AUTOMATA WITH FINITE CONGRUENCE LATTICES *

István Babcsányi

Department of Algebra, Mathematical Institute,
Budapest University of Technology and Economics,
1111 Budapest, Egry József u. 1, HUNGARY
E-mail: babcs@math.bme.hu

To the memory of Balázs Imreh

Abstract

In this paper we prove that if the congruence lattice of an automaton $\mathbf{A}$ is finite then the endomorphism semigroup $E(\mathbf{A})$ of $\mathbf{A}$ is finite. Moreover, if $\mathbf{A}$ is commutative then $\mathbf{A}$ is A-finite. We prove that if $3 \leq |A|$ then a commutative automaton $\mathbf{A}$ is simple if and only if it is a cyclic permutation automaton of prime order. We also give some results concerning cyclic, strongly connected and strongly trap-connected automata.

1 Preliminaries

In this paper, by an *automaton* $\mathbf{A} = (A, X, \delta)$ we mean always an automaton without outputs, where $A \neq \emptyset$ is the *state set* and $X \neq \emptyset$ is the *input set*. Denote $|A|$ the cardinality of the set A. The automaton $\mathbf{A}$ is called *A-finite* if $|A| < \infty$. If $|A| = n$ then we say that n is the *order of* $\mathbf{A}$ and if n is a prime then $\mathbf{A}$ is an *automaton of prime order*. The *input monoid* [*semigroup*] X^* $[X^+]$ of $\mathbf{A}$ is the free monoid [semigroup] over X. The *transition function* $\delta : A \times X \to A$ can be extended in the usual way. If $e \in X^*$ is the empty word then let $\delta(a, e) = a$ for every $a \in A$; if $a \in A$, $p \in X^*$ and $x \in X$ then let $\delta(a, px) = \delta(\delta(a, p), x)$. Sometimes, we shall use the notation ap instead of $\delta(a, p)$.

*Research supported by the Hungarian NFSR grant No 67639

As known, every automaton can be considered as a unary algebra. Thus the notions such as subautomaton, congruence, homomomorphism, isomorphism etc. can be introduced in the following natural way.

An equivalence relation ρ of state set A of the automaton $\mathbf{A}$ is called a *congruence* on $\mathbf{A}$ if

$$(a,b) \in \rho \Longrightarrow (ax,bx) \in \rho,$$

for all $a,b \in A$ and $x \in X$. The ρ-class of $\mathbf{A}$ containing the state a is denoted by $\rho[a]$. Denote $C(\mathbf{A})$ the congruence lattice of $\mathbf{A}$. Let ι_A [ω_A] be the equality [universal] relation on A. The automaton $\mathbf{A}$ is called *simple* if $C(\mathbf{A}) = \{\iota_A, \omega_A\}$. It is evident that if $|A| \leq 2$ then $\mathbf{A}$ is simple.

The automaton $\mathbf{A}' = (A', X, \delta')$ is a *subautomaton* of the automaton $\mathbf{A} = (A, X, \delta)$ if $A' \subseteq A$ and δ' is the restriction of δ to $A' \times X$. The congruence

$$\rho_{A'} = \{(a,b) \in A^2;\ a = b \text{ or } a,b \in A'\}$$

is called *the Rees congruence of* $\mathbf{A}$ *induced by* $\mathbf{A}'$ ([2]). The set $R(\mathbf{A})$ of Rees congruences of $\mathbf{A}$ is a sublattice of $C(\mathbf{A})$. It is called *the Rees congruence lattice* of $\mathbf{A}$.

Let $\mathbf{A} = (A, X, \delta)$ and $\mathbf{B} = (B, X, \delta')$ be arbitrary automata. We say that a mapping $\varphi : A \to B$ is a *homomorphism* of $\mathbf{A}$ into $\mathbf{B}$ if

$$\varphi(ax) = \varphi(a)x,$$

for all $a \in A$ and $x \in X$. The *kernel* of φ is the congruence $\operatorname{Ker}\varphi$ defined by $(a,b) \in \operatorname{Ker}\varphi$ if and only if $\varphi(a) = \varphi(b)$ $(a,b \in A)$. If $A = B$ then φ is an *endomorphism* of $\mathbf{A}$. Furthermore, if φ is bijective then it is an *automorphism* of $\mathbf{A}$. The set $E(\mathbf{A})$ [$G(\mathbf{A})$] of all endomorphisms [automorphisms] of $\mathbf{A}$ is a monoid [group] under the usual multiplication of mappings. $E(A)$ [$G(A)$] is called the *endomorphism semigroup* [*automorphism group*] of $\mathbf{A}$.

For notations and notions not defined here we refer to the books P.M. Cohn [5], F. Gécseg [7], F. Gécseg, F. and I. Peák [8], K.H. Kim and F.W. Roush [10] and G. Lallement [11].

