<table>
<thead>
<tr>
<th>Title</th>
<th>Characterization of finite Automata by the Images and the Kernels of their Transition Functions (Algebraic Semigroups, Formal Languages and Computation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Saito, Tatsuhiko</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2001), 1222: 53-57</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2001-07</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/41315">http://hdl.handle.net/2433/41315</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Characterization of finite Automata by the Images and the Kernels of their Transition Functions

T. Saito (斎藤 立彦)

Mukunoura 374, Innoshima, Hiroshima, Japan, 722-23221
e-mail: tatusaito@mx4.tiki.ne.jp

1. Introduction

By an automaton $\mathcal{A}$, we mean here a 3-tuple $(X, A, \delta)$, where $X$ is a finite set (the set of states), $A$ is a finite alphabet (the set of inputs) and $\delta$ is a mapping of $X \times A$ into $X$ (the transition function).

As usual, $A^*$ and $A^+$ denotes the free monoid and free semigroup generated by $A$, respectively, and $\delta$ is extended from $X \times A$ to $X \times A^*$. In this case, $\delta(x, s)$ is denoted simply by $xs$ for $x \in X$, $s \in A^*$.

Let $\rho = \{(s, t) \in A^* \times A^* : xs = xt$ for every $x \in X\}$. Then $\rho$ is a congruence on $A^*$ and $A^*/\rho$ is a finite transformation semigroup on $X$ by defining the action of $s\rho \in A^*/\rho$ on $X$ as $x(s\rho) = xs$. The semigroup $A^*/\rho$ is called the characteristic semigroup of $\mathcal{A}$. Let $\mathcal{V}$ be a class of semigroups not necessarily a variety. Then an automaton $\mathcal{A}$ is called a $\mathcal{V}$-type if $A^*/\rho \in \mathcal{V}$.

For $s \in A^*$, let $\text{im } s = \{xs : x \in X\} = Xs$ and $\text{ker } s = \{(x, y) \in X \times X : xs = ys\}$, which are called the image and the kernel of $s$, respectively. Then $\text{ker}(s)$ is an equivalence on $X$.

Let $\mathcal{V}$ and $\mathcal{U}$ be two classes of semigroups. Then the direct product of $\mathcal{V}$ and $\mathcal{U}$ is defined by $\mathcal{V} \times \mathcal{U} = \{V \times U : V \in \mathcal{V}, U \in \mathcal{U}\}$. Let $U \in \mathcal{U}$
and let $S$ be a semigroup. If for each $s \in V$, there exists $U_s \in \mathcal{U}$ such that $S = \sqcup\{U_s : s \in U\}$ and $U_s \cdot U_t = \{u_s u_t : u_s \in U_s, u_t \in U_t\} \subseteq U_{st}$, then we say that $S$ belongs to $\mathcal{V}(\mathcal{U})$, where $\sqcup$ denotes a disjoint union..

As our start, we consider the following classes of semigroups: $\mathcal{G} = \{\text{groups}\}$, $\mathcal{LZ} = \{\text{left zero semigroups } [st = s]\}$, $\mathcal{RZ} = \{\text{right zero semigroups } [st = t]\}$ and $\mathcal{SL} = \{\text{semilattices } [st = ts, s^2 = s]\}$. We first characterize, for the classes $\mathcal{G}, \mathcal{LZ} \times \mathcal{G}, \mathcal{G} \times \mathcal{RZ}$ and $\mathcal{LZ} \times \mathcal{G} \times \mathcal{RZ}$, their types automata by the images and the kernels of their transition functions. By using the results, we characterize, for $\mathcal{V} \in \{\mathcal{SL}, \mathcal{LZ}, \mathcal{RZ}\}$ and $\mathcal{U} \in \{\mathcal{G}, \mathcal{LZ} \times \mathcal{G}, \mathcal{G} \times \mathcal{RZ}, \mathcal{LZ} \times \mathcal{G} \times \mathcal{RZ}\}$, $\mathcal{V}(\mathcal{U})$-type automaton by the same way.

