JOURNAL OF COMPUTER AND SYSTEM SCIENCES 7, 300–305 (1973)

A Structure Theory of Automata Characterized by Groups

YOSHIFUMI MASUNAGA AND SHOICHI NOGUCHI

Research Institute of Electrical Communication, Tohoku University, Sendai 980, Japan

AND

JURO OIZUMI

Research Center of Applied Information Sciences, Tohoku University, Sendai 980, Japan

Received March 24, 1972

The structure of a strongly connected permutation automaton, a quasiperfect automaton, and a perfect automaton are discussed algebraically using group theory. A characterization theorem for the three classes of automata, a condition for direct product decomposability of a strongly connected permutation automaton, and some other related results are proposed in this paper.

1. INTRODUCTION

There are many articles discussing the structure of automata algebraically. In Fleck's first article [1], an automorphism group of an automaton is introduced, and it is shown that direct product decomposability of a "perfect" automaton is equivalent to that of its automorphism group. Trauth [2] extends the discussion to a "quasiperfect" automaton and gives analogous results under a stronger condition. The same results are also given in Fleck [3]. Bayer [4] defines a "total" automaton, which is equivalent to a quasiperfect automaton, and gives a characterization of homomorphisms of that automaton. Extended discussions are also made in [5, 6].

On the other hand, an "input semigroup associated with an automaton" is introduced by Weeg [7], and relationships between an associated input semigroup and an automorphism group of an automaton are discussed by Arbib [9], Oehmke [10], and others. It is also shown that the associated input semigroup of perfect and quasiperfect automata forms a group respectively [1, 2].

Now, an automaton with associated input "group" is said to be "group-type," and it is easily proved that a strongly connected automaton is group-type if and only if it is a "permutation" automaton. So the classes of perfect and quasiperfect automata are proper subclasses of the strongly connected permutation one.

In Section 2 of this paper, a condition for one-to-one correspondence between all the homomorphisms and all the subgroups of an automorphism group is established in the strongly connected case. In Section 3, a characterization theorem for the three classes of automata is given. In the last section, a necessary and sufficient condition for a strongly connected permutation automaton to be decomposed into a direct product of automata is given as a condition for an input group to be satisfied.

2. Homomorphisms of Automata

An automaton is a three-tuple $A = (Q, M, I)$, where Q is a nonempty set of states, I is an input semigroup and $M: Q \times I \to Q$ is a next state function.

Let $G(A)$ be an automorphism group of A, and H be a subgroup of $G(A)$. Then a quotient automaton A/H of A mod H is defined using the congruence relation on Q induced by H, which is a homomorphic image of A [3]. That is, a subgroup of $G(A)$ induces a homomorphism of A. But usually, not every homomorphism of an automaton can be induced by a subgroup in this sense [11, 12].

A is said to be "transitive with respect to a subgroup H of $G(A)$" if $\forall q, q' \in Q$, $\exists h \in H$, $q' = h(q)$. A strongly connected automaton with a transitive automorphism group is called quasiperfect according to Trauth [2].

Let A be quasiperfect and η be a homomorphism of it. Define

$$H = \{h \in G(A) \mid \eta(h(q_0)) = \eta(q_0)\}$$

for some fixed q_0 in Q. Then H forms a subgroup of $G(A)$ and the homomorphic image A/η of A under η is isomorphic to A/H.

Then a homomorphism of A induces a subgroup of $G(A)$ and vice versa when A is quasiperfect.

Proposition 2.1. *An automaton B is a homomorphic image of a quasiperfect automaton A if and only if there exists a subgroup H of $G(A)$ such that B is isomorphic to A/H.*

We can find the same result in [11], since a right regular automaton of a group is equivalent to a quasiperfect one [4].

For a strongly connected automaton, a stronger version of this proposition can be obtained.

Theorem 2.1. *Let A be a strongly connected automaton. The following two statements are equivalent: (i) All the homomorphisms of A are induced by the subgroups of $G(A)$ by constructing quotient automata modulo in these subgroups.*

(ii) A is quasiperfect.

Proof. To induce a trivial homomorphism (i.e., a homomorphism to one-state automaton), A must be transitive with respect to $G(A)$ because A is strongly connected. The converse is true by Proposition 2.1. Q.E.D.

