Remarks on finite commutative automata

By Z. ÉSIK and B. IMREH

A. C. Fleck has proved in [1] that a strongly connected commutative quasi-automaton — called perfect quasi-automaton in [2] — is directly irreducible if and only if its characteristic semigroup, which is actually an Abelian group, is directly irreducible. I. Peák generalized this result for commutative cyclic automata (cf. [4]). In this paper we point out that this connection between automata and their characteristic semigroups is based on the fact that the congruence lattice of a commutative cyclic automaton is isomorphic to the congruence lattice of its characteristic semigroup. Furthermore, we give a characterization of strongly connected commutative automata through their corresponding algebraic structures. Finally, we employ these results to obtain isomorphically complete systems for the class of all strongly connected commutative automata with respect to the direct product and quasi-direct product.

By an automaton $\mathbf{A}=(A, X, \delta)$ we always mean a finite automaton. Isomorphisms of automata are A-isomorphisms. For arbitrary automaton $\mathbf{A}$ we denote by $C(\mathbf{A})$ and $C(S(\mathbf{A}))$ the congruence lattices of $\mathbf{A}$ and its characteristic semigroup,* respectively. Otherwise we use the terminology and notations in accordance with [2].

Theorem 1. The following three conditions are satisfied for arbitrary commutative cyclic automaton $\mathbf{A}=(A, X, \delta)$:

(i) $S(\mathbf{A}) \cong E(\mathbf{A})$,

(ii) $|A| = |E(\mathbf{A})|$,

(iii) $C(\mathbf{A}) \cong C(S(\mathbf{A}))$.

Proof. The validity of (i) and (ii) was already proved by I. Peák in [4]. The proof of this fact is based on the observation that every commutative cyclic automaton $\mathbf{A}$ is a free commutative automaton generated by one of its states. In other words, $\mathbf{A}$ is a free commutative unoid in the equational class generated by $\mathbf{A}$ and each generator of $\mathbf{A}$ is a free generator of $\mathbf{A}$. This means that if $a_0 \in A$ generates the automaton $\mathbf{A}$ then every correspondence $a_0 \to a (\in A)$ has a unique A-homomorphic extension of $\mathbf{A}$ into itself. By Corollary to Theorem 24.2 in [3] this implies that $\mathbf{A}' \cong \mathbf{A}$ where $\mathbf{A}'=(S(\mathbf{A}), X, \delta')$ and δ' is defined by $\delta'(C_\varrho(p), x)=C_\varrho(px)$.

* By the characteristic semigroup $S(\mathbf{A})$ of an automaton $\mathbf{A}$ we always mean a monoid with identity $C_\varrho(\lambda)$, where λ denotes the empty word.

Indeed, if a_0 denotes an arbitrary generator of A then a natural isomorphism can be given by the correspondence $C_\varrho(p)\to\delta(a_0, p)$ $(C_\varrho(p)\in S(\mathbf{A}))$. Therefore $C(\mathbf{A})\cong\cong C(\mathbf{A}')$. On the other hand $C(\mathbf{A}')\cong C(\mathbf{A}'')$ where the automaton A″ is the semigroup-automaton corresponding to A′ with transition $\delta''(C_\varrho(p), C_\varrho(q))=C_\varrho(pq)$. It is evident that each congruence relation of the semigroup $S(\mathbf{A})$ is a congruence relation of the semigroup-automaton A″ as well. The converse follows by the commutativity of $S(\mathbf{A})$. Thus $C(\mathbf{A}'')\cong C(S(\mathbf{A}))$. Putting together these isomorphisms we get $C(\mathbf{A})\cong C(S(\mathbf{A}))$. This ends the proof of Theorem 1.

It is interesting to note that I. Peák gave an example in [4] for a commutative automaton which is not cyclic but satisfies conditions (i) and (ii) of Theorem 1. It is not difficult to see that this example does not satisfy (iii). We now give another automaton which contents each of the conditions (i)—(iii) of Theorem 1 and which is not cyclic. This automaton is the following $\mathbf{A}=(\{1, 2, 3, 4\}, \{x, y\}, \delta)$, where δ is defined by the table below:

	1	2	3	4
x	1	2	3	2
y	2	3	3	3

Thus the converse of Theorem 1 is not true in general. However, in spite of the previous example, in case of strongly connected commutative automata, we have succeeded in proving a certain converse of Theorem 1.

Theorem 2. An automaton $\mathbf{A}=(A, X, \delta)$ is strongly connected and commutative if and only if each of the following conditions is satisfied by A:

(i) $S(\mathbf{A})$ is an Abelian group,

(ii) $S(\mathbf{A}) \cong E(\mathbf{A})$,

(iii) $|A| = |E(\mathbf{A})|$,

(iv) $C(\mathbf{A}) \cong C(S(\mathbf{A}))$.

Proof. Necessity follows by Theorem 1. Conversely, the commutativity of A is immediate by (i). In order to prove that A is strongly connected first observe that since (ii) is also satisfied by A there is a natural isomorphism ν of $S(\mathbf{A})$ onto $E(\mathbf{A})$. This isomorphism is defined in the following manner: $\nu(C_\varrho(p))$ is the mapping induced by the word p on the set of states of A. In other words, $\nu(C_\varrho(p))$ is simply the polynomial induced by p in the automaton A being considered as a unoid.

