

A Proof of the Krohn-Rhodes Decomposition Theorem

Z. Ésik*

A. József University
Department of Computer Science
Szeged, Hungary
esik@inf.u-szeged.hu

Abstract

We give a new proof of one part of the Krohn-Rhodes decomposition theorem for automata.

1 Introduction

The Krohn-Rhodes Decomposition Theorem [8] has a number of formulations in terms of automata, transformation semigroups, or semigroups, see [1, 6, 2, 9, 7, 5, 10], or [3], for an extension. The aim of this paper is to give a simple proof of the hard part of the theorem involving automata: Each finite automaton \mathbf{A} is the homomorphic image of a subautomaton of a (generalized) cascade composition of automata $\mathbf{A}_1, \dots, \mathbf{A}_k$, where each \mathbf{A}_i is either the two-state identity-reset automaton \mathbf{U} or a group-type automaton $\mathbf{Aut}(G)$ corresponding to a simple group G which divides the semigroup of \mathbf{A} . In addition to the well-known decomposition of permutation-reset automata, the new argument uses a single construction and is based on the following observation. Given the automaton \mathbf{A} , there is a sequence

$$\mathbf{B}_0, \mathbf{B}_1, \dots, \mathbf{B}_m$$

of finite automata such that \mathbf{B}_0 is trivial, \mathbf{B}_m is the automaton \mathbf{A} , and for each integer $1 \leq i \leq m$, either there is a surjective simple regular \mathcal{G} -homomorphism $A_i \rightarrow A_{i-1}$, or there is a surjective simple regular \mathcal{G} -homomorphism $A_{i-1} \rightarrow A_i$. Here \mathcal{G} denotes the class of simple groups dividing the semigroup of \mathbf{A} , and a homomorphism $\mathbf{B} \rightarrow \mathbf{C}$ is termed a simple regular \mathcal{G} -homomorphism if its kernel ρ satisfies the following conditions.

- The non-singleton equivalence classes of ρ , or ρ -blocks, for short, have equal cardinality.
- If C and D are (non-singleton) ρ -blocks and u is an input word of \mathbf{B} with $Cu \subseteq D$, then either $Cu = D$ or Cu is a singleton set.
- For any two non-singleton ρ -blocks C and D there is a word u with $Cu = D$.
- If C is a ρ -block and G is the group of all bijections $C \rightarrow C$ induced by an input word, then any simple group divisor of G belongs to \mathcal{G} .

*Partially supported by the National Foundation for Scientific Research of Hungary under grant No. T7383 and by the Japan Society for the Promotion of Science.

We then show that if $h : \mathbf{B} \rightarrow \mathbf{C}$ is a surjective simple regular \mathcal{G} -homomorphism with kernel ρ , then \mathbf{B} is isomorphic to a subautomaton of a cascade composition of \mathbf{C} and a permutation-reset automaton \mathbf{D} such that each simple group divisor of the semigroup of \mathbf{D} is in \mathcal{G} .

The proof presented here has been used in [4] to show that the Conway axioms and an identity associated with each finite (simple) group provide a complete axiomatization of iteration theories.

2 Preliminaries

2.1 Automata

Suppose that X is a finite nonempty set. We denote by X^* the free monoid of all words over X including the empty word λ . We set $X^+ = X^* - \{\lambda\}$, so that X^+ is the free semigroup of nonempty words over X .

An X -automaton \mathbf{A} is a system (A, X, δ) consisting of the finite nonempty set A of states, the finite nonempty set X of input letters, and the transition function $\delta : A \times X \rightarrow A$ which can be extended to a function $A \times X^* \rightarrow A$ in the usual way. When $a \in A$ and $u \in X^*$, we will usually write au for $\delta(a, u)$, in particular when \mathbf{A} is understood. Suppose that $C \subseteq A$ and $u \in X^*$. We define $Cu = \{cu : c \in C\}$.

Homomorphisms, congruences and subautomata are defined in the usual way.

2.2 Cascade Composition

Suppose that $\mathbf{A}_i = (A_i, X, \delta_i)$ are given automata, for $i \in [k] = \{1, \dots, k\}$, $k \geq 0$. Let X denote a finite nonempty nonempty set, and for each $i \in [k]$, let φ_i be a function

$$A_1 \times A_2 \times \dots \times A_{i-1} \times X \rightarrow X_i.$$

The *generalized cascade composition* of the \mathbf{A}_i determined by the set X and functions φ_i is defined to be the automaton $\mathbf{A} = (A, X, \delta)$, where A is the set $A_1 \times \dots \times A_k$, and for each $(a_1, \dots, a_k) \in A$ and $x \in X$,

$$(a_1, \dots, a_k)x = (a_1x_1, \dots, a_kx_k)$$

with

$$x_i = \varphi_i(a_1, \dots, a_{i-1}, x),$$

all $i \in [k]$.

When $X = X_1 = \dots = X_k$ and $\varphi_i(a_1, \dots, a_{i-1}, x) = x$, for each $x \in X$, $a_1 \in A_1, \dots, a_{i-1} \in A_{i-1}$ and $i \in [k]$, the cascade composition becomes the *direct product* $\mathbf{A}_1 \times \dots \times \mathbf{A}_k$.

In the sequel, we will never use a generalized cascade composition of more than two automata at a time. Accordingly, we will write

$$\mathbf{A}_1 \times \mathbf{A}_2(X, \varphi_1, \varphi_2) \tag{1}$$

to denote the generalized cascade composition of \mathbf{A}_1 and \mathbf{A}_2 determined by the set X and functions φ_i , $i = 1, 2$. When X is the input set of the automaton \mathbf{A}_1 and φ_1 is the identity function $X \rightarrow X$, we call the automaton (1) the *cascade composition* of \mathbf{A}_1 and \mathbf{A}_2 determined by the function φ_2 . Denoting $\varphi = \varphi_2$, we will write

$$\mathbf{A}_1 \times_{\varphi} \mathbf{A}_2 \tag{2}$$

for short.