2 Automata with finite congruence lattices

Let B be a nonempty subset of the state set A of an automaton $\mathbf{A} = (A, X, \delta)$. Denote $[\mathbf{B}] = ([B], X, \delta')$ the subautomaton of $\mathbf{A}$ generated by B, that is, $[B] = \{bp; b \in B, p \in X^*\}$. Specially, denote $[\mathbf{a}] = ([a], X, \delta')$ the subautomaton generated by $a \in A$. If $A = [B]$ then B is called a *generating set* of $\mathbf{A}$. If there exists a finite generating set of $\mathbf{A}$ then we say that $\mathbf{A}$ is *finitely*

generated. Specially, if there exists a generating set containing only one element a then $\mathbf{A}$ is called a *cyclic automaton* and we say that a is a *generating element* of $\mathbf{A}$.

Lemma 1 *If the congruence lattice of an automaton* $\mathbf{A}$ *is finite then* $\mathbf{A}$ *has finitely many subautomata and the congruence lattices of its subautomata are also finite.*

Proof. Assume that the congruence lattice $C(\mathbf{A})$ of the automaton $\mathbf{A} = (A, X, \delta)$ is finite. Thus the Rees congruence lattice $R(\mathbf{A})$ is finite. From this it follows that $\mathbf{A}$ has finitely many subautomata.

If $\mathbf{A}' = (A', X, \delta')$ is a subautomaton of $\mathbf{A}$ and $\rho \in C(\mathbf{A}')$ then $\rho \cup \iota_A \in C(\mathbf{A})$. Furthermore, if $\rho, \rho' \in C(A')$ and $\rho \neq \rho'$ then $\rho \cup \iota_A \neq \rho' \cup \iota_A$. Thus $C(\mathbf{A}')$ is also finite. ■

Corollary 1 *If the congruence lattice of an automaton is finite then the automaton is finitely generated.*

Proof. If the congruence lattice of an automaton is finite then by Lemma 1, the number of its subautomata and thus the number of its cyclic subautomata is finite. Therefore, the automaton is finitely generated. ■

S. Radeleczki has prowed in [15] that if the congruence lattice of a unary algebra is finite then its automorphism group is finite, too. The following theorem is a generalization of this result.

Theorem 1 *If the congruence lattice* $C(\mathbf{A})$ *of an automaton* $\mathbf{A} = (A, X, \delta)$ *is finite then the endomorphism semigroup* $E(\mathbf{A})$ *is finite.*

Proof. First, we show that the automorphism group $G(\mathbf{A})$ is finite. Assume that the order of $\alpha \in G(\mathbf{A})$ is infinite. For every positive integer m, we define the binary relation ρ_{α^m} on A, as follows. For $a, b \in A$, $(a, b) \in \rho_{\alpha^m}$ if and only if there is an element c of A and there are integers i, k, l such that $0 \leq i \leq m-1$ and

$$a = \alpha^{km+i}(c), \quad b = \alpha^{lm+i}(c).$$

It can be easily verified that ρ_{α^m} is a congruence of $\mathbf{A}$. Furthermore, if $m \neq n$ then $\rho_{\alpha^m} \neq \rho_{\alpha^n}$ in a contradiction with our assumption that the congruence lattice $C(\mathbf{A})$ is finite. Thus the order of every $\alpha \in G(\mathbf{A})$ is finite.

Let r be the order of $\alpha \in G(\mathbf{A})$. Take the binary relation ρ_α on A for which $(a, b) \in \rho_\alpha$ if and only if there are $c \in A$ and integers $0 \leq i, j \leq r-1$ such that

$$a = \alpha^i(c), \quad b = \alpha^j(c).$$

For every $\alpha \in G(\mathbf{A})$, the relation ρ_α is a congruence of $\mathbf{A}$. Assume that

$$\rho_\alpha = \rho_\beta, \quad \beta \in G(\mathbf{A}).$$

By Corollary 1, the automaton $\mathbf{A}$ is finitely generated. If $\{c_1, c_2, \ldots, c_k\}$ is a finite generating set of $\mathbf{A}$ then

$$\rho_\beta[c_1] = \rho_\alpha[c_1],\ \rho_\beta[c_2] = \rho_\alpha[c_2], \ldots, \rho_\beta[c_k] = \rho_\alpha[c_k],$$

that is,

$$\beta(c_1) = \alpha^{i_1}(c_1),\ \beta(c_2) = \alpha^{i_2}(c_2), \ldots, \beta(c_k) = \alpha^{i_k}(c_k)$$

$(0 \leq i_1, i_2, \ldots, i_k \leq r-1)$. This means that $\beta = \alpha^{i_j}$ on $[c_j]$ $(j = 1, 2, \ldots, k)$. From this it follows that the number of such β is finite for arbitrary $\alpha \in G(\mathbf{A})$. Since $C(\mathbf{A})$ is finite, the number of different ρ_α's is finite. From these results it follows that $G(\mathbf{A})$ is finite.