Assume to the contrary A is not strongly connected. As $S(\mathbf{A})$ is a group we can decompose A into the direct sum of its strongly connected subautomata $\mathbf{A}_t==(A_t, X, \delta_t)$ $(t=1, \ldots, n, n>1)$. According to the previously established natural isomorphism ν, the inclusion $\varphi(A_t)\subseteq A_t$ $(t=1, \ldots, n)$ is satisfied for any $\varphi\in E(\mathbf{A})$. Consequently, $|A_t|>1$ $(t=1, \ldots, n)$ and $\prod_{t=1}^{n} E(\mathbf{A}_t)\cong E(\mathbf{A})$ under the mapping $\varphi\to(\varphi_{|A_1}, \ldots, \varphi_{|A_n})$. Thus, by Theorem 1 and our assumption (iii), $\prod_{t=1}^{n} |A_t|==\prod_{t=1}^{n} |E(\mathbf{A}_t)|=|E(\mathbf{A})|=|A|=\sum_{t=1}^{n} |A_t|$.

It is not difficult to see by $|A_t|>1$ $(t=1, \ldots, n)$ that the above equality is possible only if $n=2$ and $|A_1|=|A_2|=2$. In this case $C(\mathbf{A})$ contains the chain induced by the compatible partitions

$$C_0 = \{\{a_{11}\}, \{a_{12}\}, \{a_{21}\}, \{a_{22}\}\},$$
$$C_1 = \{A_1, \{a_{21}\}, \{a_{22}\}\},$$
$$C_2 = \{A_1, A_2\},$$
$$C_3 = \{A\},$$

where $A_t=\{a_{t1}, a_{t2}\}$ $(t=1, 2)$. On the other hand $S(\mathbf{A})$ can contain only shorter chains. This is a simple consequence of the well-known fact that the congruence lattice of an Abelian group is isomorphic to the lattice of its subgroups.

COROLLARY. The following conditions are equivalent for every strongly connected commutative automaton $\mathbf{A}=(A, X, \delta)$:

(i) $\mathbf{A}$ is subdirectly irreducible,

(ii) $\mathbf{A}$ is directly irreducible,

(iii) $S(\mathbf{A})$ is a cyclic group of prime-power order,

(iv) The cardinality of A is a prime-power and there is an input-sign $x\in X$ inducing a cyclic permutation of A.

Proof. The equivalence of (i), (ii) and (iii) is a consequence of Theorem 2 and the Fundamental Theorem of Finite Abelian Groups. The implication (iv)⇒(iii) is trivial. It remains to prove that (iii)⇒(iv).

In the proof of Theorem 1 we have shown that $\mathbf{A}\cong\mathbf{A}'$ therefore, $|A|$ is a prime-power, say $|A|=r^n$. Assume that none of the signs $x\in X$ induces a cyclic permutation of A. Then, for each $x\in X$, the order of $C_\varrho(x)$ in $S(\mathbf{A})$ is less than r^n. But this yields a contradiction since for arbitrary word $p=x_1\ldots x_k$ the order of $C_\varrho(p)$ can not exceed the maximum of the orders of the signs $x_1, \ldots, x_k$, which completes the proof of the Corollary.

It is evident that the automata given in (iv) form a minimal isomorphically complete system of strongly connected commutative automata with respect to the direct product for any fixed set of input signs X. We proceed by stating a similar result with respect to the quasi-direct product.

Let $n(>1)$ be an arbitrary natural number and let $\mathbf{M}_n=(\{0, \ldots, n-1\}, \{x_0, \ldots, x_{n-1}\}, \delta_n)$ denote the automaton with transition $\delta_n(j, x_s)=j+s \pmod n$ $(j\in\{0, \ldots, n-1\}, x_s\in\{x_0, \ldots, x_{n-1}\})$. Let $\mathfrak{K}$ consist of all automata $\mathbf{M}_n$ where $n>1$ and n is a prime-power.

Theorem 3. A system Σ of automata is isomorphically complete for the class of all strongly connected commutative automata with respect to the quasi-direct product if and only if each $\mathbf{M}_n\in\mathfrak{K}$ can be embedded isomorphically into a quasi-direct product of an automaton $\mathbf{A}\in\Sigma$ with a single factor.

Proof. Sufficiency is obvious. In order to prove necessity let $\mathbf{M}_n\in\mathfrak{K}$ be arbitrary. $\mathbf{M}_n$ can be embedded isomorphically into a quasi-direct product of automata from Σ, and hence it can be embedded isomorphically into a direct product whose each component is a quasi-direct product of an automaton from Σ with a single factor. But, by Corollary to Theorem 2, $\mathbf{M}_n$ is subdirectly irreducible. Therefore $\mathbf{M}_n$ can be embedded isomorphically into a quasi direct product of an automaton from Σ with a single factor.

COROLLARY. There exists no system of automata which is isomorphically complete for the class of all strongly connected commutative automata with respect to the quasi-direct product and minimal.

Proof. It is easy to show that the class $\mathfrak{K}\setminus\{M_{r^t} \mid t \leq s\}$ constitutes a complete system for any fixed prime r and integer s.

DEPT. OF COMPUTER SCIENCE
A. JÓZSEF UNIVERSITY
ARADI VÉRTANÚK TERE 1.
SZEGED, HUNGARY
H—6720

References

[1] FLECK, A. C., Isomorphism groups of automata, *J. Assoc. Comput. Mach.*, v. 9, 1962, pp. 469—476.
[2] GÉCSEG, F. and I. PEÁK, *Algebraic theory of automata*, Akadémia Kiadó, Budapest, 1972.
[3] GRÄTZER, G., *Universal algebra*, Van Nostrand, Princeton, N. J., 1968.
[4] PEÁK, I., Автоматы и полугруппы, II., *Acta Sci. Math. (Szeged)*, v. 26, 1965, pp. 49—54.

(Received March 25, 1980)