On characteristic semigroups of Mealy automata

G. TANAKA

Hiroshima Shudo University Numata-cho, Asaminami-ku Hiroshima 731—31, JAPAN

Dedicated to Professor Miyuki Yamada on his 60th birthday.

Abstract

The purpose of this paper is to investigate the characteristic semigroup of a Mealy automaton. We show that there exists a bijection from the set of regular $\mathcal{D}$-classes of a characteristic semigroup $S'(M)$ of a Mealy automaton M onto the set of regular $\mathcal{D}$-classes of the semigroup $S(M^*)$ of the projection M^*.

1. Introduction

For a set I, the cardinality of I is denoted by $|I|$. I^* is the free monoid with an identity ε generated by I, and $I^+=I^*-\{\varepsilon\}$. If $w\in I^+$ is a nonempty word, then we denote by $\overline{w}$ the last letter of w. We use the symbol $\emptyset$ for the empty set.

Let $\delta\colon S\to S_1$ and $\lambda\colon S_1\to S_2$ be mappings of S and S_1, respectively. We read a product $\delta\lambda$ from left to right: $(s)\delta\lambda=((s)\delta)\lambda$, $s\in S$. The set $(S)\delta$ is called the image of δ and it is denoted by $\operatorname{Im}\delta$. The equivalence relation $\operatorname{Ker}\delta$ defined on S by $(s_1, s_2)\in\operatorname{Ker}\delta$ if and only if $(s_1)\delta=(s_2)\delta$ is called the kernel of δ.

An *automaton A* is a triple $A=(S, I, \delta)$, where S is a nonempty set of states, I is a nonempty set of inputs, δ is a state transition function such that $\delta(s, xy)=$ $=\delta(\delta(s, x), y)$ and $\delta(s, \varepsilon)=s$ for all $s\in S$ and all $x, y\in I^*$.

A *Mealy automaton M* is a quintuple $M=(S, I, U, \delta, \lambda)$, where $M^*=(S, I, \delta)$ is an automaton, U is a nonempty set of outputs, $\lambda\colon S\times I\to U$ is an output function. The output function is also used in the extended sence; for $s\in S$ and $xy\in I^*$ such that $x\in I^*$ and $y\in I$, $\lambda(s, \varepsilon)=\varepsilon$ and $\lambda(s, xy)=\lambda(s, x)\lambda(\delta(s, x), y)$.

The automaton M^* mentioned above is called the *projection* of the Mealy automaton M.

Let $M=(S, I, U, \delta, \lambda)$ be a Mealy automaton. To each $x\in I^+$ we assign the transformation δ_x on S, where $\delta_x\colon s\to\delta(s, x)$, $s\in S$. Let $S(M^*)=\{\delta_x|x\in I^+\}$.

Then $S(M^*)$ is a subsemigroup of the full transformation semigroup on S. To each $x \in I^+$ we assign the mapping λ_x: $s \to \lambda(s, x)$, $s \in S$. If xy is an element of I^+ such that both x and y are in I^+, then $(s)\lambda_{xy} = (s)\delta_x \lambda_y$.

The congruence ϱ on I^+ is defined by $x\varrho y$ if and only if $\delta_x = \delta_y$ and $\lambda_x = \lambda_y$. Put $S'(M) = \{(\lambda_x, \delta_x) | x \in I^+\}$. In $S'(M)$ we introduce the multiplication as follows:

$$(\lambda_x, \delta_x)(\lambda_y, \delta_y) = (\delta_x \lambda_y, \delta_x \delta_y).$$

Since $(\delta_x \lambda_y, \delta_x \delta_y) = (\lambda_{xy}, \delta_{xy}) \in S'(M)$, the set $S'(M)$ forms a semigroup which is isomorphic to I^+/ϱ. In this paper $S'(M)$ is called the *characteristic semigroup* of M. We note that if $\lambda_x = \lambda_y$ and $\delta_x = \delta_z$ $(x, y, z \in I^+)$, then $(\lambda_y, \delta_z) = (\lambda_x, \delta_x)$ as a pair of mappings and $(\lambda_y, \delta_z) \in S'(M)$.