Now we show that the endomorphism semigroup $E(\mathbf{A})$ is also finite. If $\alpha \in E(\mathbf{A})$ then $\mathbf{A}_\alpha = (\alpha(A), X, \delta')$ is a subautomaton of $\mathbf{A}$, where $\alpha(A) = \{\alpha(a); a \in A\}$. Let $\beta \in E(\mathbf{A})$ such that

$$\operatorname{Ker}\beta = \operatorname{Ker}\alpha \quad \text{and} \quad \beta(A) = \alpha(A).$$

Define the mapping $\varphi_{\alpha,\beta} : \alpha(A) \to \beta(A)$ such that

$$\varphi_{\alpha,\beta}(\alpha(a)) = \beta(a)$$

for every $a \in A$. This means that

$$\varphi_{\alpha,\beta}\alpha = \beta.$$

Since $\operatorname{Ker}\beta = \operatorname{Ker}\alpha$, $\varphi_{\alpha,\beta}$ is a bijective mapping. If $a \in A$ and $x \in X$ then

$$\varphi_{\alpha,\beta}(\alpha(a)x) = \varphi_{\alpha,\beta}\alpha(ax) = \beta(ax) = \beta(a)x = \varphi_{\alpha,\beta}(\alpha(a))x,$$

that is, $\varphi_{\alpha,\beta} \in G(\mathbf{A}_\alpha)$. By Lemma 1, $C(\mathbf{A}_\alpha)$ is finite and thus, by the first part of this proof, $G(\mathbf{A}_\alpha)$ is finite. Furthermore, if

$$\operatorname{Ker}\beta = \operatorname{Ker}\beta' = \operatorname{Ker}\alpha, \quad \beta(A) = \beta'(A) = \alpha(A)$$

and

$$\varphi_{\alpha,\beta} = \varphi_{\alpha,\beta'},$$

then $\beta = \beta'$. Thus, for arbitrary $\alpha \in E(\mathbf{A})$, the number of $\beta \in E(\mathbf{A})$ such that $\operatorname{Ker}\beta = \operatorname{Ker}\alpha$ and $\beta(A) = \alpha(A)$ is finite. Since the number of different $\operatorname{Ker}\alpha$'s and different $\beta(A)$'s $(\alpha, \beta \in E(\mathbf{A}))$ is finite, $E(\mathbf{A})$ is also finite. ■

For every $a \in A$, consider the binary relation $\rho_{A,a}$ on X^* defined as

$$(p, q) \in \rho_{A,a} \quad \Longleftrightarrow \quad ap = aq \quad (p, q \in X^*).$$

It is clear that $\rho_{A,a}$ $(a \in A)$ is a right congruence on X^*. The relation $\rho_A = \cap_{a \in A} \rho_{A,a}$ is congruence on X^*. The *characteristic semigroup* $S(\mathbf{A})$ of the automaton $\mathbf{A}$ is the factor semigroup X^*/ρ_A.

R.H. Oehmke has shown in [13] the first part of the following lemma, that is, for arbitrary cyclic automaton $\mathbf{A} = (A, X, \delta)$, $|E(\mathbf{A})| \leq |A|$. We have shown in our paper [1] that $|A| \leq |S(\mathbf{A})|$.

Lemma 2 *For every cyclic automaton* $\mathbf{A} = (A, X, \delta)$,

$$|E(\mathbf{A})| \leq |A| \leq |S(\mathbf{A})|.$$

Proof. If a_0 is a generating element of $\mathbf{A}$ and $\alpha(a_0) = \beta(a_0)$ $(\alpha, \beta \in E(\mathbf{A}))$ then, for every $p \in X^*$,

$$\alpha(a_0 p) = \alpha(a_0)p = \beta(a_0)p = \beta(a_0 p),$$

that is, $\alpha = \beta$. Thus the mapping $\varphi : E(\mathbf{A}) \to A$ such that $\varphi(\alpha) = \alpha(a_0)$, for every $\alpha \in E(\mathbf{A})$, is an injective mapping of $E(\mathbf{A})$ into A. This means that $|E(\mathbf{A})| \leq |A|$.

If $a_0 p \neq a_0 q$ $(p, q \in X^*)$ then $\rho_A[p] \neq \rho_A[q]$. From this it follows that $|A| \leq |S(\mathbf{A})|$. ■

Lemma 3 *If the relation* ρ_{A,a_0} *is a congruence on* X^**, for a generating element* a_0 *of a cyclic automaton* $\mathbf{A} = (A, X, \delta)$*, then* $E(\mathbf{A}) \cong S(\mathbf{A})$ *and* $|E(\mathbf{A})| = |A|$.

