Automata with Finite Congruence Lattices

István Babcsányi†

To the memory of Balázs Imreh

Abstract

In this paper we prove that if the congruence lattice of an automaton \( A \) is finite then the endomorphism semigroup \( E(A) \) of \( A \) is finite. Moreover, if \( A \) is commutative then \( A \) is \( A \)-finite. We prove that if \( 3 \leq |A| \) then a commutative automaton \( A \) 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 \( A = (A, X, \delta) \) 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 \( A \) is called \( A \)-finite if \( |A| < \infty \). If \( |A| = n \) then we say that \( n \) is the order of \( A \) and if \( n \) is a prime then \( A \) is an automaton of prime order. The input monoid [semigroup] \( X^* [X^+] \) of \( A \) is the free monoid [semigroup] over \( X \). The transition function \( \delta : A \times X \rightarrow A \) 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 \( \delta(a, p) \).

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

An equivalence relation \( \rho \) of state set \( A \) of the automaton \( A \) is called a congruence on \( A \) if

\[
(a, b) \in \rho \implies (ax, bx) \in \rho,
\]

for all \( a, b \in A \) and \( x \in X \). The \( \rho \)-class of \( A \) containing the state \( a \) is denoted by \( \rho[a] \). Denote \( C(A) \) the congruence lattice of \( A \). Let \( \iota_A [\omega_A] \) be the equality [universal] relation on \( A \). The automaton \( A \) is called simple if \( C(A) = \{\iota_A, \omega_A\} \).

It is evident that if \( |A| \leq 2 \) then \( A \) is simple.

*Research supported by the Hungarian NFSR grant No 67639.
†Department of Algebra, Mathematical Institute, Budapest University of Technology and Economics, 1111 Budapest, Egry József u. 1, Hungary. E-mail: babcs@math.bme.hu
The automaton $A' = (A', X, \delta')$ is a subautomaton of the automaton $A = (A, X, \delta)$ if $A' \subseteq A$ and $\delta'$ is the restriction of $\delta$ 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 $A$ induced by $A'$ ([2]). The set $R(A)$ of Rees congruences of $A$ is a sublattice of $C(A)$. It is called the Rees congruence lattice of $A$.

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

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

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


## 2 Automata with finite congruence lattices

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

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

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

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

**Corollary 2.** 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 proved 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 3.** If the congruence lattice \( C(A) \) of an automaton \( A = (A, X, \delta) \) is finite then the endomorphism semigroup \( E(A) \) is finite.

**Proof.** First, we show that the automorphism group \( G(A) \) is finite. Assume that the order of \( \alpha \in G(A) \) is infinite. For every positive integer \( m \), we define the binary relation \( \rho_{\alpha m} \) 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

\[
a = \alpha^i m(c), \quad b = \alpha^i m(c).
\]

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

Let \( r \) be the order of \( \alpha \in G(A) \). Take the binary relation \( \rho_{\alpha} \) on \( A \) for which

\[
(a, b) \in \rho_{\alpha}(c) \quad \text{if and only if there are} \quad c \in A \quad \text{and integers} \quad 0 \leq i, j \leq r - 1 \quad \text{such that} \quad a = \alpha^i(c), \quad b = \alpha^j(c).
\]

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

\[
\rho_{\alpha} = \rho_{\beta}, \quad \beta \in G(A).
\]

By Corollary 2, the automaton \( A \) is finitely generated. If \( \{c_1, c_2, \ldots, c_k\} \) is a finite generating set of \( A \) then

\[
\rho_{\beta}[c_1] = \rho_{\alpha}[c_1], \quad \rho_{\beta}[c_2] = \rho_{\alpha}[c_2], \ldots, \rho_{\beta}[c_k] = \rho_{\alpha}[c_k],
\]

that is,

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

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

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

\[
\ker \beta = \ker \alpha \quad \text{and} \quad \beta(A) = \alpha(A).
\]
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 \( \text{Ker} \beta = \text{Ker} \alpha \), \( \varphi_{\alpha,\beta} \) 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, \( \varphi_{\alpha,\beta} \in G(A_\alpha) \). By Lemma 1, \( C(A_\alpha) \) is finite and thus, by the first part of this proof, \( G(A_\alpha) \) is finite. Furthermore, if
\[
\text{Ker} \beta = \text{Ker} \beta' = \text{Ker} \alpha, \quad \beta(A) = \beta'(A) = \alpha(A)
\]
and
\[
\varphi_{\alpha,\beta} = \varphi_{\alpha,\beta'},
\]
then \( \beta = \beta' \). Thus, for arbitrary \( \alpha \in E(A) \), the number of \( \beta \in E(A) \) such that \( \text{Ker} \beta = \text{Ker} \alpha \) and \( \beta(A) = \alpha(A) \) is finite. Since the number of different \( \text{Ker} \alpha \)'s and different \( \beta(A) \)'s \( (\alpha, \beta \in E(A)) \) is finite, \( E(A) \) is also finite.