Suppose that $\mathbf{A} = (A, X, \delta)$ and $\mathbf{B} = (A, Y, \delta')$ are given finite automata with identical state sets. We say that \mathbf{B} is a *renaming* of \mathbf{A} if there is a function $\varphi : Y \rightarrow X$ such that

$$\delta'(a, y) = \delta(a, y\varphi),$$

for all $a \in A$ and $y \in Y$.

Suppose that K is a class of automata. We define:

- $\mathbf{S}(K)$: all subautomata of automata in K ;
- $\mathbf{N}(K)$: all renamings of automata in K ;
- $\mathbf{H}(K)$: all homomorphic images of automata in K ;
- $\mathbf{I}(K)$: all isomorphic images of automata in K ;
- $\mathbf{P}_c(K)$: all generalized cascade compositions of automata in K .

It is known that for any nonempty class K of automata, $\mathbf{V}_c(K) = \mathbf{HSP}_c(K)$ is the smallest class containing K and closed under the operators \mathbf{H} , \mathbf{S} and \mathbf{P}_c , and also the smallest class containing K and closed under the operators \mathbf{H} , \mathbf{S} , \mathbf{N} and the cascade composition (2). See [5].

2.3 Semigroups

Except for free semigroups X^+ and free monoids X^* , each semigroup will be assumed to be finite. We will use standard terminology. A submonoid of a semigroup is a subsemigroup which is a monoid. Similarly, a subgroup of a semigroup is a subsemigroup which is a group. Suppose that S and T are semigroups. We say that S *divides* T , denoted $S|T$, if S is a homomorphic image (or quotient) of a subsemigroup of T . It is known that this relation is transitive, see, e.g., [2, 9]. A proof of the following lemma can be found, e.g., in [5].

LEMMA 2.1 *Suppose that $S|T$ and that S is a monoid (group, respectively). Then there is a submonoid T' (subgroup, respectively) of T such that S is a quotient of T' .*

Suppose that $\mathbf{A} = (A, X, \delta)$ is an automaton. Each word $u \in X^*$ induces a function

$$\begin{aligned} u^{\mathbf{A}} : A &\rightarrow A \\ a &\mapsto au. \end{aligned}$$

The functions $u^{\mathbf{A}}$, $u \in X^*$, form a monoid denoted $M(\mathbf{A})$ whose unit is the identity function $\lambda^{\mathbf{A}} : A \rightarrow A$. We will denote by $S(\mathbf{A})$ the subsemigroup of $M(\mathbf{A})$ determined by the functions $u^{\mathbf{A}}$ induced by the nonempty words $u \in X^+$. The group $G(\mathbf{A})$ consists of those functions in $M(\mathbf{A})$ which are permutations.

We may generalize the above concepts. Suppose that C and D are two nonempty subsets of A . We define:

- $M_{\mathbf{A}}(C, D)$: all functions $f : C \rightarrow D$ such that there exists a word $u \in X^*$ with $u^{\mathbf{A}}|_C = f$, where $u^{\mathbf{A}}|_C$ denotes the restriction of $u^{\mathbf{A}}$ to C ;
- $S_{\mathbf{A}}(C, D)$: all functions $f : C \rightarrow D$ such that there exists a word $u \in X^+$ with $u^{\mathbf{A}}|_C = f$;

- $G_{\mathbf{A}}(C, D)$: the bijections in $M_{\mathbf{A}}(C, D)$.

Of course, if $G_{\mathbf{A}}(C, D) \neq \emptyset$, then $|C| = |D|$, i.e., the sets C and D have equal number of elements. We write $M_{\mathbf{A}}(C)$ for $M_{\mathbf{A}}(C, C)$. Note that $M_{\mathbf{A}}(C)$ is a monoid. We define the semigroup $S_{\mathbf{A}}(C)$ and the group $G_{\mathbf{A}}(C)$ in a similar way. Note that $S_{\mathbf{A}}(C)$ may be empty. For a proof of the following lemma, see [5].

LEMMA 2.2 *Suppose that G is a subgroup of $M_{\mathbf{A}}(C)$ or a subgroup of $S_{\mathbf{A}}(C)$. Then there is a nonempty set $D \subseteq C$ such that G is isomorphic to a subgroup of $G_{\mathbf{A}}(D)$. In particular, if G is a subgroup of $M(\mathbf{A})$ or a subgroup $S(\mathbf{A})$, then there is a set $D \subseteq A$ such that G is isomorphic to a subgroup of $G_{\mathbf{A}}(D)$.*

2.4 Permutation-Reset Automata

An X -automaton is a *permutation automaton* if each function $x^{\mathbf{A}}$, $x \in X$, is a permutation. It then follows that the functions $u^{\mathbf{A}}$, $u \in X^*$, are also permutations, so that $M(\mathbf{A}) = S(\mathbf{A}) = G(\mathbf{A})$. Conversely, if $S(\mathbf{A}) = G(\mathbf{A})$, or if $M(\mathbf{A}) = G(\mathbf{A})$, then \mathbf{A} is a permutation automaton. When G is a group, the system $\mathbf{Aut}(G) = (G, G, \delta)$ with $\delta(g, h) = gh$, the product of the group elements g and h , for all $g, h \in G$, is a permutation automaton.