Proof. If the relation ρ_{A,a_0} is a congruence on X^* then $\rho_{A,a_0} = \rho_A$. Define the mapping $\alpha_p : A \to A$, for every $p \in X^*$, such that

$$\alpha_p(a_0 q) = a_0 pq \quad (q \in X^*).$$

It can easily be shown that $\alpha_p \in E(\mathbf{A})$. Furthermore, if $\alpha \in E(\mathbf{A})$ and $\alpha(a_0) = a_0 r$ $(r \in X^*)$ then $\alpha = \alpha_r$. The mapping $\varphi : E(\mathbf{A}) \to S(\mathbf{A})$ such that

$$\varphi(\alpha_p) = \rho_A[p] \quad (p \in X^*)$$

is an isomorphism of $E(\mathbf{A})$ onto $S(\mathbf{A})$. By Lemma, $|E(\mathbf{A})| = |A|$. ■

From Theorem 1, Lemma 2 and Lemma 3, we get the following corollary.

Corollary 2 *Let the congruence lattice* $C(\mathbf{A})$ *of the cyclic automaton* $\mathbf{A} = (A, X, \delta)$ *be finite. If the relation* ρ_{A,a_0} *is a congruence on* X^**, for a generating element* a_0*, then* $\mathbf{A}$ *is A-finite.* ■

The automaton $\mathbf{A}$ is *commutative* if $apq = aqp$ for every $a \in A$ and $p, q \in X^*$. It is immediate that every subautomaton of a commutative automaton is also commutative. I. Peák proved in [14] that $E(\mathbf{A}) \cong S(\mathbf{A})$ and $|E(\mathbf{A})| = |A|$ for arbitrary cyclic commutative automaton $\mathbf{A}$. (See also F. Gécseg and I. Peák [8], Z. Ésik and B. Imreh [6].) The statement of Lemma 3 is a generalization of this result. A.P. Grillet showed in [9] that if the congruence lattice of a commutative semigroup S is finite then S is finite. The following theorem generalizes this statement for commutative automata.

Theorem 2 *If the congruence lattice $C(\mathbf{A})$ of a commutative automaton $\mathbf{A} = (A, X, \delta)$ is finite then the automaton $\mathbf{A}$ is A-finite.*

Proof. By Corollary 1, $\mathbf{A}$ is finitely generated. Then, it is a union of commutative cyclic subautomata $\mathbf{A}_i = (A_i, X, \delta_i)$ $(i = 1, 2, \ldots, n)$. But, if $a_i \in A_i$ is a generating element of $\mathbf{A}_i$ then ρ_{A_i, a_i} is a congruence on X^*, since $\mathbf{A}_i$ $(i = 1, 2, \ldots, n)$ is commutative. By Corollary 2, $\mathbf{A}_i$ $(i = 1, 2, \ldots, n)$ is A-finite and thus $\mathbf{A}$ is also finite. ■

3 Simple automata

We discussed in our papers [3] and [4] the simple Mealy and Moore automata. In this paper we investigate the simplicity of the automata $\mathbf{A} = (A, X, \delta)$ without outputs. In this case $C(\mathbf{A}) = \{\iota_A, \omega_A\}$.

Let $H \neq \emptyset$ be a subset of the state set A and let $Hp = \{ap; a \in H\}$ for every $p \in X^*$. Define the binary relation τ_H on A as follows.

$$(a, b) \in \tau_H \quad \text{if and only if} \quad (ap \in H \iff bp \in H)$$

for every $p \in X^*$. τ_H is a congruence of $\mathbf{A}$ and H is a union of certain τ_H-congruence classes. The state $a \in A$ is called *disjunctive*, if $\tau_{\{a\}} = \iota_A$.

The set H is called a *separator* of $\mathbf{A}$ if, for every $p \in X^*$,

$$Hp \subseteq H \quad \text{or} \quad Hp \cap H = \emptyset.$$

The one-element subsets of A and itself A are separators of $\mathbf{A}$. We say that these separators are the *trivial separators*.

Lemma 4 *The automaton $\mathbf{A} = (A, X, \delta)$ is simple if and only if every separator of $\mathbf{A}$ is trivial.*

Proof. Assume that all separators of $\mathbf{A}$ are trivial. If ρ is a congruence of $\mathbf{A}$ then every ρ-class is a separator of $\mathbf{A}$. Therefore, $\rho = \iota_A$ or $\rho = \omega_A$, that is, $\mathbf{A}$ is a simple automaton.

