Acta Cybernetica, Vol. 11, No. 3, Szeged, 1994

Mealy-automata in which the output-equivalence is a congruence*

I. Babcsányi† A. Nagy†

Dedicated to Professor A. ÁDÁM on his 60th birthday

Abstract

Every Mealy-automaton whose output equivalence is not the universal relation has a non-trivial simple state-homomorphic image. Thus the simple Mealy-automata play an importante role in the theory of Mealy-automata. It is very difficult to describe the structure of these automata. Contrary to the earlier investigations, in our present paper we concentrate our attention only to a special kind of simplicity, namely the strongly simplicity. Besides we give a construction for strongly simple Mealy-automata, we also describe the structure of all Mealy-automata which have strongly simple state-homomorphic image.

1 Preliminaries

By a *Mealy-automaton* we mean a system $\underline{A} = (A, X, Y, \delta, \lambda)$ consisting of a state set A, an input set X, an output set Y, a transition function $\delta : A \times X \to A$ and an output function $\lambda : A \times X \to Y$. In that case when $|A|, |X|, |Y|$ are finite, $\underline{A} = (A, X, Y, \delta, \lambda)$ is called finite ($|S|$ denotes the cardinality of a set S). A Mealy-automaton $\underline{A}$ is called a *Moore-automaton* if

$$\delta(a_1, x_1) = \delta(a_2, x_2) \Longrightarrow \lambda(a_1, x_1) = \lambda(a_2, x_2)$$

for all $a_1, a_2 \in A$ and $x_1, x_2 \in X$. It means that the function λ can be given in the form

$$\lambda(a, x) = \mu(\delta(a, x)) \quad (a \in A, x \in X),$$

where $\mu : A \to Y$ is a single-valued mapping. The function μ is said to be the *sign function* of $\underline{A}$.

*Research supported by project 11281 of the Academy of Finland, the Basic Research ASMICS II Working Group, and, in the case of the second author, also by the Alexander von Humboldt Foundation.

†Department of Mathematics, Transport Engineering Faculty, Technical University of Budapest, H-1111 Budapest, Műegyetem rkp. 9., Hungary

Let X^* and X^+ denote the free monoid and the free semigroup over a nonempty set X, respectively. We extend the functions δ and λ of $\underline{A}$ in the usual forms $\delta : A \times X^* \longrightarrow A^*$ and $\lambda : A \times X^* \longrightarrow Y^*$ as follows :

$$\delta(a,e) = a, \quad \delta(a,px) = \delta(a,p)\delta(ap,x),$$

$$\lambda(a,e) = e, \quad \lambda(a,px) = \lambda(a,p)\lambda(ap,x),$$

where $a \in A$, $p \in X^+$, $x \in X$, ap denotes the last letter of $\delta(a,p)$ and e denotes the empty word.

An equivalence relation τ of a state set A of a Mealy-automaton $\underline{A} = (A, X, Y, \delta, \lambda)$ is called a *congruence* on $\underline{A}$ if

$$(a,b) \in \tau \Longrightarrow (ap, bp) \in \tau \quad \text{and} \quad \overline{\lambda(a,p)} = \overline{\lambda(b,p)}$$

for all $a, b \in A$ and $p \in X^+$. (If $r \in Y^+$ then $\overline{r}$ denotes the last letter of r.)

Let ρ_{max} denote the relation on the state set A of a Mealy-automaton $\underline{A} = (A, X, Y, \delta, \lambda)$ defined by

$$(a,b) \in \rho_{max} \Longleftrightarrow \overline{\lambda(a,p)} = \overline{\lambda(b,p)} \quad \text{for all} \quad p \in X^+ \quad ([2]).$$

The ρ_{max}-class of $\underline{A}$ containing the state a of $\underline{A}$ is denoted by $\rho_{max}[a]$.

Denoting the identity relation of a Mealy-automaton $\underline{A}$ by ι, we say that $\underline{A}$ is *simple* if $\rho_{max} = \iota$.