An automaton $\mathbf{A} = (A, X, \delta)$ is a *permutation-reset automaton* if each function $x^{\mathbf{A}}$, $x \in X$, is either a permutation or a constant map. It then follows that each function $u^{\mathbf{A}}$ for $u \in X^*$ is also either a permutation or a constant map. For example, the automaton $\mathbf{U} = ([2], \{x_0, x_1, x_2\}, \delta)$ is a permutation-reset automaton, where $ix_0 = i$ and $ix_j = j$, for $i, j = 1, 2$.

For any automaton \mathbf{A} , let $\mathcal{G}(\mathbf{A})$ denote the collection of simple groups G with $G|M(\mathbf{A})$. (Note that for any group G , $G|M(\mathbf{A})$ iff $G|S(\mathbf{A})$.) Moreover, we define $\mathcal{K}_g(\mathbf{A}) = \{\mathbf{Aut}(G) : G \in \mathcal{G}(\mathbf{A})\}$ and $\mathcal{K}(\mathbf{A}) = \mathcal{K}_g(\mathbf{A}) \cup \{\mathbf{U}\}$.

LEMMA 2.3 *Suppose that \mathbf{A} is a permutation-reset automaton. Then*

$$\mathbf{A} \in \mathbf{V}_c(\mathcal{K}(\mathbf{A})).$$

If \mathbf{A} is a permutation automaton such that at least one letter induces a nontrivial permutation, then

$$\mathbf{A} \in \mathbf{V}_c(\mathcal{K}_g(\mathbf{A})).$$

For a proof of Lemma 2.3, see [5], or [9].

3 The Krohn-Rhodes Decomposition Theorem

The Krohn-Rhodes Decomposition Theorem consists of two parts, Theorem 3.1 and Theorem 3.2. Let U denote a semigroup isomorphic to $M(\mathbf{U}) = S(\mathbf{U})$. (The automaton \mathbf{U} was defined above).

THEOREM 3.1 *Suppose that S is either a semigroup dividing U or a simple group. Let \mathbf{A} be an automaton and K a nonempty class of automata with $\mathbf{A} \in \mathbf{V}_c(K)$. If $S|S(\mathbf{A})$ then there is an automaton $\mathbf{B} \in K$ with $S|S(\mathbf{B})$. If $S|M(\mathbf{A})$ then there is an automaton $\mathbf{B} \in K$ with $S|M(\mathbf{B})$.*

THEOREM 3.2 *For each automaton \mathbf{A} ,*

$$\mathbf{A} \in \mathbf{V}_c(\mathcal{K}(\mathbf{A})).$$

The class $\mathcal{K}(\mathbf{A})$ was defined above.

The rest of the paper is devoted to proving Theorem 3.2. In our argument, we will make use of Lemma 2.3, which is a particular instance of Theorem 3.2.

4 Congruences

In this section we assume that \mathcal{G} is a class of simple groups closed under division. Thus, if G and H are simple groups with $G|H$ and $H \in \mathcal{G}$, then G is also in \mathcal{G} . The class $\overline{\mathcal{G}}$ consists of the groups whose simple group divisors are in \mathcal{G} . Note that $\overline{\mathcal{G}}$ is closed under the formation of subgroups and homomorphic images. It follows from Theorem 3.1 that $\overline{\mathcal{G}}$ is also closed under semidirect product and thus under direct product.

DEFINITION 4.1 *Suppose that $\mathbf{A} = (A, X, \delta)$ is an automaton and that $\rho \subseteq A \times A$ is a congruence relation. We call ρ*

- **simple**, if $|C| = |D|$ holds for any two non-singleton ρ -blocks $C, D \in A/\rho$, and if each member of $M_{\mathbf{A}}(C, D)$ is either a bijection or a constant map;
- **regular**, if for each non-singleton ρ -block C , the smallest congruence relation which collapses the states in C is the relation ρ itself;
- **A \mathcal{G} -congruence**, if for each ρ -block C , each subgroup of $M_{\mathbf{A}}(C)$ is in $\overline{\mathcal{G}}$.

Note that ρ is a \mathcal{G} -congruence iff for each ρ -block C , each subgroup of $S_{\mathbf{A}}(C)$ is in $\overline{\mathcal{G}}$, i.e., when $G \in \mathcal{G}$ holds for the simple groups G dividing $S_{\mathbf{A}}(C)$ or $M_{\mathbf{A}}(C)$. Moreover, a simple congruence ρ is a \mathcal{G} -congruence iff $G_{\mathbf{A}}(C) \in \overline{\mathcal{G}}$, for each (non-singleton) ρ -block C . This follows by noting that when ρ is simple, each nontrivial subgroup of $M_{\mathbf{A}}(C)$ is a subgroup of $G_{\mathbf{A}}(C)$.

DEFINITION 4.2 *Suppose that \mathbf{A} and \mathbf{B} are X -automata and that h is a homomorphism $\mathbf{A} \rightarrow \mathbf{B}$. We call h a simple, regular, or a \mathcal{G} -homomorphism, if $\ker h$, the kernel of h has the appropriate property.*

When \mathcal{G} is empty, a \mathcal{G} -homomorphism will be termed *aperiodic*.

LEMMA 4.3 *Suppose that $\mathbf{A}_1, \mathbf{A}_2$ and \mathbf{A}_3 are X -automata with homomorphisms $h_1 : \mathbf{A}_1 \rightarrow \mathbf{A}_2$ and $\mathbf{A}_2 \rightarrow \mathbf{A}_3$. If h_1 is surjective and if*

$$h = \mathbf{A}_1 \xrightarrow{h_1} \mathbf{A}_2 \xrightarrow{h_2} \mathbf{A}_3$$

is a \mathcal{G} -homomorphism, then so are h_1 and h_2 .