Conversely, assume that $\mathbf{A}$ is simple. If H is a separator of $\mathbf{A}$ then τ_H is a congruence of $\mathbf{A}$ such that H is a τ_H-class. But $\tau_H = \iota_A$ or $\tau_H = \omega_A$. Thus $|H| = 1$ or $H = A$ therefore H is a trivial separator of $\mathbf{A}$. ■

If every state of an automaton $\mathbf{A} = (A, X, \delta)$ is a generating element of $\mathbf{A}$ then we say that $\mathbf{A}$ is *strongly connected*. In other words, $\mathbf{A}$ is *strongly connected* if, for arbitrary states $a, b \in A$, there exists a $p \in X^+$ such that $ap = b$. If $[c] = \{c\}$ then the state $c \in A$ is called a *trap* of $\mathbf{A}$. The automaton $\mathbf{A}$ is called *strongly trap-connected* if it has a trap c and for every state $a \in A - \{c\}$ and $b \in A$, there exists a $p \in X^*$ such that $ap = b$. It is known that the automaton $\mathbf{A}$ is strongly connected if and only if it has no subautomaton $\mathbf{A}' = (A', X, \delta)$ of $\mathbf{A}$ such that $A' \neq A$. Furthermore, if $\mathbf{A}$ strongly trap-connected then it has only one trap.

Corollary 3 *(G. Thierrin [16]) Every simple automaton with at least three states is strongly connected or strongly trap-connected.*

Proof. If $\mathbf{A}' = (A', X, \delta')$ is a subautomaton of the automaton $\mathbf{A} = (A, X, \delta)$ then A' is a separator of $\mathbf{A}$. Thus $A' = A$ or $|A'| = 1$. If $\mathbf{A}$ is not strongly connected, then it has only one subautomaton $\mathbf{A}' = (A', X, \delta)$, namely $|A'| = 1$. In the latter case if $A' = \{c\}$ then c is a trap of $\mathbf{A}$. Hence if $\mathbf{A}$ is not strongly connected then it is strongly trap-connected. ■

Theorem 3 *The strongly trap-connected automaton $\mathbf{A} = (A, X, \delta)$ with at least three states is simple if and only if the trap of $\mathbf{A}$ is disjunctive.*

Proof. Let $c \in A$ be the trap of $\mathbf{A}$. First, we show that if ρ is a congruence of $\mathbf{A}$ and $\rho \neq \omega_A$ then $\rho[c] = \{c\}$. Let $a, b \in A$ be arbitrary states. Assume that $(a, c) \in \rho$. If $a \neq c$ then there exists a $p \in X^*$ such that $ap = b$. Thus

$$(b, c) = (ap, cp) \in \rho.$$

From this it follows that $\rho = \omega_A$. This is impossible. Thus we get that $a = c$ and $\rho[c] = \{c\}$.

Now assume that c is disjunctive, that is, $\tau_{\{c\}} = \iota_A$. Let $\rho \neq \omega_A$ be a congruence of $\mathbf{A}$. Since $\rho[c] = \{c\}$, if $a, b \in A - \{c\}$ and $(a, b) \in \rho$ then $(a, b) \in \tau_{\{c\}}$, that is, $a = b$. We get $\rho = \iota_A$ and thus $\mathbf{A}$ is simple.

Conversely, assume that $\mathbf{A}$ is simple. But $\mathbf{A}$ is strongly trap-connected automaton with at least three states, thus $\tau_{\{c\}} \neq \omega_A$. Therefore $\tau_{\{c\}} = \iota_A$ and so c is disjunctive. ■

4 Commutativity of simple automata

Theorem 4 *If the strongly trap-connected automaton $\mathbf{A} = (A, X, \delta)$ with at least three states is simple then it is not commutative. Furthermore $G(\mathbf{A}) = \{\iota_A\}$ and $E(\mathbf{A}) = \{\iota_A, \alpha_c\}$, where c is the trap of $\mathbf{A}$, and α_c defined by $\alpha_c(a) = c$ $(a \in A)$.*

Proof. Assume that $\mathbf{A}$ is commutative. Let $a, b \in A - \{c\}$ and $a \neq b$. Since $\mathbf{A}$ is strongly trap-connected, there are $q, r \in X^*$ such that $aq = b$ and $br = a$. Thus, for arbitrary $p \in X^*$,

$$bp = aqp = apq \quad \text{and} \quad ap = brp = bpr.$$

Then, $ap = c$ if and only if $bp = c$. Thus $(a, b) \in \tau_{\{c\}}$, that is, $a = b$, which contradicts the assumption. We get that $\mathbf{A}$ is not commutative.