It is easy to see that ρ_{max} is the greatest congruence of $\underline{A}$ and $\underline{A}/\rho_{max}$ is simple.

Let $\underline{A} = (A, X, Y, \delta, \lambda)$ and $\underline{A}' = (A', X, Y, \delta', \lambda')$ be arbitrary Mealy-automata. We say that a mapping $\alpha : A \longrightarrow A'$ is a *state-homomorphism* of $\underline{A}$ into $\underline{A}'$ if

$$\alpha(\delta(a,x)) = \delta'(\alpha(a), x), \quad \lambda(a,x) = \lambda'(\alpha(a), x)$$

for all $a \in A$ and $x \in X$. If α is surjective then $\underline{A}'$ is called a *state-homomorphic image* of $\underline{A}$. If α is bijective then α is called a *state-isomorphism* and the automata $\underline{A}$ and $\underline{A}'$ are said to be *state-isomorphic*.

Let $\underline{A} = (A, X, Y, \delta, \lambda)$ be a Mealy-automaton. By the *output-equivalence* of $\underline{A}$ we mean the equivalence ρ defined as

$$\rho = \{(a,b) \in A \times A : \quad (\forall x \in X) \quad \lambda(a,x) = \lambda(b,x)\} \quad ([3]).$$

It is evident that $\rho_{max} \subseteq \rho$. Moreover ρ is a congruence if and only if $\rho = \rho_{max}$. If ρ is the universal relation of A then, for every $a, b \in A$, $q \in X^*$ and $x \in X$,

$$\overline{\lambda(a,qx)} = \lambda(aq,x) = \lambda(bq,x) = \overline{\lambda(b,qx)}.$$

From this it follows that if ρ is the universal relation of A then $\rho = \rho_{max}$.

For notations and notions not defined here, we refer to [4] and [5].

2 Strongly simple Mealy-automata

Definition A Mealy-automaton will be called a *strongly simple* Mealy-automaton if $\rho = \iota$.

The next construction plays an importante role throughout this paper.

Construction 1 *Let $\underline{A} = (A, X, Y, \delta, \lambda)$ be a Mealy-automaton. To arbitrary states a of $\underline{A}$, we can associate mappings α_a of X into Y defined as follows:*

$$\alpha_a : x \to \lambda(a, x).$$

Consider the set $\mathcal{A} = \{\alpha_a; a \in A\}$ and, for every $a \in A$ and $x \in X$, let

$$\delta'(\alpha_a, x) = \alpha_{\delta(a,x)}, \quad \lambda'(\alpha_a, x) = \alpha_a(x).$$

Theorem 1 *For an arbitrary Mealy-automaton $\underline{A} = (A, X, Y, \delta, \lambda)$, the following four conditions are equivalent:*

(i) The quintuple $\underline{\mathcal{A}} = (\mathcal{A}, X, Y, \delta', \lambda')$, where $\mathcal{A}$, δ', λ' are defined as in Construction 1, is a Mealy-automaton;

(ii) $\rho = \rho_{max}$ in $\underline{A}$;

(iii) $\underline{\mathcal{A}}$ and $\underline{A}/\rho_{max}$ are state-isomorphic;

(iv) $\underline{A}/\rho_{max}$ is strongly simple.

Proof. Assume that $\underline{\mathcal{A}}$ is a Mealy-automaton. Then $\alpha_a = \alpha_b$ implies $\alpha_{\delta(a,x)} = \alpha_{\delta(b,x)}$ for every $a, b \in A$ and $x \in X$, because δ' is well-defined. We show that $\rho = \rho_{max}$ in $\underline{A}$. Consider two arbitrary elements a and b of A with $(a, b) \in \rho$. Then $\alpha_a = \alpha_b$ and so we get $\alpha_{\delta(a,x)} = \alpha_{\delta(b,x)}$ for every $x \in X$. Using this idea and the fact that δ is extended to $A \times X^*$, we get $\alpha_{ap} = \alpha_{bp}$ for every $p \in X^*$. Thus

$$\overline{\lambda(a, px)} = \lambda(ap, x) = \lambda(bp, x) = \overline{\lambda(b, px)}$$

for every $p \in X^*$ and $x \in X$. Consequently $(a, b) \in \rho_{max}$ which implies that $\rho = \rho_{max}$ in $\underline{A}$. Thus (i) implies (ii).