Proof. Denote $\rho_i = \ker h_i$, $i = 1, 2$, and $\rho = \ker h$. Each ρ_1 -block C is included in some ρ -block D . The functions $g \in M_{\mathbf{A}_1}(D)$ with $Cg \subseteq C$ form a submonoid M of $M_{\mathbf{A}_1}(D)$, and the map $g \mapsto g|_C$, $g \in M$ is a surjective homomorphism $M \rightarrow M_{\mathbf{A}_1}(C)$. Thus $M_{\mathbf{A}_1}(C)|M_{\mathbf{A}_1}(D)$, so that any divisor of $M_{\mathbf{A}_1}(C)$ divides $M_{\mathbf{A}_1}(D)$. Since ρ is a \mathcal{G} -congruence, it follows that ρ_1 is also a \mathcal{G} -congruence, hence h_1 is a \mathcal{G} -homomorphism.

Suppose now that C is a ρ_2 -block. Define $D = h_1^{-1}(C)$, so that D is a ρ -block. Since h_1 is surjective, the monoid $M_{\mathbf{A}_2}(C)$ is a quotient of $M_{\mathbf{A}_1}(D)$, a surjective homomorphism $M_{\mathbf{A}_1}(D) \rightarrow M_{\mathbf{A}_2}(C)$ is given by

$$u^{\mathbf{A}_1}|_D \mapsto u^{\mathbf{A}_2}|_C,$$

all $u \in X^*$ with $Du \subseteq D$. Thus any divisor of $M_{\mathbf{A}_2}(C)$ divides $M_{\mathbf{A}_1}(D)$. It follows that ρ_2 is a \mathcal{G} -congruence and thus h_2 is a \mathcal{G} -homomorphism. \square

COROLLARY 4.4 *Suppose that $\rho_1 \leq \rho_2$ are congruence relations of the automaton \mathbf{A} . If ρ_2 is a \mathcal{G} -congruence, then so is ρ_1 . Further, ρ_2/ρ_1 is a \mathcal{G} -congruence of the quotient automaton \mathbf{A}/ρ_1 .*

REMARK 4.5 The assumption that h_1 is surjective was needed only in order to show that h_2 is a \mathcal{G} -congruence.

In order to prove the converse of Lemma 4.3, we need the following fact.

LEMMA 4.6 *Suppose that $\mathbf{A} = (A, X, \delta)$ is a permutation X -automaton. Let ρ be a \mathcal{G} -congruence relation of \mathbf{A} such that $G(\mathbf{A}/\rho) \in \overline{\mathcal{G}}$. Then $G(\mathbf{A})$ is in $\overline{\mathcal{G}}$.*

Proof. Assume first that \mathbf{A} is strongly connected, i.e., for each $a, b \in A$ there is some $u \in X^*$ with $au = b$. Let C_0 be a ρ -block. Define

$$Y = \{y_g : g \in G_{\mathbf{A}}(C_0)\}.$$

We turn C_0 into an Y -automaton $\mathbf{C}_0 = (C_0, Y, \delta_0)$ by defining

$$\delta_0(c, y_g) = cg,$$

for all $c \in C_0$ and $y_g \in Y$. It is known, see, e.g., [6, 2, 7], that \mathbf{A} is isomorphic to a cascade composition of \mathbf{A}/ρ and \mathbf{C}_0 . See also Remark 6.3. Thus, by Theorem 3.1, each simple group divisor of $G(\mathbf{A})$ divides $G(\mathbf{A}/\rho)$ or $G(\mathbf{C}_0)$. (Note that \mathbf{C}_0 is a permutation automaton.) Since ρ is a \mathcal{G} -congruence, $G(\mathbf{C}_0) = G_{\mathbf{A}}(C_0) \in \overline{\mathcal{G}}$. Further, $G(\mathbf{A}/\rho) \in \overline{\mathcal{G}}$, by assumption. It follows that $G(\mathbf{A}) \in \overline{\mathcal{G}}$.

When \mathbf{A} is not strongly connected, then \mathbf{A} is the disjoint sum of its strongly connected components $\mathbf{A}_1 = (A_1, X, \delta_1), \dots, \mathbf{A}_m = (A_m, X, \delta_m)$. Thus each \mathbf{A}_i is a strongly connected permutation automaton, moreover, the sets A_i are pairwise disjoint, $\cup_{i=1}^m A_i = A$, and $\delta(a, x) = \delta_i(a, x)$ for each $a \in A_i$ and $x \in X$ with $i \in [m]$. The group $G(\mathbf{A})$ is isomorphic to a subgroup of the direct product of the groups $G(\mathbf{A}_i)$, in particular

$$G(\mathbf{A}) \mid \prod_{i=1}^m G(\mathbf{A}_i). \quad (3)$$

For each $i \in [m]$, let ρ_i denote the restriction of ρ to A_i . Then each ρ_i is a \mathcal{G} -congruence relation of the strongly connected permutation automaton \mathbf{A}_i . But $G(\mathbf{A}_i/\rho_i)$ is a quotient of $G(\mathbf{A}/\rho)$, which is in $\overline{\mathcal{G}}$, by assumption. Thus each group $G(\mathbf{A}_i/\rho_i)$ is in $\overline{\mathcal{G}}$, so that $G(\mathbf{A}_i) \in \overline{\mathcal{G}}$, by the first part of the proof. Since $\overline{\mathcal{G}}$ is closed under direct product, it follows by (3) that $G(\mathbf{A})$ is also in $\overline{\mathcal{G}}$. \square

LEMMA 4.7 *Suppose that $\mathbf{A}_1, \mathbf{A}_2$ and \mathbf{A}_3 are X -automata and $h_1 : \mathbf{A}_1 \rightarrow \mathbf{A}_2$ and $h_2 : \mathbf{A}_2 \rightarrow \mathbf{A}_3$ are \mathcal{G} -homomorphisms. Then the composite*

$$h = A_1 \xrightarrow{h_1} A_2 \xrightarrow{h_2} A_3$$

is a \mathcal{G} -homomorphism $\mathbf{A}_1 \rightarrow \mathbf{A}_3$.