We shall remark on another aspect of the characteristic semigroup of a finite Mealy automaton.

Remark. Assume that S is a finite set. On the output set U we define a multiplication by $ab = b$, $(a, b \in U)$. In such a way we obtain a right zero semigroup U. To each (λ_x, δ_x) in $S'(M)$ we define the $|S| \times |S|$ row-monomial matrix $M(\lambda_x, \delta_x)$ by

$$M(\lambda_x, \delta_x)_{st} = \begin{cases} (s)\lambda_x & \text{if} \quad (s)\delta_x = t, \\ 0 & \text{otherwise.} \end{cases}$$

Two matrices are multiplied in the obvious way, and the set of all matrices forms a semigroup. Since the mapping $(\lambda_x, \delta_x) \to M(\lambda_x, \delta_x)$ is an isomorphism, $S'(M)$ is isomorphic to a subsemigroup of the wreath product $U \mathrm{wr} S(M^*)$ of U and $S(M^*)$ (see [7]).

2. Regular $\mathscr{D}$-class

On a semigroup T Green's relations are defined by

$$a\mathscr{R}b \Leftrightarrow aT^1 = bT^1, \quad a\mathscr{L}b \Leftrightarrow T^1 a = T^1 b,$$

$$a\mathscr{D}b \Leftrightarrow a\mathscr{L}c \quad \text{and} \quad c\mathscr{R}b \quad \text{for some} \quad c \in T.$$

The intersection of two equivalences $\mathscr{R}$ and $\mathscr{L}$ is denoted by $\mathscr{H}$. An element x of a semigroup T is called *regular* if there exists y in T with $xyx = x$. If D is a $\mathscr{D}$-class, then either every element of D is regular or no element of D is regular. Therefore we call a $\mathscr{D}$-class regular if all its elements are regular. In a regular $\mathscr{D}$-class each $\mathscr{R}$-class and each $\mathscr{L}$-class contains at least one idempotent.

Let T be a subsemigroup of the full transformation semigroup on a set S, and let D be a regular $\mathscr{D}$-class of T. If $x, y \in D$, then we have $x\mathscr{L}y$ in $T \Leftrightarrow \mathrm{Im}\, x = \mathrm{Im}\, y$, and $x\mathscr{R}y$ in $T \Leftrightarrow \mathrm{Ker}\, x = \mathrm{Ker}\, y$ (see [2, p 39]).

The proof of the next lemma is omitted.

Lemma 1. Let δ be a transformation on a set S_1 such that $\delta^2 = \delta$, and let λ be a mapping from S_1 to S_2. Then $\delta\lambda = \lambda$ if and only if $\mathrm{Ker}\, \delta \subseteq \mathrm{Ker}\, \lambda$.

In what follows M means a Mealy automaton such that $M = (S, I, U, \delta, \lambda)$.

Theorem 1. $(\lambda_x, \delta_x) \in S'(M)$ is a regular element if and only if δ_x is a regular element of $S(M^*)$ and $\operatorname{Ker} \delta_x \subseteqq \operatorname{Ker} \lambda_x$.

Proof. "only if" part. Since (λ_x, δ_x) is a regular element, there exists some (λ_y, δ_y) in $S'(M)$ such that $\delta_x \delta_y \delta_x = \delta_x$ and $\delta_x \delta_y \lambda_x = \lambda_x$. This implies that $\operatorname{Ker} \delta_x \subseteqq \subseteqq \operatorname{Ker} \delta_x \delta_y \lambda_x = \operatorname{Ker} \lambda_x$. "if" part. Since δ_x is a regular element, $\delta_x \delta_y \delta_x = \delta_x$ for some δ_y in $S(M^*)$. From $\delta_x \delta_y \mathcal{R} \delta_x$ we have $\operatorname{Ker} \delta_{xy} = \operatorname{Ker} \delta_x \subseteqq \operatorname{Ker} \lambda_x$.

