as the associative operation. If  $S$  consists of permutations of  $X$ , then  $(X, S)$  is a *permutation group*. If  $s \in S$  and  $x \in X$ , we write  $x \cdot s$  for  $s(x)$ . The permutation group  $(G, G)$  is the right regular representation of  $G$ , where  $G$  acts on itself by right multiplication. For any automaton  $\mathcal{A} = (X, \Sigma, \delta)$  with have its *associated transformation semigroup*  $(X, S(\mathcal{A}))$  with  $x \cdot [w] = x \cdot w$  for all  $x \in X$  and  $[w] \in S(\mathcal{A}) = \Sigma^+/\equiv$ , and its *associated transformation monoid*  $(X, M(\mathcal{A}))$  with  $M(\mathcal{A}) = \Sigma^*/\equiv$ , which includes the identity mapping on  $X$ . Note that we can always regard a transformation semigroup or monoid  $(X, S)$  as an automaton with input letters  $S$  and transition function  $\delta(x, s) = s(x)$ .

The *wreath product*  $(X, S) \wr (Y, T)$  of transformation semigroups is the transformation semigroup  $(X \times Y, W)$  where

$$W = \{(s, f) : s \in S, f \in T^X\},$$

whose elements map  $X \times Y$  to itself as follows

$$(x, y) \cdot (s, f) = (x \cdot s, y \cdot f(x))$$

for  $x \in X, y \in Y$ . Here  $T^X$  is the semigroup of all functions  $f$  from  $X$  to  $T$  (under pointwise multiplication), and we have write  $y \cdot f(x)$  for the element  $f(x) \in T$  applied to  $y \in Y$ . The wreath product of permutation groups is again a permutation group. The wreath product construction is associative on the class of transformation semigroups (up to isomorphism). A morphism of transformation semigroups is defined in the obvious way. One transformation semigroup *divides* another,  $(X, S) \preceq (Y, T)$ , if  $(X, S)$  is a homomorphic image of a substructure of  $(Y, T)$ : precisely, there exists a subset  $Z \subseteq Y$  and a subsemigroup  $U \leq T$ , with a surjective function  $\theta_1 : Z \rightarrow Y$  and surjective homomorphism  $\theta_2 : U \rightarrow S$  such that  $\theta_1(z \cdot u) = \theta_1(z) \cdot \theta_2(u)$  for all  $z \in Z$  and  $u \in U$ . (NB:  $U$  is a subsemigroup of  $Y^Y$ , but not necessarily of  $Z^Z$ , as distinct elements of  $U$  might map  $Z$  to itself in the same way.) We write  $(X, S) \leq (Y, T)$  and call the division an *embedding* if  $\theta_1$  and  $\theta_2$  are injective. Similarly for semigroups, we write  $S \leq T$  if  $S$  embeds in  $T$ . We write  $S \preceq T$  and say  $S$  *divides*  $T$ , if  $S$  is a homomorphic image of some subsemigroup  $U$  of  $T$ , i.e.,  $S \leftarrow U \leq T$ . For more details on the basics of transformation semigroups and algebraic automata theory, see e.g. [KRT68, Eil76, DN05, Rho10].

## 2. State-homomorphisms of reachable automata

From now on we consider only state-homomorphisms and reachable automata unless otherwise stated. We show that a morphism is completely determined by how it acts at an initial state.

**Lemma 1.** *Let  $\pi : \mathcal{A} \rightarrow \mathcal{B}$  be a morphism of automata and suppose  $\mathcal{A}$  is reachable from some state  $x_0$ . Then  $\pi$  agrees with another such morphism  $\pi'$  at  $x_0$  if and only if  $\pi = \pi'$ .*

*Proof.* Let  $x$  be any state of  $\mathcal{A}$ . Then  $x = x_0 \cdot s$  for some  $s \in M(\mathcal{A})$ , whence

$$\pi(x) = \pi(x_0 \cdot s) = \pi(x_0) \cdot s = \pi'(x_0) \cdot s = \pi'(x_0 \cdot s) = \pi'(x). \quad \square$$

**Corollary 2.** *There can be at most  $|Y|$  distinct automata morphisms from  $\mathcal{A} = (X, \Sigma, \delta)$  to  $\mathcal{B} = (Y, \Sigma', \delta')$ .*

These results can be used to construct efficient algorithms for calculating all morphisms, further improving backtrack based search techniques for transformation semigroups [ABMN10].