Proof. Define $\rho_i = \ker h_i$, $i = 1, 2$, and $\rho = \ker h$. Suppose that D is a ρ -block and that G is a subgroup of $M_{\mathbf{A}_1}(D)$. We need to show that $G \in \overline{\mathcal{G}}$. By Lemma 2.2, there exists a nonempty set $D_0 \subseteq D$ such that G is isomorphic to a subgroup of $G_{\mathbf{A}_1}(D_0)$. Let

$$Y = \{y_g : g \in G_{\mathbf{A}_1}(D_0)\}.$$

Defining

$$\delta_0(a, y_g) = ag,$$

D_0 becomes the state set of the permutation Y -automaton $\mathbf{D}_0 = (D_0, Y, \delta_0)$. Since h_1 is a \mathcal{G} -homomorphism, the restriction ρ'_1 of ρ_1 to D_0 is a \mathcal{G} -congruence of \mathbf{D}_0 . Further, \mathbf{D}_0/ρ'_1 is a permutation automaton, and since h_2 is a \mathcal{G} -homomorphism, the group $G(\mathbf{D}_0/\rho'_1)$ is in $\overline{\mathcal{G}}$. Thus, by Lemma 4.6, $G(\mathbf{D}_0) \in \overline{\mathcal{G}}$. But the two groups $G(\mathbf{D}_0)$ and $G_{\mathbf{A}_1}(D_0)$ are isomorphic, so that $G_{\mathbf{A}_1}(D_0)$ is also in $\overline{\mathcal{G}}$. \square

COROLLARY 4.8 *Suppose that $\rho_1 \leq \rho_2$ are congruence relations of the automaton \mathbf{A} . If ρ_1 is a \mathcal{G} -congruence and if ρ_2/ρ_1 is a \mathcal{G} -congruence of \mathbf{A}/ρ_1 , then ρ_2 is a \mathcal{G} -congruence.*

LEMMA 4.9 *Suppose that \mathbf{A} and \mathbf{B} are X -automata and that h is a simple homomorphism $\mathbf{A} \rightarrow \mathbf{B}$ which is not injective. Then there is an X -automaton \mathbf{C} , a surjective simple regular homomorphism $h_1 : \mathbf{A} \rightarrow \mathbf{C}$ and a simple homomorphism $h_2 : \mathbf{C} \rightarrow \mathbf{B}$ such that h_1 is not injective and*

$$h = \mathbf{A} \xrightarrow{h_1} \mathbf{C} \xrightarrow{h_2} \mathbf{B}.$$

Proof. Let ρ be minimal among those congruence relations of \mathbf{A} which collapse the states in at least one non-singleton congruence class of $\ker h$. Then let $\mathbf{C} = \mathbf{A}/\rho$ and let h_1 be the natural homomorphism $\mathbf{A} \rightarrow \mathbf{A}/\rho$. The definition of h_2 is forced. \square

REMARK 4.10 By Lemma 4.3 and Lemma 4.7, h is a \mathcal{G} -homomorphism iff h_1 and h_2 are \mathcal{G} -homomorphisms.

COROLLARY 4.11 *Suppose that \mathbf{A} is an X -automaton and ρ is a simple congruence relation of \mathbf{A} other than the identity relation. Then there is a simple regular congruence relation $\rho' \leq \rho$ which is not the identity relation and such that ρ/ρ' is also simple. Further, ρ is a \mathcal{G} -congruence iff both ρ' and ρ/ρ' are \mathcal{G} -congruences.*

5 Two Relations

Throughout this section \mathcal{G} denotes a given class of simple groups closed under division. We define two relations on automata.

DEFINITION 5.1 *Suppose that \mathbf{A} and \mathbf{B} are X -automata. We define:*

- $\mathbf{A} \geq \mathbf{B}$ if there is a surjective \mathcal{G} -homomorphism $\mathbf{A} \rightarrow \mathbf{B}$;
- $\mathbf{A} \succeq \mathbf{B}$ if there is a surjective simple regular \mathcal{G} -homomorphism $\mathbf{A} \rightarrow \mathbf{B}$.

Thus, if $\mathbf{A} \succeq \mathbf{B}$, then $\mathbf{A} \geq \mathbf{B}$. Moreover, both relations are reflexive, and the relation \geq is transitive, by Lemma 4.7. We let \equiv (\sim , respectively) denote the smallest equivalence relation containing the relation \geq (\succeq , respectively).

LEMMA 5.2 *Suppose that \mathbf{A} and \mathbf{B} are X -automata with $\mathbf{A} \geq \mathbf{B}$. Then $\mathbf{A} \sim \mathbf{B}$.*

Proof. Suppose that ρ is a \mathcal{G} -congruence of the X -automaton $\mathbf{A} = (A, X, \delta)$. We prove that $\mathbf{A} \sim \mathbf{A}/\rho$. We argue by induction on

$$\#\rho = \max\{|D| : D \in A/\rho\}.$$

The basis case that $\#\rho = 1$ is obvious. Suppose that $\#\rho > 1$. Define the X -automaton $\mathbf{A}' = (A, X, \delta')$ on the set A as follows. For each $a \in A$ and $x \in X$ with $\rho(a)x \subset \rho(ax)$ and $|\rho(ax)| = \#\rho$, let $\delta'(a, x)$ be some fixed element of $\rho(ax) - \rho(a)x$, depending only on $\rho(a)$ and x . Otherwise define $\delta'(a, x) = ax$. (Here, for any $b \in A$, $\rho(b)$ denotes the ρ -block containing b .) Note that ρ is a congruence relation of \mathbf{A}' and \mathbf{A}/ρ is isomorphic to \mathbf{A}'/ρ .