For every \( a \in A \), consider the binary relation \( \rho_{A,a} \) on \( X^* \) defined as
\[
(p, q) \in \rho_{A,a} \iff ap = aq \quad (p, q \in X^*).
\]
It is clear that \( \rho_{A,a} \) \((a \in A)\) is a right congruence on \( X^* \). The relation \( \rho_A = \bigcap_{a \in A} \rho_{A,a} \) is congruence on \( X^* \). The characteristic semigroup \( S(A) \) of the automaton \( A \) is the factor semigroup \( X^*/\rho_A \).

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

**Lemma 4.** For every cyclic automaton \( A = (A, X, \delta) \),
\[
|E(A)| \leq |A| \leq |S(A)|.
\]

**Proof.** If \( a_0 \) is a generating element of \( A \) and \( \alpha(a_0) = \beta(a_0) \) \((\alpha, \beta \in E(A))\) then, for every \( p \in X^* \),
\[
\alpha(a_0p) = \alpha(a_0)p = \beta(a_0)p = \beta(a_0p),
\]
that is, \( \alpha = \beta \). Thus the mapping \( \varphi : E(A) \to A \) such that \( \varphi(\alpha) = \alpha(a_0) \), for every \( \alpha \in E(A) \), is an injective mapping of \( E(A) \) into \( A \). This means that \( |E(A)| \leq |A| \).

If \( aop \neq aq \) \((p, q \in X^*)\) then \( \rho_A[p] \neq \rho_A[q] \). From this it follows that \( |A| \leq |S(A)| \).

**Lemma 5.** If the relation \( \rho_{A,a_0} \) is a congruence on \( X^* \), for a generating element \( a_0 \) of a cyclic automaton \( A = (A, X, \delta) \), then \( E(A) \cong S(A) \) and \( |E(A)| = |A| \).
Proof. If the relation $\rho_{A,a_0}$ is a congruence on $X^*$ then $\rho_{A,a_0} = \rho_A$. Define the mapping $\alpha_p : A \rightarrow A$, for every $p \in X^*$, such that

$$\alpha_p(a_0q) = a_0pq \quad (q \in X^*)$$

It can easily be shown that $\alpha_p \in E(A)$. Furthermore, if $\alpha \in E(A)$ and $\alpha(a_0) = a_0r$ ($r \in X^*$) then $\alpha = \alpha_r$. The mapping $\varphi : E(A) \rightarrow S(A)$ such that

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

is an isomorphism of $E(A)$ onto $S(A)$. By Lemma, $|E(A)| = |A|$. □

From Theorem 3, Lemma 4 and Lemma 5, we get the following corollary.

Corollary 6. Let the congruence lattice $C(A)$ of the cyclic automaton $A = (A, X, \delta)$ be finite. If the relation $\rho_{A,a_0}$ is a congruence on $X^*$, for a generating element $a_0$, then $A$ is $A$-finite.

The automaton $A$ 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. Péák proved in [14] that $E(A) \cong S(A)$ and $|E(A)| = |A|$ for arbitrary cyclic commutative automaton $A$. (See also F. Gécseg and I. Péák [8], Z. Ésik and B. Imreh [6].) The statement of Lemma 5 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 7. If the congruence lattice $C(A)$ of a commutative automaton $A = (A, X, \delta)$ is finite then the automaton $A$ is $A$-finite.

Proof. By Corollary 2, $A$ is finitely generated. Then, it is a union of commutative cyclic subautomata $A_i = (A_i, X_i, \delta_i)$ ($i = 1, 2, \ldots, n$). But, if $a_i \in A_i$ is a generating element of $A_i$, then $\rho_{A_i,a_i}$ is a congruence on $X^*$, since $A_i$ ($i = 1, 2, \ldots, n$) is commutative. By Corollary 6, $A_i$ ($i = 1, 2, \ldots, n$) is $A$-finite and thus $A$ 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 $A = (A, X, \delta)$ without outputs. In this case $C(A) = \{\iota_A, \omega_A\}$.