**Proposition 3.** *The (state-)endomorphism monoid  $End(\mathcal{A})$  of an automaton  $\mathcal{A}$  is a homomorphic image of a certain submonoid  $J$  of the characteristic monoid of  $\mathcal{A}$ :  $M(\mathcal{A}) \geq J \xrightarrow{\alpha} End(\mathcal{A})$ .*

*Proof.* First define a certain submonoid of  $M = M(\mathcal{A})$  consisting of all elements of  $M$  that act like some endomorphism of  $\mathcal{A}$  at the generating state  $x_0$ :

$$J = \{s \in M : x_0 \cdot s = \pi(x_0) \text{ for some } \pi \in End(\mathcal{A})\}.$$

We call  $J$  the *Fleck submonoid* of the characteristic monoid  $M(\mathcal{A})$ . To see that this is really a submonoid, observe (1) that corresponding to identity endomorphism the identity element of  $M(\mathcal{A})$  is in  $J$ , and (2)  $J$  is closed under multiplication: Take  $s_1, s_2 \in J$ . By definition, for  $i \in \{1, 2\}$ , we have some  $\pi_i \in End(\mathcal{A})$  such that  $x_0 \cdot s_i = \pi_i(x_0)$ . Now

$$\begin{aligned} x_0 \cdot s_1 s_2 &= (x_0 \cdot s_1) \cdot s_2 \\ &= \pi_1(x_0) \cdot s_2 \text{ by choice of } \pi_1 \\ &= \pi_1(x_0 \cdot s_2) \text{ since } \pi_1 \text{ is an endomorphism} \\ &= \pi_1(\pi_2(x_0)) \text{ by choice of } \pi_2 \end{aligned}$$

Therefore, since  $\pi_1 \pi_2 \in End(\mathcal{A})$ , we have that  $s_1 s_2 \in J$ . Note: the action of the characteristic monoid is on the right of states, while the action of endomorphisms or automorphisms is on the left of states.

Now define  $\alpha : J \rightarrow End(\mathcal{A})$  by  $\alpha(s) = \pi$  where  $x_0 \cdot s = \pi(x_0)$ , with  $\pi \in End(\mathcal{A})$ . (NB:  $\pi$  exists by definition of  $J$ .) The function  $\alpha$  is well-defined by Lemma 1.

Moreover, the above calculation shows that  $\alpha(s_1) = \pi_1$  and  $\alpha(s_2) = \pi_2$  implies that  $\alpha(s_1 s_2) = \pi_1 \pi_2$ . So since  $\alpha(1_{M(\mathcal{A})}) =$  the identity morphism,  $\alpha$  is a monoid homomorphism.

Finally, given  $\pi \in End(\mathcal{A})$  consider the state  $\pi(x_0)$ . By reachability, there is some  $s \in S$  with  $x_0 \cdot s = \pi(x_0)$ , whence  $s \in J$  and  $\alpha(s) = \pi$ . This proves  $\alpha$  is surjective.  $\square$

**Proposition 4.** *The (state-)automorphism group  $Aut(\mathcal{A})$  of an automaton  $\mathcal{A}$  is a divisor of  $M(\mathcal{A})$ , a homomorphic image of a submonoid of the characteristic monoid of  $M(\mathcal{A})$ .*

*Proof.* The proof of this is exactly like that of Proposition 3 except that one replaces  $End(\mathcal{A})$  by  $Aut(\mathcal{A})$  the word ‘endomorphism’ by ‘automorphism’ throughout. Alternatively, this is immediate from the proposition since  $Aut(\mathcal{A})$  is the group of units of  $End(\mathcal{A})$ .  $\square$

The following lemma is well-known (e.g. Proposition 1.11. in [DN05]).