It is evident that $\alpha_c \in E(\mathbf{A})$. If $\alpha \in E(\mathbf{A})$ then, for every $p \in X^*$,

$$\alpha(c)p = \alpha(cp) = \alpha(c),$$

and so $\alpha(c)$ is a trap of $\mathbf{A}$, that is $\alpha(c) = c$. If $a \in A - \{c\}$ and $\alpha(a) = c$ then, for every $p \in X^*$,

$$\alpha(ap) = \alpha(a)p = cp = c,$$

that is, $\alpha = \alpha_c$. Assume that $a, b \in A - \{c\}$, $a \neq b$ and $\alpha(a) = \alpha(b)$. If, for every $p \in X^*$, $ap = c$ if and only if $bp = c$ then $(a, b) \in \tau_{\{c\}}$. By Theorem 3, $a = b$. This is a contradiction. Thus there exists a $q \in X^*$ such that for instance $aq = c$ and $bq \neq c$. Then

$$\alpha(bq) = \alpha(b)q = \alpha(a)q = \alpha(aq) = \alpha(c) = c.$$

From this it follows that $\alpha = \alpha_c$, thus $G(\mathbf{A}) = \{\iota_A\}$ and $E(\mathbf{A}) = \{\iota_A, \alpha_c\}$. ■

Lemma 5 *Every endomorphism of a strongly connected automaton is surjective.*

Proof. Let $\mathbf{A} = (A, X, \delta)$ be a strongly connected automaton. If $\alpha \in E(\mathbf{A})$ then $\mathbf{A}_\alpha = (\alpha(A), X, \delta')$ is a subautomaton of $\mathbf{A}$. Therefore, $\alpha(A) = A$, that is, α is a surjective mapping. ■

Theorem 5 *Let the strongly connected automaton $\mathbf{A} = (A, X, \delta)$ with at least three states be simple. If $E(\mathbf{A}) = \{\iota_A\}$ then $\mathbf{A}$ is not commutative. If $E(\mathbf{A}) \neq \{\iota_A\}$ then $\mathbf{A}$ is an A-finite commutative automaton, $|E(\mathbf{A}| = |A|$ and $E(\mathbf{A}) = G(\mathbf{A})$ is a cyclic group of prime order.*

Proof. First, we show that if the strongly connected automaton $\mathbf{A}$ with at least three states is simple then $E(\mathbf{A}) = G(\mathbf{A})$ is a finite group. Since $\operatorname{Ker}\alpha$ ($\alpha \in E(\mathbf{A})$) is a congruence of $\mathbf{A}$, $\operatorname{Ker}\alpha = \iota_A$ or $\operatorname{Ker}\alpha = \omega_A$. By Lemma 5, α is surjective mapping. From this it follows that $\operatorname{Ker}\alpha = \iota_A$ and thus $\alpha \in G(\mathbf{A})$. This means that $E(\mathbf{A}) = G(\mathbf{A})$. By Theorem 1, $E(\mathbf{A})$ is finite.

Assume that $E(\mathbf{A}) = \{\iota_A\}$ and $\mathbf{A}$ is commutative. Since $\mathbf{A}$ is strongly connected, there are $a_0 \in A$ and $p \in X^+$ such that $a_0 \neq a_0 p$. Define the mapping α_p in the same way as in the proof of Lemma 3. Since the relation ρ_{A,a_0} is a congruence on X^*, $\alpha_p \in E(\mathbf{A})$ and $\alpha_p \neq \iota_A$. This is impossible, and so $\mathbf{A}$ is not commutative.

Now assume that $E(\mathbf{A}) = G(\mathbf{A}) \neq \{\iota_A\}$. Let $\alpha \in G(\mathbf{A})$ and $\alpha \neq \iota_A$. Consider the congruence ρ_α defined in the proof of Theorem 1. Since $\mathbf{A}$ is simple, $\rho_\alpha = \iota_A$ or $\rho_\alpha = \omega_A$. If $\rho_\alpha = \iota_A$ then $\alpha = \iota_A$. If $\rho_\alpha = \omega_A$ then, for arbitrary state $d \in A$,

$$A = \{d, \alpha(d), \ldots, \alpha^{r-1}(d)\}.$$

If $\beta \in G(\mathbf{A})$ then there exists an integer $0 \leq j \leq r-1$ such that $\beta(d) = \alpha^j(d)$. Thus, for every $p \in X^*$, we have $\beta(dp) = \alpha^j(dp)$, that is, $\beta = \alpha^j$. Then, $G($**A** is a cyclic group.

If r is not prime then $r = ln$ $(1 < l, n < r)$. Define the binary relation $\rho_{l,n}$ on A as follows. For $a, b \in A$ $(a, b) \in \rho_{l,n}$ if and only if there are integers $0 \leq i \leq l-1$ and $0 \leq j, k \leq n-1$ such that

$$a = \alpha^{i+jl}(d), \quad b = \alpha^{i+kl}(d).$$

It is easy to show that $\rho_{l,n}$ is a congruence of $\mathbf{A}$ and $\rho_{l,n} \neq \iota_A, \omega_A$. It is a contradiction. Hence r is a prime number.