Since δ_{xy} is an idempotent, by Lemma 1, $\delta_{xy} \lambda_x = \lambda_x$. Therefore we have $(\lambda_x, \delta_x) \cdot \cdot (\lambda_y, \delta_y)(\lambda_x, \delta_x) = (\lambda_x, \delta_x)$. Q.E.D.

For a subset H of $S'(M)$ we define the sets of mappings by

$$H^{(1)} = \{\lambda_x | (\lambda_x, \delta_x) \in H\}, \quad H^{(2)} = \{\delta_x | (\lambda_x, \delta_x) \in H\}.$$

Theorem 2. If L is an $\mathcal{L}$-class contained in a regular $\mathcal{D}$-class of $S'(M)$, then $L^{(2)}$ is an $\mathcal{L}$-class of $S(M^*)$.

Proof. It is clear that there exists some regular $\mathcal{L}$-class L^* of $S(M^*)$ such that $L^{(2)} \subseteqq L^*$. Now we show the validity of the reverse inclusion. Let $(\lambda_e, \delta_e) \in L$ be an idempotent of $S'(M)$. Then δ_e is an idempotent of L^* and δ_e is a right identity for L^*. Hence for every δ_x in L^* we have $\delta_x \delta_e = \delta_x$ and $\delta_p \delta_x = \delta_e$ for some δ_p in $S(M^*)$. Consequently, $(\delta_x \lambda_e, \delta_x) = (\lambda_{xe}, \delta_{xe}) \in S'(M)$ and $(\delta_x \lambda_e, \delta_x)(\lambda_e, \delta_e) = (\delta_x \lambda_e, \delta_x)$. Moreover, we have $(\lambda_p, \delta_p)(\delta_x \lambda_e, \delta_x) = (\lambda_e, \delta_e)$. This yields that $(\lambda_e, \delta_e) \mathcal{L} (\delta_x \lambda_e, \delta_x)$ in $S'(M)$, and therefore $\delta_x \in L^{(2)}$. Q.E.D.

Theorem 3. If L is an $\mathcal{L}$-class contained in a regular $\mathcal{D}$-class of $S'(M)$, then $(\lambda_x, \delta_x) \to \delta_x$ is a bijection from L onto $L^{(2)}$.

Proof. An idempotent (λ_e, δ_e) in L is a right identity for L. If $(\lambda_p, \delta_x), (\lambda_q, \delta_x) \in L$, then

$$(\lambda_p, \delta_x) = (\lambda_p, \delta_x)(\lambda_e, \delta_e) = (\delta_x \lambda_e, \delta_x) = (\lambda_q, \delta_x)(\lambda_e, \delta_e) = (\lambda_q, \delta_x).$$

Q.E.D.

Let H_1 and H_2 be $\mathcal{H}$-classes contained in the same $\mathcal{D}$-class of $S'(M)$. Then, using Green's lemma, it can be seen that $|H_1^{(2)}| = |H_2^{(2)}|$ holds (see [5]). However, there are examples that show that in general the equality $|H_1^{(1)}| = |H_2^{(1)}|$ does not hold. Therefore, in the next theorem, the condition that boht H_1 and H_2 are in the same $\mathcal{L}$-class is indispensable.

Theorem 4. Let L be an $\mathcal{L}$-class in a regular $\mathcal{D}$-class of $S'(M)$. If H_1 and H_2 are two $\mathcal{H}$-classes contained in L, then $|H_1^{(1)}| = |H_2^{(1)}|$.