Assume that $\rho = \rho_{max}$ in a Mealy-automaton $\underline{A}$. To show that $\underline{\mathcal{A}}$ is a Mealy-automaton, it is sufficient to prove that δ' is well-defined. Let a and b be arbitrary elements of A with $\alpha_a = \alpha_b$. Then $(a, b) \in \rho = \rho_{max}$ from which we get $(\delta(a, x), \delta(b, x)) \in \rho = \rho_{max}$ for every $x \in X$. Thus $\alpha_{\delta(a,x)} = \alpha_{\delta(b,x)}$ $(x \in X)$ and so δ' is well-defined. Consequently, (ii) implies (i).

To show that (ii) implies (iii), assume $\rho = \rho_{max}$ in $\underline{A}$. Then $\alpha_a = \alpha_b$ if and only if $(a, b) \in \rho_{max}$ which implies that $\alpha_a \to \rho_{max}[a]$, $a \in A$ is a state-isomorphism of $\underline{\mathcal{A}}$ onto $\underline{A}/\rho_{max}$. Consequently, (iii) is satisfied.

Assume (iii). Then $\underline{\mathcal{A}}$ is a Mealy-automaton. Thus λ' is well-defined. From this it follows that $\underline{\mathcal{A}}$ and so $\underline{A}/\rho_{max}$ is strongly simple. Therefore, (iv) is true.

Condition (ii) follows from (iv) in a trivial way. □

Construction 2 *Let M be a non-empty subset of the set Y^X of all mappings of X into Y, where X and Y are arbitrary non-empty sets. Consider the Mealy-automaton $\underline{M} = (M, X, Y, \delta^*, \lambda^*)$, where δ^* is arbitrary and λ^* is defined as follows:*

$$\lambda^*(\alpha, x) = \alpha(x), \quad \alpha \in M, \ x \in X.$$

For non-empty sets X and Y, denote $\mathcal{M}[X,Y]$ the set of all Mealy-automata defined in Construction 2. It is evident that $\underline{\mathcal{A}} \in \mathcal{M}[X,Y]$ supposing that $\rho = \rho_{max}$ in the Mealy-automaton $\underline{A} = (A, X, Y, \delta, \lambda)$.

Theorem 2 *A Mealy-automaton is strongly simple if and only if it is state-isomorphic to a Mealy-automaton* $\underline{M} = (M, X, Y, \delta^*, \lambda^*)$ *defined in Construction 2 for some* X, Y, δ^* *and* λ^*.

Proof. It is trivial that Mealy-automata defined in Construction 2 are strongly simple.

Conversely, let $\underline{A} = (A, X, Y, \delta, \lambda)$ be an arbitrary strongly simple Mealy-automaton. For this Mealy-automaton consider $\underline{\mathcal{A}} = (\mathcal{A}, X, Y, \delta', \lambda')$ with $\mathcal{A}$, δ' λ' defined in Construction 1. By Theorem 1, $\underline{A}$ is isomorphic to $\underline{\mathcal{A}} \in \mathcal{M}[X,Y]$. □

Lemma 1 $\underline{M}_1$, $\underline{M}_2 \in \mathcal{M}[X,Y]$ *are state-isomorphic if and only if* $\underline{M}_1 = \underline{M}_2$.