**Lemma 5.** *Let  $S$  be a finite semigroup.*

- 1) *If  $S$  maps homomorphically onto a group  $G$ , then there is a subgroup  $\tilde{G}$  of  $S$  mapping onto  $G$ .*
- 2) *If a group  $G$  divides  $S$ , then  $G$  divides a subgroup of  $S$ .*

*Proof.* Suppose  $\varphi : S \rightarrow G$ . Then the collection of subsemigroups of  $S$  mapping onto  $G$  under  $\varphi$  is obviously non-empty. Let  $\tilde{G}$  be a member of this collection minimal under inclusion. (It must exist by finiteness.) Then  $\tilde{G}\tilde{G}$  is a subsemigroup with the same property and is contained in  $\tilde{G}$ . Whence, by minimality,  $\tilde{G}^2 = \tilde{G}$ . By finiteness,  $\tilde{G}$  contains an idempotent  $e^2 = e$  since any finite semigroup does. By minimality  $e\tilde{G}e = \tilde{G}$ , and  $e$  is thus a left- and right-identity for all elements of  $\tilde{G}$ , thus  $\tilde{G}$  is a monoid. To show that inverses exist take  $t \in e\tilde{G}e$ , and  $e'$  be the unique idempotent power of  $t$  (which exists again by finiteness). Then with same reasoning  $e\tilde{G}e = e'\tilde{G}e'$ , for which both  $e'$  and  $e$  are clearly left- and right- identity elements, and so  $e = ee' = e'$ , therefore  $e = e'$ . Thus for each  $t$  there exists  $n > 1$  such that  $t^n = e$ , so  $tt^{n-1} = t^{n-1}t = e$ . So  $\tilde{G}$  is a group mapping homomorphically onto  $G$ . The second assertion is a trivial consequence of the first.  $\square$

**Corollary 6.** *The (state-)automorphism group  $Aut(\mathcal{A})$  of a finite automaton  $\mathcal{A}$  is a homomorphic image of a subgroup of its characteristic monoid  $M(\mathcal{A})$ .*

*Proof.* This follows from the Proposition 4 by Lemma 5 and finiteness of  $M(\mathcal{A})$ .  $\square$

**Remark.** Propositions 3 and 4 and Corollary 6 are due to the second named author based on streamlining and generalizing the methods of [Fle65].

Corollary 6 is the generalization of the result of Fleck [Fle65, Theorem 2.4] from strongly connected automata to those each of whose states are accessible from some initial state. That the result for reachable automata is not a vacuous generalization can be clearly seen by many examples of non-trivial state-automorphisms of automata which are not strongly connected.

**Examples 7.** Reachable automata  $\mathcal{A}_1$ ,  $\mathcal{A}_2$ , and  $\mathcal{A}_3$  with state set  $X = \{1, 2, 3, 4\}$ , input symbols  $\Sigma = \{a, b\}$ , and initial state 1: Each automorphism group  $\text{Aut}(\mathcal{A}_i) \cong \mathbb{Z}_2$  for  $1 \leq i \leq 3$ , and it is also true that  $\mathbb{Z}_2 \leq M(\mathcal{A}_i)$ , as  $a$  is a transposition. These automata are not strongly connected, as from states  $\{3, 4\}$  there is no way to states  $\{1, 2\}$ . All automorphisms of these automata are state-automorphisms.

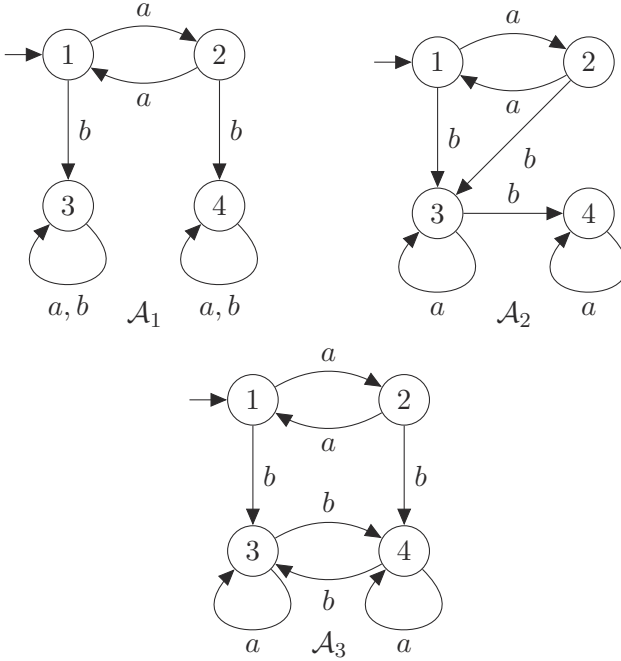


FIGURE 1. Reachable, but not strongly connected automata with automorphism group  $\mathbb{Z}_2$ .