3. The Class of Automata Characterized by Groups

$\bar{I}$, the input semigroup associated with an automaton A, defined by Weeg [7] (just the same notion is also defined by Krohn and Rhodes [8]), is a quotient semigroup of I under the congruence ρ: $x, y \in I$, $x\rho y \Leftrightarrow \forall q \in Q$, $M(q, x) = M(q, y)$. An equivalence class of ρ containing x is denoted by $[x]$.

An automaton is called "group-type" if the associated semigroup forms a group. An automaton is called a "permutation" one if each input permutes a set of states [13, 14].

It is obvious that the class of permutation automata forms proper subclass of that of group-type one. But assuming the strongly connectedness, we can show the equivalence.

Proposition 3.1. *For a strongly connected automaton A, the following two statements are equivalent*: (i) *A is a permutation automaton.*

(ii) *A is a group-type automaton.*

Proof is straightforward and, therefore, omitted.

Hereafter, a characterization theorem for the classes of three types of automata will be given.

First, we characterize a strongly connected permutation automaton.

Proposition 3.2. *For an automaton A, the following two statements are equivalent*:

(i) *A is a strongly connected permutation automaton.*

(ii) *A is a homomorphic image of some quasiperfect automaton.*

Proof. Let $\bar{I}$ be an input semigroup associated with a strongly connected permutation automaton A. By Proposition 3.1, $\bar{I}$ forms a group. Next define $A_I = (\bar{I}, M_I, I)$, where $\forall [x] \in \bar{I}$, $\forall y \in I$, $M_I([x], y) = [xy]$. Then A_I is quasiperfect and A is a homomorphic image of A_I. This is a proof of (i) $\to$ (ii).

The converse can be shown directly. Q.E.D.

A characterization for a quasiperfect automaton is already given by Bayer [4] as follows.

Proposition 3.3. *A quasiperfect automaton B is a homomorphic image of a quasiperfect automaton A if and only if there exists a normal subgroup H of $G(A)$ such that B is isomorphic to A/H.*

An automaton A is called perfect if it is strongly connected and $\forall q \in Q$, $\forall x, y \in I$, $M(q, xy) = M(q, yx)$ [1]. It is known that the class of perfect automata forms a proper subclass of that of quasiperfect automata [2].

A perfect automaton is characterized as follows.

PROPOSITION 3.4. *A perfect automaton B is a homomorphic image of a quasiperfect automaton A if and only if there exists a normal subgroup H of G(A) which contains a commutator subgroup of G(A) such that B is isomorphic to A/H.*

Proof. First, there must exist a normal subgroup H of $G(A)$ such that B is isomorphic to A/H. Next, let define an operation $*$ on the state set $Q_H = \{[q]_H \mid \forall q \in Q\}$ of A/H as follows: $[q]_H * [q']_H = [q'']_H \Leftrightarrow q'' = M(q, xy)$, where $q = M(q_0, x)$ and $q' = M(q_0, y)$ for some fixed q_0 in Q. Then it can be proved that the algebraic system $(Q_H, *)$ forms a group which is isomorphic to the quotient group $G(A)/H$. But, since A/H is perfect, $(Q_H, *)$ must be commutative. So must be $G(A)/H$.

The sufficiency is directly shown by constructing A/H. Q.E.D.

Now, we can show a desired characterization theorem.

THEOREM 3.1. *Let A be a quasiperfect automaton. The next three propositions hold.*

(i) *An automaton B is a homomorphic image of A if and only if there exists a subgroup H of G(A) such that B is isomorphic to A/H. In this case, B is always a strongly connected permutation automaton.*

(ii) *A quasiperfect automaton B is a homomorphic image of A if and only if there exists a normal subgroup H of G(A) such that B is isomorphic to A/H.*

(iii) *A perfect automaton B is a homomorphic image of A if and only if there exists a normal subgroup H of G(A) which contains a commutator subgroup of G(A) such that B is isomorphic to A/H.*

4. DIRECT PRODUCT DECOMPOSITION OF AN AUTOMATON

The input semigroup $\bar{I}$ associated with a quasiperfect automaton A is isomorphic to $G(A)$ under the next correspondence $\phi: G(A) \to \bar{I}$, $\phi(g) = [x]$ where $g \in G(A)$, $[x] \in \bar{I}$ such that $g(q_0) = M(q_0, x)$ for some fixed q_0 in Q [2].