Proof. Assume that $\underline{M}_1$, $\underline{M}_2 \in \mathcal{M}[X,Y]$ are state-isomorphic. Let φ be a state-isomorphism of $\underline{M}_1$ onto $\underline{M}_2$. Then, for every $\alpha \in M_1$ and $x \in X$,

$$\alpha(x) = \lambda_1^*(\alpha, x) = \lambda_2^*(\varphi(\alpha), x) = \varphi(\alpha)(x)$$

and

$$\varphi(\delta_1^*(\alpha, x)) = \delta_2^*(\varphi(\alpha), x).$$

From the first expression we get that φ is identical and so $M_1 = M_2$, $\lambda_1^* = \lambda_2^*$. Then the second expression implies $\delta_1^* = \delta_2^*$. Consequently, $\underline{M}_1 = \underline{M}_2$. □

Corollary 1 *If* X *and* Y *are finite non-empty sets then*

$$|\mathcal{M}[X,Y]| = \sum_{k=1}^{|Y|^{|X|}} \binom{|Y|^{|X|}}{k} k^{k|X|}.$$

Proof. Let X and Y be arbitrary finite non-empty sets. Then $|Y^X| = |Y|^{|X|}$. Let $M \subseteq Y^X$ be arbitrary with $|M| = k$. By the Lemma, the number of all different Mealy-automata defined in Construction 2 with the state set M is $k^{k|X|}$, because we can choose $\delta^* : M \times X \to M$ in $k^{k|X|}$ different way. This implies our assertion. □

It is known that every Mealy-automaton is equivalent ([4]) to some Moore-automaton. Therefore, it is interesting for us to know how we can construct the strongly simple Moore-automata. We note that a Mealy-automaton $\underline{M}$ defined in Construction 2 is a Moore-automaton if and only if we choose δ^* such that

$$\alpha_1(x_1) \neq \alpha_2(x_2) \Longrightarrow \delta^*(\alpha_1, x_1) \neq \delta^*(\alpha_2, x_2)$$

for every $\alpha_1, \alpha_2 \in M$ and $x_1, x_2 \in X$. Moreover, the output function λ^* of $\underline{M}$ does not depend on the input signs if and only if all mappings $\alpha \in M$ are constant. In this case $\underline{M}$ can be considered as a special Moore-automaton ([1]) with the sign function λ^* and the output function λ defined by $\lambda(\alpha, x) = \lambda^*(\delta^*(\alpha, x))$. Thus the number of these special Moore-automata belonging to $\mathcal{M}[X,Y]$ is

$$\sum_{k=1}^{|Y|} \binom{|Y|}{k} k^{k|X|},$$

supposing that X and Y are finite.

Introduce a partially ordering "$\leq$" on $\mathcal{M}[X,Y]$ as follows: $\underline{M_1} \leq \underline{M_2}$ if and only if $M_1 \subseteq M_2$ and δ_1 equals the restriction of δ_2 to $M_1 \times X$. Under this ordering an element of $\mathcal{M}[X,Y]$ is maximal if and only if its state set is Y^X. If X and Y are finite then the number of maximal elements of $\mathcal{M}[X,Y]$ is

$$|Y|^{(|Y|^{|X|})|X|^2}.$$

It can be easily verified that the number of maximal elements of $\mathcal{M}[X,Y]$ which are special Moore-automata (see above) is $|Y|^{|Y||X|}$.

3 Mealy-automata having a strongly simple state-homomorphic image

In this chapter we give a construction for Mealy-automata which has the property $\rho = \rho_{max}$.

Construction 3 *Let $\underline{M} = (M, X, Y, \delta^*, \lambda^*)$ be a strongly simple Mealy-automaton (defined in Construction 2). Consider a family of sets B_m, $m \in M$ such that $B_m \cap B_{m'} = \emptyset$ if $m \neq m'$. For all $x \in X$ and $m \in M$, let $\varphi_{m,x}$ be a mapping of B_m into $B_{\delta^*(m,x)}$. Let $B = \cup_{m\in M} B_m$. Define the functions $\delta^\circ : B \times X \to B$ and $\lambda^\circ : B \times X \to Y$ as follows. For arbitrary $b \in B_m$, let*

$$\delta^\circ(b,x) = \varphi_{m,x}(b) \quad \textit{and} \quad \lambda^\circ(b,x) = m(x).$$

It can be easily verified that δ° and λ° are well-defined and so $\underline{B} = (B, X, Y, \delta^\circ, \lambda^\circ)$ is a Mealy-automaton.