### 3. Internal versus external automorphisms

#### 3.1. Internal symmetries

Now we can answer the question ‘*What is the relation between the automorphism group of the automata and some subgroups of its characteristic monoid?*’ The results of the previous section can be interpreted as saying that all state-automorphisms are ‘internal’, i.e. arise through a homomorphism from some group element inside the characteristic monoid. Similarly, Proposition 3 can be interpreted as saying that all state-endomorphisms are ‘internal’, i.e. arise from some monoid element inside the characteristic monoid.



There is also a very fine distinction amongst internal automorphisms. Being internal does not necessarily mean that an automorphism can be realized by directly by the action of an element of the characteristic semigroup on the states of  $\mathcal{A}$ , but it is always realized as the image of an element of the Fleck monoid under the map  $\alpha$  defined previously.

**Examples 8.** Let  $\mathcal{A}_1$ ,  $\mathcal{A}_2$ , and  $\mathcal{A}_3$  be the automata from the Examples 7. Then  $M(\mathcal{A}_1)$  is

$$\{a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, b = ba = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 3 & 4 \end{pmatrix}, ab = b^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 3 & 4 \end{pmatrix}, id = a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}\},$$

and  $Aut(\mathcal{A}_1)$  is the order 2 cyclic group  $\mathbb{Z}_2$  generated by  $(1, 2)(3, 4)$  ( $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$  written in transformation notation), which is not an element of the characteristic monoid. Similarly,  $Aut(\mathcal{A}_3) = \langle (1, 2)(3, 4) \rangle \cong \mathbb{Z}_2$ , and no letter or word of  $\mathcal{A}_3$  realizes this permutation. However,  $Aut(\mathcal{A}_2)$  is also  $\mathbb{Z}_2$  but generated by  $(1, 2)$  which is  $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ , a transformation corresponding to an input symbol of  $\mathcal{A}_2$ . Although the automorphism groups are internal in all three cases, the automorphisms are realized by input words for  $\mathcal{A}_2$ , but not for  $\mathcal{A}_1$  or  $\mathcal{A}_3$ . Nevertheless, in each case  $Aut(\mathcal{A}_i) = Aut^*(\mathcal{A}_i) = \langle \alpha(a) \rangle$ , where the action of the one-letter word  $a$  at state 1 determines the generator (as in Proposition 3).

### 3.2. External symmetries

There exist automorphisms of automata which are not state-automorphisms. An automorphism or endomorphism which is not the identity on inputs cannot be realized by applying words to states since these have no effect on input letters. These automorphisms are in a sense ‘external’.

**Example 9.** The flip-flop is a 2-state identity-reset automaton.

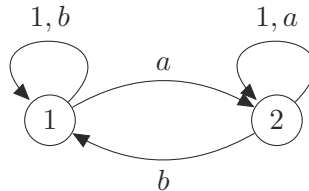


FIGURE 2. Flip-flop automaton  $\mathcal{F}$  with two states, and three input letters: the identity map and two resets.



The automorphism  $(\pi, \theta)$  with  $\pi(1) = 2, \pi(2) = 1, \theta(a) = b, \theta(b) = a,$  and  $\theta(1) = 1$  generates the automorphism group  $Aut^*(\mathcal{F}) = \mathbb{Z}_2$ , while  $M(\mathcal{F})$  is aperiodic (has no nontrivial subgroups).

**Caveat:** The group of general automorphisms need not divide the characteristic monoid of the automaton. Here in Example 9,  $Aut^*(\mathcal{F}) \not\leq M(\mathcal{F})$ . A symmetry of the diagram of the automaton does not entail the existence of non-trivial subgroups in the characteristic monoid of the automaton, unless these symmetries are internal automorphisms (i.e., the identity on input letters).

## 4. Symmetries and wreath product

The presence of a non-trivial symmetry group of state-automorphisms permits better understanding of an automaton's structure. Formally, the 'better understanding' corresponds to a wreath product decomposition.