As was shown in the proof of Proposition 3.2, a strongly connected permutation automaton A must be isomorphic to a quotient automaton A_I/H of A_I mod some subgroup H of $G(A_I)$. But, by the construction of A_I, it is clear that an input group associated with A_I is identical to that with A. Then, there must exist a subgroup K

in $\bar{I}$, the input group associated with A, which is isomorphic to the subgroup H of $G(A_I)$ under the correspondence shown previously.

We call K the "natural subgroup" of $\bar{I}$.

THEOREM 4.1. *A strongly connected permutation automaton A is decomposed into a direct product of two automata if and only if there exist subgroups K_1 and K_2 in $\bar{I}$, the input group associated with A, such that $K_1 \cap K_2 = K$ and $K_1K_2 = \bar{I}$, where K is the natural subgroup of $\bar{I}$.*

Proof. Suppose a strongly connected permutation automaton A is decomposed into a direct product of two automata A_1 and A_2, i.e., $A \cong A_1 \times A_2$. Then there exist H of $G(A_I)$ such that $A_I/H \simeq A_1 \times A_2$. Therefore, there must exist H_1 and H_2 of $G(A_I)$ which contain H such that $A_1 \cong A_I/H_1$ and $A_2 \cong A_I/H_2$, respectively. In these cases, homomorphisms η_H: A_I onto A, η_1: A_I/H onto A_I/H_1 and η_2: A_I/H onto A_I/H_2 are defined by $\eta_H([x]) = [x]_H$, $\eta_1([x]_H) = [x]_{H_1}$ and $\eta_2([x]_H) = [x]_{H_2}$.

Therefore, for states $[x]_H$, $[y]_H$ of A_I/H, $[x]_H(\eta_1 \circ \eta_1^{-1})[y]_H \Leftrightarrow$

$$\eta_H([x])\,(\eta_1 \circ \eta_1^{-1})\,\eta_H([y]) \Leftrightarrow [x]((\eta_1\eta_H) \circ (\eta_1\eta_H)^{-1})[y] \Leftrightarrow [x]_{H_1} = [y]_{H_1}$$

and similarly $[x]_H\,(\eta_2 \circ \eta_2^{-1})[y]_H \Leftrightarrow [x]_{H_2} = [y]_{H_2}$. Where $\eta \circ \eta^{-1}$ denotes a congruence relation on the set of states induced by an automaton homomorphism η.

By the necessary and sufficient condition for the direct product decomposability of an automaton, $\eta_1 \circ \eta_1^{-1} \cap \eta_2 \circ \eta_2^{-1}$ (intersection) must be an identity relation and $\eta_1 \circ \eta_1^{-1} \square\, \eta_2 \circ \eta_2^{-1}$ (composition) must be an universal relation.

The first relation implies: $[x]_H = [y]_H \Leftrightarrow [x]_H\,(\eta_1 \circ \eta_1^{-1} \cap \eta_2 \circ \eta_2^{-1})[y]_H \Leftrightarrow [x]_H\,(\eta_1 \circ \eta_1^{-1})[y]_H$ and $[x]_H\,(\eta_2 \circ \eta_2^{-1})[y]_H \Leftrightarrow [x]_{H_1} = [y]_{H_1}$ and $[x]_{H_2} = [y]_{H_2}$. This implies the following: $(\exists h \in H, h([x]) = [y]) \Leftrightarrow (\exists h_1 \in H_1, h_1([x]) = [y]$ and $\exists h_2 \in H_2$, $h_2([x]) = [y])$.

Then we have $h = h_1 = h_2$ by the strongly connectedness of A [1], which implies $H = H_1 \cap H_2$.