Let R denote the set

$$\{(a, b) \in A \times A : a \rho b \ \& \ (|\rho(a)| < \#\rho \text{ or } a \neq b)\}.$$

Then R determines a subautomaton of the direct product $\mathbf{A} \times \mathbf{A}'$. To prove this, suppose that $(a, b) \in R$ and $x \in X$. We need to show that $(a, b)x \in R$.

CASE 1 $|\rho(ax)| = \#\rho$ and $\rho(a)x = \rho(ax)$. Then $a \neq b$ and x induces in \mathbf{A} a bijection $\rho(a) \rightarrow \rho(ax)$. Thus $(a, b)x = (ax, bx)$ and $ax \neq bx$, proving $(a, b)x \in R$.

CASE 2 $|\rho(ax)| = \#\rho$ and $\rho(a)x \subset \rho(ax)$. Then $bx \neq ax$, since $bx \notin \rho(a)x$. Thus $(a, b)x \in R$.

CASE 3 $|\rho(ax)| < \#\rho$. Then $(a, b)x \in R$ holds obviously.

As noted above, ρ is a congruence relation of \mathbf{A}' . We show that ρ is a \mathcal{G} -congruence. For each ρ -block C , $M_{\mathbf{A}'}(C)$ is a submonoid of $M_{\mathbf{A}}(C)^c$, the semigroup obtained by adding the constant maps $C \rightarrow C$ to $M_{\mathbf{A}}(C)$. But since ρ is a \mathcal{G} -congruence of \mathbf{A} , each subgroup of $M_{\mathbf{A}}(C)$ is in $\overline{\mathcal{G}}$, moreover, each nontrivial subgroup of $M_{\mathbf{A}}(C)^c$ is a subgroup of $M_{\mathbf{A}}(C)$. Since ρ is a \mathcal{G} -congruence of \mathbf{A} , it follows that ρ is a \mathcal{G} -congruence of \mathbf{A}' .

The functions

$$\begin{aligned} \pi : R &\rightarrow A, & (a, b) &\mapsto a \\ \pi' : R &\rightarrow A, & (a, b) &\mapsto b \end{aligned}$$

are surjective homomorphisms $\mathbf{R} \rightarrow \mathbf{A}$ and $\mathbf{R} \rightarrow \mathbf{A}'$, respectively, where \mathbf{R} denotes the subautomaton of $\mathbf{A} \times \mathbf{A}'$ determined by the set R . Define $\theta = \ker \pi$ and $\theta' = \ker \pi'$. Then $\#\theta < \#\rho$ and $\#\theta' < \#\rho$. Thus, if π and π' are \mathcal{G} -homomorphisms, then $\mathbf{A} \sim \mathbf{R}$ and $\mathbf{A}' \sim \mathbf{R}$, by the induction assumption, so that

$$\mathbf{A} \sim \mathbf{A}'. \tag{4}$$

To prove that π is a \mathcal{G} -homomorphism, note that each θ -block C is either of the form

$$\{a\} \times \rho(a)$$

or

$$\{a\} \times (\rho(a) - \{a\}),$$

for some $a \in A$. Thus, writing $D = \rho(a)$ or $D = \rho(a) - \{a\}$, $M_{\mathbf{R}}(C)$ is a quotient of the submonoid of $M_{\mathbf{A}'}(\rho(a))$ determined by the functions $g = u^{\mathbf{A}'}|_D$, $u \in X^*$ with $Dg \subseteq D$ and $au^{\mathbf{A}} = a$. Since ρ is a \mathcal{G} -congruence of \mathbf{A}' , it follows that each simple group divisor of $M_{\mathbf{R}}(C)$ is in \mathcal{G} . Thus θ is a \mathcal{G} -congruence and π is a \mathcal{G} -homomorphism. The proof of the fact that π' is also a \mathcal{G} -homomorphism is similar. Thus (4) has been established.

By (4) and since \mathbf{A}/ρ and \mathbf{A}'/ρ are isomorphic, to complete the proof we need to show that $\mathbf{A}' \sim \mathbf{A}'/\rho$. Let τ denote the congruence relation of \mathbf{A}' whose non-singleton blocks are those ρ -blocks C with $|C| < \#\rho$. Then $\tau \leq \rho$, so that τ is a \mathcal{G} -congruence of \mathbf{A}' , by Corollary 4.4. Moreover, $\#\tau < \#\rho$, and ρ/τ is a simple \mathcal{G} -congruence of \mathbf{A}'/τ . Thus, $\mathbf{A}' \sim \mathbf{A}'/\tau$, by the induction assumption. But by Lemma 5.3 below, $\mathbf{A}'/\tau \sim \mathbf{A}'/\rho$, completing the proof. \square

LEMMA 5.3 *Suppose that \mathbf{A} and \mathbf{B} are X -automata and h is a surjective simple \mathcal{G} -homomorphism $\mathbf{A} \rightarrow \mathbf{B}$. Then there is chain*

$$\mathbf{A} \succeq \mathbf{A}_1 \succeq \dots \succeq \mathbf{A}_n \succeq \mathbf{B}.$$

Proof. By Lemma 4.9, there exist X -automata $\mathbf{A}_1, \dots, \mathbf{A}_n$ and surjective simple regular \mathcal{G} -homomorphisms

$$\mathbf{A} \xrightarrow{h_0} \mathbf{A}_1 \xrightarrow{h_1} \dots \xrightarrow{h_{n-1}} \mathbf{A}_n \xrightarrow{h_n} \mathbf{B}. \quad \square$$

COROLLARY 5.4 *For any two X -automata \mathbf{A} and \mathbf{B} , $\mathbf{A} \sim \mathbf{B}$ iff $\mathbf{A} \equiv \mathbf{B}$.*

6 Proof of Theorem 3.2

In this section we complete our proof of Theorem 3.2.