We show that $\mathbf{A}$ is commutative. If $p, q \in X^*$ then let $ap = \alpha^k(a)$ and $aq = \alpha^l(a)$ $(0 \leq k, l \leq r-1)$. Then, for arbitrary $0 \leq i \leq r-1$,

$$\alpha^i(a)pq = \alpha^i(ap)q = \alpha^i\alpha^k(a)q = \alpha^i\alpha^k(aq) =$$

$$= \alpha^i\alpha^k\alpha^l(a) = \alpha^i\alpha^l\alpha^k(a) =$$

$$= \alpha^i\alpha^l(ap) = \alpha^i\alpha^l(a)p = \alpha^i(aq)p = \alpha^i(a)qp,$$

that is, $\mathbf{A}$ is commutative.

By Theorem 2, the automaton $\mathbf{A}$ is A-finite. By Lemma 2 and Lemma 3, $|E(\mathbf{A}| = |A|$. ■

We note that W. Lex proved in [12], if $\mathbf{A}$ is a simple automaton then $|G(\mathbf{A})| = 1$ or $G(\mathbf{A})$ is a cyclic group of prime order.

The automaton $\mathbf{A} = (A, X, \delta)$ is called a *permutation automaton* if every input sign $x \in X$ is a permutation sign, that is, if $ax = bx$ $(a, b \in A)$ then

$a = b$. Let the automaton $\mathbf{A}$ be A-finite and $|A| = r$. The input sign $x \in X$ is called *cyclic permutation sign* if, for any $a \in A$,

$$A = \{a, ax, ax^2, \ldots, ax^{r-1}\} \quad (ax^r = a).$$

The input sign $x \in X$ is called *identical permutation sign* if $ax = a$ for every $a \in A$. The permutation automaton $\mathbf{A}$ is called a *cyclic permutation automaton* of order r if there exists an $x \in X$ cyclic permutation sign.

The congruence ρ of the automaton $\mathbf{A} = (A, X, \delta)$ is called *uniform* if, for every $a, b \in A$, $|\rho[a]| = |\rho[b]|$.

Lemma 6 *Every congruence of a strongly connected permutation automaton is uniform.*

Proof. Let $\mathbf{A} = (A, X, \delta)$ be a strongly connected permutation automaton. Assume that ρ is a congruence of $\mathbf{A}$ and $a, b \in A$ arbitrary states. Since $\mathbf{A}$ is strongly connected, there are $p, q \in X^*$ such that $b = ap$ and $a = bq$. Then $\rho[a]p \subseteq \rho[b]$ and $\rho[b]q \subseteq \rho[a]$. As every input sign is a permutation sign, we get

$$|\rho[a]| = |\rho[a]p| \leq |\rho[b]| = |\rho[b]q| \leq |\rho[a]|,$$

that is, $|\rho[a]| = |\rho[b]|$. ■

From Lemma 6 it follows that every strongly connected permutation automaton of prime order is simple. By the following example this is generally not true.

Example 1 *If* $A = \{1, 2, 3\}$, $X = \{x, y\}$ *and*

$$1x = 2x = 3,\ 3x = 2,\ 1y = 2,\ 2y = 1,\ 3y = 1,$$

then the automaton $\mathbf{A} = (A, X, \delta)$ *is strongly connected of prime order, but not simple.*

By the following example, there is a simple strongly connected permutation automaton whose order is not a prime number.

Example 2 $A = \{1, 2, 3, 4\}$, $X = \{x, y\}$ *and*

$$1x = 2,\ 2x = 3,\ 3x = 4,\ 4x = 1,\ 1y = 1,\ 2y = 2,\ 3y = 4,\ 4y = 3.$$

The automaton $\mathbf{A} = (A, X, \delta)$ *is a cyclic permutation automaton.*

Theorem 6 *The commutative automaton* $\mathbf{A} = (A, X, \delta)$ *with at least three states is simple if and only if it is a cyclic permutation automaton of prime order.*

Proof. Assume that the commutative automaton $\mathbf{A}$ is simple. By Theorem 5, $\mathbf{A}$ is an A-finite automaton of prime order. By Corollary 6 and Theorem 4, $\mathbf{A}$ is strongly connected. Let $x \in X$ be an arbitrary input sign. Define the binary relation ρ_x on A as follows.

$$(a, b) \in \rho_x \quad \text{if and only if} \quad ax = bx.$$

Using the commutativity of $\mathbf{A}$, it is not difficult to seen that the relation ρ_x is a congruence of $\mathbf{A}$. If $\rho_x = \omega_A$ then there is an element $c \in A$ such that for every $a \in A$ $ax = c$. Hence c is a trap of $\mathbf{A}$. It is impossible. Thus $\rho_x = \iota_A$, that is, x is a permutation sign. We get that $\mathbf{A}$ is a permutation automaton. Since $\mathbf{A}$ strongly connected and $3 \leq |A|$, there are $a \in A$ and $x \in X$ such that $ax \neq a$. But x is a permutation sign. Therefore, if $ax^i = ax^j$ $(0 \leq i < j)$ then $a = ax^{j-i}$ and $2 \leq j - i$. Let k be the smallest positive integer for which $ax^k = a$. Since $ax \neq a$, therefore $2 \leq k$. The set $H = \{a, ax, \ldots, ax^{k-1}\}$ is a separator of $\mathbf{A}$. From this it follows that $H = A$. Thus x is a cyclic permutation sign, that is, $\mathbf{A}$ is a cyclic permutation automaton of prime order.