The second relation implies: $\forall[x]_H$, $\forall[y]_H$, $\exists[z]_H$, $[x]_H\,(\eta_1 \circ \eta_1^{-1})[z]_H$ and $[z]_H\,(\eta_2 \circ \eta_2^{-1})[y]_H \Leftrightarrow \forall[x]$, $\forall[y]$, $\exists[z]$, $[x]_{H_1} = [z]_{H_1}$ and $[z]_{H_2} = [y]_{H_2}$. This implies for any $[x]$, $[y]$ in $\bar{I}$, there exist h_1 in H_1 and h_2 in H_2 such that $h_1^{-1}h_2([y]) = [x]$, i.e., the subset H_1H_2 of $G(A_I)$ must be transitive on the state set of A_I. Since a quasiperfect automaton cannot be transitive with respect to any proper subset of its automorphism group, H_1H_2 must be equal to $G(A_I) \cong \bar{I}$.

The sufficiency can be proved in a straight manner by constructing the quotient automata and, therefore, omitted here. Q.E.D.

Notice that the factor automata are also strongly connected permutation ones, since every homomorphism preserves strongly connectedness and group-typeness.

COROLLARY 4.1. *A strongly connected permutation automaton is decomposed into a direct product of two automata if the associated input group is decomposed into a direct product of two groups.*

Proof. Assume $\bar{I}$ is decomposed into a direct product of two groups J_1 and J_2. Let K be a natural subgroup of $\bar{I}$ and define $K_1 = KJ_1$ and $K_2 = KJ_2$. Clearly K_1 and K_2 satisfy the condition of Theorem 4.1. Q.E.D.

The result for the direct product decomposability of perfect or quasiperfect automata given by Fleck [1, 3] or Trauth [2] are shown as the corollaries of this theorem in a straight manner, since the natural subgroup is a trivial group of identity when the given strongly connected permutation automaton is quasiperfect.

ACKNOWLEDGMENTS

The authors acknowledge Prof. D. E. Muller of the University of Illinois for his helpful suggestions, Prof. E. K. Blum of University of Southern California for giving us advice on revising the original article, and the referee for pointing out a few references of which we were not aware.

The authors also thank T. Inose and H. Uematsu for their fruitful discussions.

REFERENCES

1. A. C. FLECK, Isomorphism group of automata, *J. ACM* (4), **9** (1962), 469–476.
2. C. A. TRAUTH, JR., Group-type automata, *J. ACM* (1), **13** (1966), 170–175.
3. A. C. FLECK, On the automorphism group of automata, *J. ACM* (4), **12** (1965), 566–569.
4. R. BAYER, Automorphism group and quotient of strongly connected automata and monadic algebras, *IEEE* 1966 *7th. Ann. Symp. Switching and Automata Theory* (1966), 282–297.
5. Y. MASUNAGA, S. NOGUCHI, AND J. OIZUMI, A semigroup theoretic consideration about the structure of automata. I, *Proc. 3rd Hawaii Int. Conf. on System Sciences* (1970), 68–71.
6. T. INOSE, Y. MASUNAGA, S. NOGUCHI, AND J. OIZUMI, A semigroup theoretic consideration about the structure of automata. II, *Proc. 3rd Hawaii Int. Conf. on System Science* (1970), 72–75.
7. G. P. WEEG, The structure of an automaton and its operation-preserving transformation group, *J. ACM* (3), **9** (1962), 345–349.
8. K. B. KROHN AND J. L. RHODES, Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines, *Trans. AMS* **116** (1965), 450–464.
9. M. A. ARBIB, Automaton automorphisms, *Information and Control* **11** (1967), 147–154.
10. R. H. OEHMKE, On the structures of an automaton and its input semigroups, *J. ACM* (4), **10** (1963), 521–525.
11. P. DEUSSEN, Some results on the set of congruence relations in a finite, strongly connected automaton, *Computing* 2 (1967), 353–367.
12. J. F. PERROT, Groups and automata, *Internat. Symp. Theory of Machines and Computations, Haifa* **1971** (1971), 287–293.
13. G. THIERREN, Permutation automata, *Mathematical Systems Theory* 2 (1968), 83–90.
14. H. P. ZEIGER, See Section 7 of "Algebraic Structure Theory of Sequential Machines" (Hartmanis and Stearns), Prentice-Hall, New York, 1966.