Proof. Let (λ_e, δ_e) be an idempotent of L, and let H be an $\mathcal{H}$-class of (λ_e, δ_e). If $\lambda_z \in H^{(1)}$, then $\delta_e \lambda_z = \lambda_z$ since (λ_e, δ_e) is an identity of H. Let $\lambda_x, \lambda_y \in H^{(1)}$ and $\lambda_x \neq \lambda_y$. Then $(s)\delta_e \lambda_x \neq (s)\delta_e \lambda_y$ for some $s \in S$, therefore λ_x and λ_y are distinct mappings on $\operatorname{Im} \delta_e$. Let H_1 be an arbitrary $\mathcal{H}$-class in L. Then $(\lambda_p, \delta_p) H = H_1$ for some (λ_p, δ_p) in $S'(M)$. Thus $H_1^{(1)} = \{\delta_p \lambda_w | \lambda_w \in H^{(1)}\}$. Assume that $\delta_p \lambda_x = \delta_p \lambda_y$ for some $\lambda_x, \lambda_y \in H^{(1)}$, $(\lambda_x \neq \lambda_y)$. Then $\delta_p \delta_e \lambda_x = \delta_p \delta_e \lambda_y$. Since $\delta_p \delta_e \in H_1^{(2)}$, we have that $\delta_p \delta_e \mathcal{L} \delta_e$, and so, $\operatorname{Im} \delta_p \delta_e = \operatorname{Im} \delta_e$. Therefore for every $s \in \operatorname{Im} \delta_e$ there exists some $t \in S$ with $(t)\delta_p \delta_e = s$. Then $(s)\lambda_x = (t)\delta_p \delta_e \lambda_x = (t)\delta_p \delta_e \lambda_y = (s)\lambda_y$ holds for every s in $\operatorname{Im} \delta_e$, which is a contradiction. Hence $\lambda_x \neq \lambda_y$ implies $\delta_p \lambda_x \neq \delta_p \lambda_y$. This shows that the mapping $\theta\colon H^{(1)} \to H_1^{(1)}$ defined by $(\lambda_w)\theta = \delta_p \lambda_w$ is a bijection from $H^{(1)}$ onto $H_1^{(1)}$. Q.E.D.

Theorem 5. If R is an $\mathscr{R}$-class contained in a regular $\mathscr{D}$-class of $S'(M)$, then $R^{(2)}$ is an $\mathscr{R}$-class of $S(M^*)$.

Proof. It is clear that there exists an $\mathscr{R}$-class R^* of $S(M^*)$ such that $R^{(2)}\subseteqq R^*$. We shall show that the reverse inclusion holds, too. Let $(\lambda_e, \delta_e)\in R$ be an idempontent. Then δ_e is an idempotent in R^*, and therefore, $\delta_e\delta_x=\delta_x$ for every $\delta_x\in R^*$. For the word $ex\in I^+$ we have $(\lambda_{ex}, \delta_{ex})=(\delta_e\lambda_x, \delta_x)\in S'(M)$. Since $\delta_x\mathscr{R}\delta_e$, there exists some $\delta_p\in S(M^*)$ such that $\delta_x\delta_p=\delta_e$. In this case $(\delta_e\lambda_x, \delta_x)(\lambda_{pe}, \delta_{pe})=(\lambda_e, \delta_e)$ and $(\lambda_e, \delta_e)(\delta_e\lambda_x, \delta_x)=(\delta_e\lambda_x, \delta_x)$. Therefore $(\delta_e\lambda_x, \delta_x)\in R$ and $\delta_x\in R^{(2)}$. Q.E.D.

Theorem 6. ([6]). Let D be a regular $\mathscr{D}$-class of $S'(M)$ and (λ_x, δ_x), $(\lambda_y, \delta_y)\in D$. Then $(\lambda_x, \delta_x)\mathscr{R}(\lambda_y, \delta_y)$ if and only if $\operatorname{Ker}\delta_x=\operatorname{Ker}\delta_y\subseteqq(\operatorname{Ker}\lambda_x\cap\operatorname{Ker}\lambda_y)$.

Theorem 7. If R_1 and R_2 are distinct $\mathscr{R}$-classes in the same regular $\mathscr{D}$-class of $S'(M)$, then $R_1^{(2)}\cap R_2^{(2)}=\emptyset$.