1 This is an abstract and the details will be published elsewhere.
For a example, we show later that an automaton $A$ is a $\mathcal{S\mathcal{L}(\mathcal{L\mathcal{Z \times G}})}$-type if and only if $\text{im } st = \text{im } s \cap \text{im } t$ for every $s, t \in A^+$.

2. Preliminaries

For a set $Y$, $|Y|$ denotes the cardinality of $Y$, for an equivalence $\lambda$, $x\lambda$ denotes the $\lambda$-class containing $x$ and $|\lambda|$ denotes the number of $\lambda$-classes, i.e., $|\lambda| = |\{x\lambda : x \in X\}|$, and for $s \in A^+$, $|s|$ denotes the length of $s$. Then clearly $|\text{im } s| = |\text{ker } s|$ for every $s \in A^+$.

For $s \in A^*$, let fix $s = \{x \in X : xs = x\}$. Let $E(A^+) = \{e \in A^+ : (e, e^2) \in \rho\}$. Then it is easy to see that $e \in E(A^+)$ if and only if $\text{im } e = \text{fix } e$. and that $(e, f) \in \rho$ for $e, f \in E(A^+)$ if and only if $\text{im } e = \text{im } f$ and $\text{ker } e = \text{ker } f$. Since $A^+ / \rho$ is finite, for every $s \in A^+$, there exists a positive integer $m$ such that $s^m \in E(A^+)$.

**Lemma 1.** Let $s, t \in A^+$. Then

1. If $|\text{ker } st| = |\text{ker } t|$, then $\text{im } st = \text{im } t$.
2. If $|\text{im } st| = |\text{im } s|$, then $\text{ker } st = \text{ker } s$.

**Lemma 2.** Let $s \in A^+$. Then the following are equivalent:

1. $\text{im } s \cap x\ker s \neq \emptyset$ for every $x \in X$.
2. $\text{im } s^m = \text{im } s$ and $\ker s^m = \ker s$ for every $m \in \mathbb{N}^+$.
3. There exists $e \in E(A^+)$ such that $\text{im } s = \text{im } e$, $\ker s = \ker e$, $(s, se) \in \rho$ and $(s, es) \in \rho$.

**Lemma 3.** The following are equivalent:

For every $s, t \in A^+$,

1. $\text{im } s \cap x\ker t \neq \emptyset$ for every $x \in X$,
2. $\text{im } st = \text{im } t$.
3. $\ker st = \ker s$.

Let $A = (X, A, \delta)$ be an automaton, and let $Y = \cup \{\text{im } a : a \in A\}$ and $\kappa = \cap \{\ker a : a \in A\}$. Then we have $Y = \cup \{\text{im } s ; s \in A^+\}$ and $\kappa = \cap \{\ker s ; s \in A^+\}$. In fact, if $s \in A^+$, then $s = s'a = bs^n$ for some $a, b \in A, s's^n \in A^*$, so that $\text{im } s'a \subseteq \text{im } a$ and $\ker b \subseteq \ker bs^n$.

Since $Ys \subseteq Y$ for every $s \in A^+$, the restriction $s_Y$ of $s$ to $Y$ can be defined. Let $A_Y = \{a_Y : a \in A\}$. Then the automaton $A_Y = (Y, A_Y, \delta)$ is called the *subautomaton of $A$ with respect to $Y$*.

Let $s, t \in A^+$ and $x \in X$. Since $(xs)t_Y = (xs)t$, the action of $st_Y$ on $X$ is defined by $x(st_Y) = x(st)$.
Let $\kappa$ be as above. Define the action of $s \in A^+$ on $X/\kappa$ by $(x\kappa)s = (xs)\kappa$. Then the action is well-defined. In fact, if $x\kappa = y\kappa$, then $(x, y) \in \kappa \subseteq \ker s$, so that $xs = ys$. When the action of $s$ is on $X/\kappa$, $s$ is denoted by $s_{\kappa}$. Let $A_{\kappa} = \{a_{\kappa} : a \in a\}$. Then the automaton $A_{\kappa} = (X/\kappa, A_{\kappa}, \delta)$ is called the automaton induced from $A$ by $\kappa$.