### 4.1. Quotient of an automaton by a group of symmetries

Let  $\mathcal{A} = (X, \Sigma, \delta)$  be an automaton and let  $G$  be a group of symmetries (via state-automorphisms) of  $\mathcal{A}$ . An equivalence relation on  $X$  is given by  $x \equiv x'$  iff there exists a symmetry  $\pi \in G, \pi(x) = x'$ . Denote by  $[x]$  the set of all states  $x' \in X$  equivalent to  $x$  under the action of  $G$ . Let  $X^G = \{[x] : x \in X\}$  be the set of orbits under the action of  $G$ , i.e., the partition blocks of this equivalence relation. Let  $[x] \cdot a = [x \cdot a]$  for each  $[x] \in X^G$  and  $a \in \Sigma$ . Since  $x' = \pi(x)$  implies  $x' \cdot a = \pi(x) \cdot a = \pi(x \cdot a)$ , so  $x' \cdot a \in [x \cdot a]$ , the action of the inputs is well-defined on  $X^G$ . We write  $\Sigma^G$  for set of the induced mappings by inputs  $\Sigma$  on the quotient set  $X^G$ . Thus the *quotient automaton*  $\mathcal{A}^G = (X^G, \Sigma^G, \delta^G)$  is well-defined for any group of state-automorphism symmetries  $G$ , and its characteristic monoid  $M(\mathcal{A}^G)$  is clearly a quotient of  $M(\mathcal{A})$ .

### 4.2. Wreath product decomposition under symmetries

The following theorem generalizes [Rho10, Fact 4.7] or the result of [Neh96, Sec. 4.2].<sup>2</sup>

**Theorem 10.** *Let  $\mathcal{A} = (X, \Sigma, \delta)$  be an automaton and let  $G \leq Aut(\mathcal{A})$  be any group of symmetries of  $\mathcal{A}$  consisting of state-automorphisms. Then*

<sup>2</sup>These references treat only the transitive case, and do not include the result that the automorphism group divides the original monoid.

- 1)  $\mathcal{A} \leq (X, M(\mathcal{A})) \preceq (X^G, M(\mathcal{A}^G)) \wr (G, G)$
- 2) If  $M(\mathcal{A})$  acts transitively on  $X$ , then this division is an embedding.
- 3) The group  $G$  divides  $M(\mathcal{A})$  and, if  $\mathcal{A}$  is a finite automaton, then  $G$  is a homomorphic image of a subgroup of  $M(\mathcal{A})$ .

In particular, we have the new result that the algebraic components of the decomposition,  $G$  and  $M(\mathcal{A}^G)$ , both divide  $M(\mathcal{A})$ . Hence internal symmetries result in a decomposition into ‘pieces’ existing in the original characteristic monoid of  $\mathcal{A}$ .

*Proof.* For each  $[x] \in X^G$ , choose a representative  $\overline{[x]} \in [x]$ . Then if  $x \in [x]$ , there exists  $\pi$  with  $\pi(\overline{[x]}) = x$ . Now each  $x$  in  $X$  is then coordinatized as  $([x], \pi)$ , and we have  $\varphi([x], \pi) = \pi(\overline{[x]}) = x$ . For  $s \in \Sigma$ , we lift  $s$  to  $\tilde{s}$  with  $([x], \pi) \cdot \tilde{s} = ([x] \cdot s, \pi \cdot \pi')$ , where  $\pi' \in G$  is chosen such that  $\pi'(\overline{[x] \cdot s}) = \overline{[x]} \cdot s$ . Then  $\tilde{s}$  has component action in  $M(\mathcal{A}^G)$  at the top level, and component action given by  $\pi' \in G$ , with  $\pi'$  depending only on  $[x]$  and  $s$ . It follows that

$$\begin{aligned} \varphi(([x], \pi) \cdot \tilde{s}) &= \varphi([x \cdot s], \pi\pi') = \pi\pi'(\overline{[x \cdot s]}) \\ &= \pi(\pi'(\overline{[x \cdot s]})) = \pi(\overline{[x]} \cdot s) \\ &= \pi(\overline{[x]}) \cdot s = x \cdot s \\ &= \varphi([x], \pi) \cdot s, \end{aligned}$$