Let $H \neq \emptyset$ be a subset of the state set $A$ and let $H_p = \{ap; a \in H\}$ for every $p \in X^*$. Define the binary relation $\tau_H$ 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 $p \in X^*$. $\tau_H$ is a congruence of $A$ and $H$ is a union of certain $\tau_H$-congruence classes. The state $a \in A$ is called disjunctive, if $\tau(a) = \iota_A$.  

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

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

The one-element subsets of $A$ and itself $A$ are separators of $A$. We say that these separators are the trivial separators.

**Lemma 8.** The automaton $A = (A, X, \delta)$ is simple if and only if every separator of $A$ is trivial.

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

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

If every state of an automaton $A = (A, X, \delta)$ is a generating element of $A$ then we say that $A$ is strongly connected. In other words, $A$ 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 $A$. The automaton $A$ 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 $A$ is strongly connected if and only if it has no subautomaton $A' = (A', X, \delta)$ of $A$ such that $A' \neq A$. Furthermore, if $A$ strongly trap-connected then it has only one trap.

**Corollary 9** (G. Thierrin [16]). Every simple automaton with at least three states is strongly connected or strongly trap-connected.

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

**Theorem 10.** The strongly trap-connected automaton $A = (A, X, \delta)$ with at least three states is simple if and only if the trap of $A$ is disjunctive.

**Proof.** Let $c \in A$ be the trap of $A$. First, we show that if $\rho$ is a congruence of $A$ 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 $A$. 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 $A$ is simple.
Conversely, assume that $A$ is simple. But $A$ is strongly trap-connected automaton with at least three states, thus $τ(τ) ≠ ω_A$. Therefore $τ(τ) = τ_A$ and so $c$ is disjunctive.

\[\text{□}\]

4 Commutativity of simple automata

**Theorem 11.** If the strongly trap-connected automaton $A = (A, X, δ)$ with at least three states is simple then it is not commutative. Furthermore $G(A) = \{τ_A\}$ and $E(A) = \{τ_A, α_c\}$, where $c$ is the trap of $A$, and $α_c$ defined by $α_c(a) = c (a ∈ A)$.

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

\[bp = aqp = apq \quad \text{and} \quad ap = bpr = bpr.\]

Then, $ap = c$ if and only if $bp = c$. Thus $(a, b) ∈ τ(c)$, that is, $a = b$, which contradicts the assumption. We get that $A$ is not commutative.

It is evident that $α_c ∈ E(A)$. If $α ∈ E(A)$ then, for every $p ∈ X^*$,

\[α(c)p = α(cp) = α(c),\]

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

\[α(ap) = α(a)p = cp = c,\]

that is, $α = α_c$. Assume that $a, b ∈ A - \{c\}$, $a ≠ b$ and $α(a) = α(b)$. If, for every $p ∈ X^*$, $ap = c$ if and only if $bp = c$ then $(a, b) ∈ τ(c)$. By Theorem 10, $a = b$. This is a contradiction. Thus there exists a $q ∈ X^*$ such that for instance $aq = c$ and $bq ≠ c$. Then

\[α(bq) = α(b)q = α(a)q = α(aq) = α(c) = c.\]

From this it follows that $α = α_c$, thus $G(A) = \{τ_A\}$ and $E(A) = \{τ_A, α_c\}$. \[\text{□}\]

**Lemma 12.** Every endomorphism of a strongly connected automaton is surjective.

**Proof.** Let $A = (A, X, δ)$ be a strongly connected automaton. If $α ∈ E(A)$ then $A_α = (α(A), X, δ')$ is a subautomaton of $A$. Therefore, $α(A) = A$, that is, $α$ is a surjective mapping. \[\text{□}\]

**Theorem 13.** Let the strongly connected automaton $A = (A, X, δ)$ with at least three states be simple. If $E(A) = \{τ_A\}$ then $A$ is not commutative. If $E(A) ≠ \{τ_A\}$ then $A$ is an $A$-finite commutative automaton, $|E(A)| = |A|$ and $E(A) = G(A)$ is a cyclic group of prime order.

**Proof.** First, we show that if the strongly connected automaton $A$ with at least three states is simple then $E(A) = G(A)$ is a finite group. Since $Kerα (α ∈ E(A))$ is a congruence of $A$, $Kerα = τ_A$ or $Kerα = ω_A$. By Lemma 12, $α$ is surjective.
mapping. From this it follows that $\text{Ker} \alpha = \iota_A$ and thus $\alpha \in G(A)$. This means that $E(A) = G(A)$. By Theorem 3, $E(A)$ is finite.