LEMMA 6.1 *Suppose that $\mathbf{A} = (A, X, \delta)$ is a given automaton and ρ is a simple regular \mathcal{G} -congruence of \mathbf{A} , for some class \mathcal{G} of simple groups closed under division. Let K consist of the automata \mathbf{A}/ρ and \mathbf{U} as well as the automata $\mathbf{Aut}(G)$ for $G \in \mathcal{G}$. Then*

$$\mathbf{A} \in \mathbf{V}_c(K).$$

Proof. We may assume that $\#\rho > 1$. Let C_1, \dots, C_k , $k > 0$, denote the ρ -blocks C_i with $|C_i| = \#\rho$, and let $D_1 = \{d_1\}, \dots, D_m = \{d_m\}$ be the singleton ρ -blocks. Since ρ is simple, the sets C_i and D_j are all of the ρ -blocks. For each $i \in [k]$ there exist words $u_i, v_i \in X^*$ with $C_1 u_i = C_i$ and $C_i v_i = C_1$, and such that $u_i v_i$ induces the identity function on C_1 and $v_i u_i$ induces the identity function on C_i , so that $(u_i v_i)^{\mathbf{A}}|_{C_1} = \lambda^{\mathbf{A}}|_{C_1}$ and $(v_i u_i)^{\mathbf{A}}|_{C_i} = \lambda^{\mathbf{A}}|_{C_i}$. (We may assume that $u_1 = v_1 = \lambda$).

Define

$$Y = \{y_a : a \in C_1\} \cup \{y_s : s \in S_{\mathbf{A}}(C_1)\}.$$

We turn C_1 into an Y -automaton \mathbf{C}_1 by defining

$$\begin{aligned} c y_a &= a \\ c y_s &= cs, \end{aligned}$$

for all $a, c \in C_1$ and $s \in S_{\mathbf{A}}(C_1)$. Then $\mathbf{A} \in \mathbf{IS}(\{\mathbf{B}\})$ holds for the cascade composition

$$\mathbf{B} = \mathbf{A}/\rho \times_{\varphi} \mathbf{C}_1,$$

where

$$\varphi : A/\rho \times X \rightarrow Y$$

is defined as follows. Let a_0 be a fixed element of C_1 . Then, for each $i \in [k]$ and $x \in X$, define

$$\varphi(C_i, x) = \begin{cases} y_s & \text{if } C_i x \subseteq C_j, \text{ where } s = (u_i x v_j)^{\mathbf{A}}|_{C_1} \text{ and } j \in [k]; \\ y_{a_0} & \text{if } C_i x = D_j \text{ for some } j \in [m]. \end{cases}$$

Moreover, for each $i \in [m]$ and $x \in X$, let

$$\varphi(D_i, x) = \begin{cases} y_a & \text{if } d_i x = b \in C_j, j \in [k], a \in C_i \text{ and } a u_j = b; \\ y_{a_0} & \text{if } d_i x = d_j, \text{ for some } j \in [m]. \end{cases}$$

Then the set

$$B_0 = \{(C_i, a) : a \in C_1, i \in [k]\} \cup \{(D_j, a_0) : j \in [m]\}$$

determines a subautomaton \mathbf{B}_0 of \mathbf{B} . Moreover, the function

$$\begin{aligned} h : B_0 &\rightarrow A \\ (C_i, a) &\mapsto a u_i \\ (D_j, a_0) &\mapsto d_j \end{aligned}$$

is an isomorphism $\mathbf{B}_0 \rightarrow \mathbf{A}$, as shown by the following commutative squares corresponding to the 4 cases in the definition of φ :

$$\begin{array}{ccc} (C_i, a) & \xrightarrow{h} & a u_i \\ \downarrow x & & \downarrow x \\ (C_j, a u_i x v_j) & \xrightarrow{h} & a u_i x v_j u_j = a u_i x \\ \\ (C_i, a) & \xrightarrow{h} & a u_i \\ \downarrow x & & \downarrow x \\ (D_j, a_0) & \xrightarrow{h} & d_j \\ \\ (D_i, a_0) & \xrightarrow{h} & d_i \\ \downarrow x & & \downarrow x \\ (C_j, a) & \xrightarrow{h} & b = a u_j \\ \\ (D_i, a_0) & \xrightarrow{h} & d_i \\ \downarrow x & & \downarrow x \\ (D_j, a_0) & \xrightarrow{h} & d_j \end{array}$$

To complete the proof, note that \mathbf{C}_1 is a permutation-reset automaton and any simple group dividing $M(\mathbf{C}_1)$ is in \mathcal{G} , since ρ is a \mathcal{G} -congruence. Thus,

$$\mathbf{C}_1 \in \mathbf{V}_c(\{\mathbf{U}, \mathbf{Aut}(G) : G \in \mathcal{G}\}),$$

by Lemma 2.3. It follows that $\mathbf{A} \in \mathbf{V}_c(K)$. \square

REMARK 6.2 The automaton \mathbf{B}_0 is a quotient of \mathbf{B} under the homomorphism $h' : \mathbf{B} \rightarrow \mathbf{B}_0$ defined by:

$$\begin{aligned} (C_i, a) &\mapsto (C_i, a) \\ (D_j, a) &\mapsto (D_j, a_0), \end{aligned}$$

for all $i \in [k]$, $j \in [m]$ and $a \in C_1$. The homomorphism h' is simple and aperiodic, and has the property that each (non-singleton) block of $\ker h'$ contains at most one state which is in the range of the transition function of \mathbf{B} . Such homomorphisms are termed *elementary* in [4].