Conversely, if $\mathbf{A}$ is a cyclic permutation automaton of prime order then, by Lemma 6, $\mathbf{A}$ is simple. ■

If a commutative automaton is a cyclic permutation automaton of prime order then every input sign is an identical permutation sign or a cyclic permutation sign.

We remark that in [16] G. Thierrin proved that if $G(\mathbf{A}) \neq \{\iota_A\}$, for a simple automaton $\mathbf{A}$, then $\mathbf{A}$ is a permutation automaton, $|G(\mathbf{A}| = |A|$ and $|G(\mathbf{A})|$ is a prime number. By Theorem 5, every commutative simple automaton is A-finite. By the following examples, it is generally not true.

Example 3 *If* $A = \{1, 2, \ldots, n, \ldots\}$, $X = \{x, y\}$ *and*

$$1y = 1,\ 2y = 2,\ nx = n + 1,\ n = 1, 2, \ldots,$$

$$n_1 = 2, \quad n_{i+1} = n_i + i, \quad i = 1, 2, \ldots,$$

$$n_{i+1}y = 1,\ (n_{i+1} + 1)y = (n_{i+1} + 2)y = \cdots = (n_{i+1} + i)y = 2,\ i = 1, 2, \ldots,$$

then the infinite automaton $\mathbf{A} = (A, X, \delta)$ *is strongly connected, simple and not commutative.*

Example 4 *If* $A = \{0, 1, 2, \ldots, n, \ldots\}$, $X = \{x, y\}$ *and*

$$0x = 0y = 1y = 0,\ nx = n + 1,\ n = 1, 2, \ldots,$$

$$n_1 = 2, \quad n_{i+1} = n_i + i, \quad i = 1, 2, \ldots,$$

$$n_i y = 1,\ (n_{i+1}+1)y = (n_{i+1}+2)y = \cdots = (n_{i+1}+i)y = 2,\ i = 1, 2, \ldots,$$

then the infinite automaton $\mathbf{A} = (A, X, \delta)$ *is strongly trap-connected with the trap* 0*, simple and not commutative.*

References

[1] Babcsányi, I., *A félperfekt kváziautomaták* (*On quasiperfect quasiautomata*), Mat. Lapok, 21 (1970), 95-102 (Hungarian with English summary).

[2] Babcsányi, I., *Rees automaták* (*Rees-automata*), Mat. Lapok, 29 (1977-1981), 139-148 (Hungarian with English summary).

[3] Babcsányi, I., *Simple Mealy and Moore automata*, Proceedings of the International Conference on Automata and Formal Languages IX, Vasszécseny, Hungary, August 9-13, 1999, Publicationes Mathematicae, Supplementum 60 (2002), 473-482.

[4] Babcsányi, I. *Equivalence of Mealy and Moore automata*, Acta Cybernetica 14 (2000), 541-552.

[5] Cohn, P.M., *Universal Algebra*, Harper and Roow Publishers, New York-Evanston-London, 1965.

[6] Ésik Z. and B. Imreh, *Remarks on finite commutative automata*, Acta Cybernetica, 5 (1981), 143-146.

[7] Gécseg, F., *Products of Automata*, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1981.

[8] Gécseg, F. and I. Peák, *Algebraic Theory of Automata*, Akadémiai Kiadó, Budapest, 1972.

[9] Grillet, A.P., *Commutative semigroups with finite congruence lattices*, Acta Sci. Math.(Szeged), 70 (2004), 551-555.

[10] Kim, K.H. and F.W. Roush, *Applied Abstract Algebra*, John Wiley and Sons, New York-Chichester-Brisbane-Ontario, 1983.

[11] Lallement, G., *Semigroups and Combinatorial Applications*, John Wiley and Sons, New York-Chichester-Brisbane-Toronto, 1979.

[12] Lex, W., *Akte* (*Acts*), Habilitationsschift, Clausthal-Zellerfeld, 1980 (German).

[13] Oehmke, R.H., *On the structures of an automaton and its input semigroup*, J. Assoc. Comp. Machinery, 10 (1963), 521-525.

[14] Peák, I., Avtomatü i polugruppü II (*Automata and semigroups II*), Acta Sci. Math.(Szeged), 26 (1965), 49-54 (Russian).

[15] Radeleczki, S., *The automorphism group of unary algebras*, Mathematica Pannonica, 7 (1996), 253-271.

[16] Thierrin, G., *Simple automata*, Kybernetika (Pragua), 5 (1970), 343-350.