Assume that $E(A) = \{\iota_A\}$ and $A$ is commutative. Since $A$ is strongly connected, there are $a_0 \in A$ and $p \in X^*$ such that $a_0 \neq a_0 p$. Define the mapping $\alpha_p$ in the same way as in the proof of Lemma 5. Since the relation $\rho_A, a_0$ is a congruence on $X^*$, $\alpha_p \in E(A)$ and $\alpha_p \neq \iota_A$. This is impossible, and so $A$ is not commutative.

Now assume that $E(A) = G(A) \neq \{\iota_A\}$. Let $\alpha \in G(A)$ and $\alpha \neq \iota_A$. Consider the congruence $\rho_\alpha$ defined in the proof of Theorem 3. Since $A$ 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 $\beta \in G(A)$ 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

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

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

We show that $A$ 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 $0 \leq i \leq r - 1$,

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

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

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

that is, $A$ is commutative.

By Theorem 7, the automaton $A$ is A-finite. By Lemma 4 and Lemma 5, $|E(A)| = |A|$.

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

The automaton $A = (A, X, \delta)$ 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 $A$ 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 $A$ is called a cyclic permutation automaton of order $r$ if there exists an $x \in X$ cyclic permutation sign.

The congruence $\rho$ of the automaton $A = (A, X, \delta)$ is called uniform if, for every $a, b \in A$, $|\rho[a]| = |\rho[b]|$. 
Lemma 14. Every congruence of a strongly connected permutation automaton is uniform.

Proof. Let $A = (A, X, \delta)$ be a strongly connected permutation automaton. Assume that $\rho$ is a congruence of $A$ and $a, b \in A$ arbitrary states. Since $A$ 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 14 it follows that every strongly connected permutation automaton of prime order is simple. By the following example this is generally not true.

Example 15. If $A = \{1, 2, 3\}$, $X = \{x, y\}$ and

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

then the automaton $A = (A, X, \delta)$ 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 16. $A = \{1, 2, 3, 4\}$, $X = \{x, y\}$ and

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

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

Theorem 17. The commutative automaton $A = (A, X, \delta)$ 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 $A$ is simple. By Theorem 13, $A$ is an $A$-finite automaton of prime order. By Corollary 9 and Theorem 11, $A$ is strongly connected. Let $x \in X$ be an arbitrary input sign. Define the binary relation $\rho_x$ on $A$ as follows.

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

Using the commutativity of $A$, it is not difficult to seen that the relation $\rho_x$ is a congruence of $A$. 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 $A$. It is impossible. Thus $\rho_x = \iota_A$, that is, $x$ is a permutation sign. We get that $A$ is a permutation automaton. Since $A$ 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 small 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 $A$. From this it follows that $H = A$. Thus $x$ is a cyclic permutation sign, that is, $A$ is a cyclic permutation automaton of prime order.

Conversely, if $A$ is a cyclic permutation automaton of prime order then, by Lemma 14, $A$ 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 $G(A) \neq \{\iota_A\}$, for a simple automaton $A$, then $A$ is a permutation automaton, $|G(A)| = |A|$ and $G(A)$ is a prime number. By Theorem 13, every commutative simple automaton is $A$-finite. By the following examples, it is generally not true.

**Example 18.** If $A = \{1, 2, \ldots, n, \ldots\}, \ X = \{x, y\}$ and

- $1y = 1, \ 2y = 2, \ nx = n + 1, \ n = 1, 2, \ldots,$
- $n_1 = 2, \ n_{i+1} = n_i + i, \ i = 1, 2, \ldots,$
- $n_{i+1}y = 1, \ (n_{i+1} + 1)y = (n_{i+1} + 2)y = \cdots = (n_{i+1} + i)y = 2, \ i = 1, 2, \ldots,$

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

**Example 19.** If $A = \{0, 1, 2, \ldots, n, \ldots\}, \ X = \{x, y\}$ and

- $0x = 0y = 1y = 0, \ nx = n + 1, \ n = 1, 2, \ldots,$
- $n_1 = 2, \ n_{i+1} = n_i + i, \ i = 1, 2, \ldots,$
- $ny = 1, \ (n_{i+1} + 1)y = (n_{i+1} + 2)y = \cdots = (n_{i+1} + i)y = 2, \ i = 1, 2, \ldots,$

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

**References**


*Received February, 2007*