Proof of Theorem 3.2. Let $\mathbf{A} = (A, X, \delta)$ be an automaton. Recall that the class $\mathcal{K}(\mathbf{A})$ consists of the automaton \mathbf{U} as well as the automata $\mathbf{Aut}(G)$ for simple groups G with $G|M(\mathbf{A})$. We need to show that

$$\mathbf{A} \in \mathbf{V}_c(\mathcal{K}(\mathbf{A})).$$

Let \mathbf{T} denote the trivial one-state X -automaton and let \mathcal{G} denote the class of simple groups G with $G|M(\mathbf{A})$. Then, with respect to this class \mathcal{G} , $\mathbf{A} \geq \mathbf{T}$, so that $\mathbf{A} \sim \mathbf{T}$, by Corollary 5.4. Thus, there exists a sequence of X -automata $\mathbf{B}_0, \dots, \mathbf{B}_k$ such that $\mathbf{B}_0 = \mathbf{T}$, $\mathbf{B}_k = \mathbf{A}$, and for each $i \in \{0, \dots, k-1\}$ either $\mathbf{B}_i \succeq \mathbf{B}_{i+1}$ or $\mathbf{B}_{i+1} \succeq \mathbf{B}_i$. We argue by induction on i to show that $\mathbf{B}_i \in \mathbf{V}_c(\mathcal{K}(\mathbf{A}))$. When $i = 0$, this is obvious. For the induction step, suppose that $i > 0$ and $\mathbf{B}_{i-1} \in \mathbf{V}_c(\mathcal{K}(\mathbf{A}))$. If $\mathbf{B}_{i-1} \succeq \mathbf{B}_i$, then $\mathbf{B}_i \in \mathbf{H}(\{\mathbf{B}_{i-1}\})$, so that $\mathbf{B}_i \in \mathbf{V}_c(\mathcal{K}(\mathbf{A}))$. Suppose that $\mathbf{B}_i \succeq \mathbf{B}_{i-1}$. Then there is a surjective simple regular \mathcal{G} -homomorphism $h : \mathbf{B}_i \rightarrow \mathbf{B}_{i-1}$. Thus, by Lemma 6.1,

$$\mathbf{B}_i \in \mathbf{V}_c(\mathcal{K}(\mathbf{A}) \cup \mathbf{B}_{i-1}).$$

It follows from the induction assumption that $\mathbf{B}_i \in \mathbf{V}_c(\mathcal{K}(\mathbf{A}))$. \square

REMARK 6.3 When \mathbf{A} is a permutation automaton and $\#\rho > 1$, there is no singleton ρ -block. We may define $Y = \{y_s : s \in G_{\mathbf{A}}(C_1)\}$, so that \mathbf{C}_1 becomes the Y -automaton with $cy_s = cs$, for all $c \in C_1$ and $s \in G_{\mathbf{A}}(C_1)$. Then \mathbf{C}_1 is a permutation automaton and $G(\mathbf{C}_1)$ is in $\bar{\mathcal{G}}$. Moreover, \mathbf{A} is isomorphic to a cascade composition of \mathbf{A}/ρ with \mathbf{C}_1 .

COROLLARY 6.4 *Suppose that \mathcal{G} is a class of simple groups closed under division. Let K consist of \mathbf{U} and the automata $\mathbf{Aut}(G)$ for $G \in \mathcal{G}$. Then the following conditions are equivalent for an automaton \mathbf{A} :*

1. Each simple group divisor of $S(\mathbf{A})$ is in \mathcal{G} .
2. There is a sequence of automata $\mathbf{A}_0, \dots, \mathbf{A}_n$ such that \mathbf{A}_0 is trivial, \mathbf{A}_n is \mathbf{A} , and for each $i \in [n]$, either \mathbf{A}_i is a quotient of \mathbf{A}_{i-1} under a simple regular \mathcal{G} -homomorphism, or \mathbf{A}_{i-1} is a quotient of \mathbf{A}_i under a simple regular \mathcal{G} -homomorphism.
3. $\mathbf{A} \in \mathbf{V}_c(K)$.

4. A is in the least class of automata containing K and closed under subautomata, simple regular \mathcal{G} -homomorphic images, renaming and cascade composition.
5. A is in the least class of automata containing K and closed under subautomata, \mathcal{G} -homomorphic images, renaming and cascade composition.

Note This paper was submitted to an editor of Theoretical Computer Science in December 1995. Unfortunately the author has not received any referee report since then.

References

- [1] M.A. Arbib, ed., *Algebraic Theory of Machines, Languages, and Semigroups*, Academic Press, 1968.
- [2] S. Eilenberg, *Automata, Languages, and Machines*, vol. B., Academic Press, 1976.
- [3] Z. Ésik, Results on homomorphic realization of automata by α_0 -products, *Theoretical Computer Science*, 87(1991), 229–249.
- [4] Z. Ésik, Group axioms for iteration, *Information and Computation*, 148(1999), 131–180.
- [5] F. Gécseg, *Products of Automata*, Springer-Verlag, 1986.
- [6] A. Ginzburg, *Algebraic Theory of Automata*, Academic Press, 1968.
- [7] W.M.L. Holcombe, *Algebraic Automata Theory*, Cambridge University Press, 1982.
- [8] K. Krohn and J. Rhodes, The algebraic theory of machines I, *Trans. Amer. Math. Soc.*, 116(1965), 450–464.
- [9] G. Lallement, *Semigroups and Combinatorial Applications*. Wiley-Interscience, 1979.
- [10] H. Straubing, *Finite Automata, Formal Logic, and Circuit Complexity*, Birkhäuser, 1994.