Theorem 3 *A Mealy-automaton has the property that $\rho = \rho_{max}$ if and only if it can be defined as in Construction 3.*

Proof. Let $\underline{B}$ be a Mealy-automaton defined in Construction 3. We prove that $\rho = \rho_{max}$. For all $m \in M$, $p \in X^*$ and $x \in X$ let $\varphi_{m,px} = \varphi_{mp,x} \circ \varphi_{m,p}$, where mp denotes the last letter of $\delta^*(m,p)$. It is clear that $\varphi_{m,p}(a) = ap$ for all $a \in B_m$ and $p \in X^*$, where ap denotes the last letter of $\delta^\circ(a,p)$. Assume $(a,b) \in \rho$ for some $a, b \in B$. Then $a, b \in B_m$ for some $m \in M$. For arbitrary $p \in X^*$ and $x \in X$,

$$\overline{\lambda^\circ(a,px)} = \lambda^\circ(ap,x) = \lambda^\circ(\varphi_{m,p}(a),x) = \lambda^\circ(\varphi_{m,p}(b),x) = \lambda^\circ(bp,x) = \overline{\lambda^\circ(b,px)}.$$

From this it follows that $(a,b) \in \rho_{max}$.

Conversely, assume that $\rho = \rho_{max}$ in a Mealy-automaton $\underline{A} = (A, X, Y, \delta, \lambda)$. By Theorem 1, $\underline{\mathcal{A}} = (\mathcal{A}, X, Y, \delta', \lambda')$ is a Mealy-automaton which is state-isomorphic with the strongly simple Mealy-automaton $\underline{A}/\rho_{max}$. Using Construction 3 for $\underline{M} = \underline{\mathcal{A}}$, consider the Mealy-automaton $\underline{B} = (B, X, Y, \delta^\circ, \lambda^\circ)$ such that $B_{\alpha_a} = \rho_{max}[a]$ and $\varphi_{\alpha_a,x}$ defined by $\varphi_{\alpha_a,x}(b) = \delta(b,x)$ for arbitrary $a \in A$, $b \in B_{\alpha_a}$, $x \in X$. It is easy to see that $A = B$, $\delta = \delta^\circ$ and $\lambda = \lambda^\circ$. Thus $\underline{A} = \underline{B}$. □

Remark. If the output equivalence ρ of a Mealy-automaton $\underline{A}$ is the universal relation of A then $\underline{A}$ is simple if and only if it is strongly simple if and only if it is trivial (it has only one state). Thus our problems are trivial in this case. We note that if $\underline{A} = (A, X, Y, \delta, \lambda)$ is a Mealy-automaton in which ρ is the universal relation then the congruences of $\underline{A}$ are the same as the congruences of the projection $\underline{A}_{pr} = (A, X, \delta)$ of $\underline{A}$. But the simplicity of automata without outputs is modified as follows: An automaton $\underline{B}$ without outputs is called simple if its every state-homomorphic image is trivial or isomorphic to $\underline{B}$. It is easy to see that this simplicity is different from the strongly simplicity. (Here the strongly simplicity means that the automaton is trivial.)

References

[1] Ádám, A., *On the question of description of the behaviour of finite automata*, Studia Sci. Math. Hungar., 13 (1978), 105-124.

[2] Babcsányi, I., *On output behaviour of Mealy-automata*, Periodica Polytechnica (Transportation Engineering), 19(1991), No 1-2, 15-21.

[3] Babcsányi, I., A. Nagy and F. Wettl, *Indistinguishable state pairs in strongly connected Moore-automata*, PU.M.A. Ser. A, 2 (1991), 15-24.

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

[5] Szász, G., *Introduction to Lattice Theory*, Academic Press, New York- London, 1963.

Received December 21, 1993