Proof. If $R_1^{(2)}\cap R_2^{(2)}\neq\emptyset$ then, by Theorem 5, we have $R_1^{(2)}=R_2^{(2)}$. If $(\lambda_x, \delta_x)\in R_1$ and $(\lambda_y, \delta_y)\in R_2$, then δ_x and δ_y are in $R_1^{(2)}$, thus $\operatorname{Ker}\delta_x=\operatorname{Ker}\delta_y$. By Theorem 1, $\operatorname{Ker}\delta_x\subseteqq\operatorname{Ker}\lambda_x$ and $\operatorname{Ker}\delta_y\subseteqq\operatorname{Ker}\lambda_y$. Therefore, by Theorem 6, we have that $(\lambda_x, \delta_x)\mathscr{R}(\lambda_y, \delta_y)$, and so $R_1=R_2$, which is a contradiction. Q.E.D.

Theorem 8. If D is a regular $\mathscr{D}$-class of $S'(M)$, then $D^{(2)}$ is a regular $\mathscr{D}$-class of $S(M^*)$.

Proof. It is obvious that there exists a regular $\mathscr{D}$-class D^* such that $D^{(2)}\subseteqq D^*$. We show that the reverse inclusion holds. Let $\delta_x\in D^*$ and let L^* be an $\mathscr{L}$-class of D^* containing δ_x. If R is an $\mathscr{R}$-class of D then, by Theorem 5, $R^{(2)}$ is an $\mathscr{R}$-class of D^*. Hence $R^{(2)}\cap L^*\neq\emptyset$. If $\delta_y\in R^{(2)}\cap L^*$, then $(\lambda_p, \delta_y)\in D$ for some λ_p. Let L be an $\mathscr{L}$-class containing (λ_p, δ_y). Then $\delta_y\in L^{(2)}\cap L^*$. Thus, by Theorem 2, $L^{(2)}=L^*$. This means that $\delta_x\in L^{(2)}\subseteqq D^{(2)}$, and so $D^*\subseteqq D^{(2)}$. Q.E.D.

Theorem 9. Let D be a regular $\mathscr{D}$-class of $S'(M)$, and let D_R and $D_R^{(2)}$ be sets of $\mathscr{R}$-classes of D and $D^{(2)}$, respectively. Then $|D_R|=|D_R^{(2)}|$.

Proof. By Theorems 7 and 8, the mapping $R\to R^{(2)}$ is a bijection from the set of $\mathscr{R}$-classes of D onto the set of $\mathscr{R}$-classes of $D^{(2)}$. Q.E.D.

If D is a finite regular $\mathscr{D}$-class, then D and $D^{(2)}$ consists of the same number of $\mathscr{R}$-classes. However, note that we cannot in general assert that D and $D^{(2)}$ have the same number of $\mathscr{L}$-classes.

Lemma 2. If (λ_w, δ_e) is a regular element of $S'(M)$ such that δ_e is an idempotent, then (λ_w, δ_e) is an idempotent and $\lambda_w=\delta_e\lambda_w$.

Proof. There exists some idempotent (λ_f, δ_f) such that $(\lambda_w, \delta_e)\mathscr{L}(\lambda_f, \delta_f)$. Since (λ_f, δ_f) is a right identity in its $\mathscr{L}$-class, we obtain that $(\lambda_w, \delta_e)(\lambda_f, \delta_f)=(\delta_e\lambda_f, \delta_e\delta_f)=$ $=(\lambda_w, \delta_e)$. Thus $\delta_e\lambda_f=\lambda_w$. From this we have that (λ_w, δ_e) is an idempotent and $\lambda_w=\delta_e\lambda_w$. Q.E.D.

Theorem 10. If D^* is a regular $\mathscr{D}$-class of $S(M^*)$, then there exists a unique regular $\mathscr{D}$-class D of $S'(M)$ such that $D^{(2)}=D^*$.