establishing (1). (2) Suppose  $M(\mathcal{A})$  acts transitively on  $X$ . Then we show  $G$  acts regularly on  $X$ . For if  $x \neq x' \in X$ , there exist  $s_1, \dots, s_k \in M(\mathcal{A})$  with  $x \cdot s_1 \dots s_k = x'$ . Then,  $\pi(x') = \pi(x \cdot s_1 \dots s_k) = \pi(x) \cdot s_1 \dots s_n$ . So if  $\pi \in G$  fixes any  $x \in X$ , then  $\pi$  fixes all  $x' \in X$  as well. Thus, if  $\pi_1(\overline{[x]}) = x$  and  $\pi_2(\overline{[x]}) = x$  for any  $\pi_1, \pi_2 \in G$ , then  $\pi_2^{-1}\pi_1(\overline{[x]}) = \overline{[x]}$ . Therefore  $\pi_2^{-1}\pi_1$  fixes all  $x' \in X$ , and so  $\pi_1 = \pi_2$ . Thus the coordinatization of  $x$  as  $([x], \pi)$  is unique. This shows state embedding. Next we show semigroup embedding: in the lift  $\tilde{s}$  of  $s$ ,  $\pi' : X^G \rightarrow G$  is uniquely determined for each  $[x]$  by the condition that  $\pi'(\overline{[x \cdot s]}) = \overline{[x]} \cdot s$ , since another  $\pi_2$  with this property would equal  $\pi'$  since  $\pi_2^{-1}\pi'$  would fix  $[x \cdot s]$  and hence all of  $X$ . Thus lifting is injective. It follows also that it is a homomorphism of transformation semigroups. (3) follows from Proposition 4 and Corollary 6.  $\square$

Theorem 10 says non-trivial state-automorphisms entail a non-trivial wreath product decomposition using only semigroups dividing the characteristic monoid. In contrast, for non-state-automorphisms, the situation is different: in the flip-flop automaton (Example 9), there is an order 2

automorphism but no corresponding wreath product decomposition with the group generated by this external symmetry as a factor, and moreover this group does not divide the characteristic monoid.

### References

- [ABMN10] J. Araújo, P.V. Bünaú, J.D. Mitchell, and M. Neunhöffer. Computing automorphisms of semigroups. *Journal of Symbolic Computation*, 45(3):373–392, 2010.
- [DN05] Pál Dömösi and Chrystopher L. Nehaniv. *Algebraic Theory of Finite Automata Networks: An Introduction*, volume 11 of *SIAM Series on Discrete Mathematics and Applications*. Society for Industrial and Applied Mathematics, 2005.
- [Eil76] Samuel Eilenberg. *Automata, Languages and Machines*, volume B. Academic Press, 1976.
- [Fle65] A. C. Fleck. On the automorphism group of an automaton. *Journal of the Association for Computing Machinery*, 12(4):566–569, 1965.
- [KRT68] Kenneth Krohn, John L. Rhodes, and Bret R. Tilson. The prime decomposition theorem of the algebraic theory of machines. In Michael A. Arbib, editor, *Algebraic Theory of Machines, Languages, and Semigroups*, chapter 5, pages 81–125. Academic Press, 1968.
- [Neh96] Chrystopher L. Nehaniv. Algebra and formal models of understanding. In Masami Ito, editor, *Semigroups, Formal Languages and Computer Systems*, volume 960, pages 145–154. Kyoto Research Institute for Mathematics Sciences, RIMS Kokyuroku, August 1996.
- [Rho10] John Rhodes. *Applications of Automata Theory and Algebra via the Mathematical Theory of Complexity to Biology, Physics, Psychology, Philosophy, and Games*. World Scientific Press, 2010. Foreword by Morris W. Hirsch, edited by Chrystopher L. Nehaniv (Unpublished version: University of California at Berkeley, Mathematics Library, circa 1971).

### CONTACT INFORMATION

- |                               |  |
|-------------------------------|--|
| <b>Attila Egri-Nagy</b>       | Centre for Research in Mathematics, SCEM,<br>University of Western Sydney (Parramatta Campus)<br>Locked Bag 1797, Penrith, NSW 2751, Australia<br><i>E-Mail(s)</i> : <a href="mailto:a.egri-nagy@uws.edu.au">a.egri-nagy@uws.edu.au</a><br><i>Web-page</i> : <a href="http://www.egri-nagy.hu">www.egri-nagy.hu</a>  |
| <b>Chrystopher L. Nehaniv</b> | Centre for Computer Science & Informatics Research,<br>University of Hertfordshire, College Lane, Hatfield,<br>Herts AL10 9AB, United Kingdom<br><i>E-Mail(s)</i> : <a href="mailto:C.L.Nehaniv@herts.ac.uk">C.L.Nehaniv@herts.ac.uk</a><br><i>Web-page</i> : <a href="http://homepages.stca.herts.ac.uk/~nehaniv">homepages.stca.herts.ac.uk/~nehaniv</a> |

Received by the editors: 02.05.2014  
and in final form 12.01.2015.