Let $s, t \in A^+$ and $x \in X$. Then clearly $(x\ker s)s = xs$. Since $\kappa \subseteq \ker s$, we have $(x\kappa)s = xs$, so that $((x\kappa)s_{\kappa})t = ((xs)\kappa)t = (xs)t$, Thus the action of $s_{\kappa}t$ on $X$ is defined by $x(s_{\kappa}t) = x(st)$.

For an automaton $A = (X, A, \delta)$, let $Im(A^+) = \{\text{im } s : s \in A^+\} = \{Y_i : i \in I\}$, i.e., for each $i \in I$, $Y_i = \text{im } s$ for some $s \in A^+$ and $\text{im } s \in Im(A^+)$ for every $s \in A^+$, and let $Ker(A^+) = \{\ker s : s \in A^+\} = \{\kappa_\mu : \mu \in \mathcal{M}'\}$, $Im(A^\kappa) = \{\text{im } s_\kappa : s \in A^+\} = \{Z_i : i \in I'\}$ and $Ker(A^\kappa) = \{\ker s_Y : s \in A^+\} = \{\kappa_\mu : \mu \in \mathcal{M}'\}$. In this case, if $\text{im } s \cap \ker s \neq \emptyset$ holds for every $s \in A^+$ and $x \in X$, then $Im(A^+) = Im(E(A^+))$ and $Ker(A^+) = Ker(E(A^+))$.

3. Main Results

A semigroup in $\mathcal{LZ} \times \mathcal{G}$ is called a left group whose class is denoted simply by $\mathcal{LG}$, i.e., $\mathcal{LG} = \mathcal{LZ} \times \mathcal{G}$.

**Theorem 1.** Let $A = (X, A, \delta)$ be an automaton. Then the following are equivalent:

1. There exists a subset $Y$ of $X$ such that $\text{im } a = Y$ and $Y \cap x\ker a \neq \emptyset$ for every $a \in A$ and $x \in X$.
2. There exists a subset $Y$ of $X$ such that $\text{im } s = Y$ for every $s \in S$.
3. $A$ is a left group type.

From Theorem 1 we obtain the following results.

**Corollary 1.1.** An automaton $A = (X, A, \delta)$ is a $\mathcal{SL}(\mathcal{LG})$-type if and only if $\text{im } st = \text{im } s \cap \text{im } t$ for every $s, t \in A^+$.

**Corollary 1.2.** An automaton $A = (X, A, \delta)$ is a $\mathcal{RZ}(\mathcal{LG})$-type if and only if $\text{im } st = \text{im } t$ for every $s, t \in A^+$.

A semigroup in $\mathcal{G} \times \mathcal{RZ}$ is called a right group whose class is denoted by $\mathcal{RG}$, i.e., $\mathcal{RG} = \mathcal{G} \times \mathcal{RZ}$.

**Theorem 2.** Let $A = (X, A, \delta)$ be an automaton. Then the following are equivalent:
(1) There exists an equivalence \( \kappa \) on \( X \) such that \( \ker a = \kappa \) and \( \im a \cap x \kappa \neq \emptyset \) for every \( a \in A \).

(2) There exists an equivalence \( \kappa \) on \( X \) such that \( \ker s = \kappa \) for every \( s \in A^+ \).

(3) \( A \) is a right group type.

**Corollary 2.1.** An automaton \( A = (X, A, \delta) \) is a \( SL(RG) \)-type if and only if \( \ker st = \ker s \vee \ker t \) for every \( s, t \in A^+ \).

**Corollary 2.2.** An automaton \( A = (X, A, \delta) \) is a \( LZ(RG) \)-type if and only if \( \im st = \im t \) for every \( s, t \in A^+ \).

From Corollaries 1.2 and 2.2 we obtain:

**Corollary 2.3.** An automaton \( RZ(LG) \)-type if and only if it is \( LZ(RG) \)-type.

**Remark.** It can be easily show that \( LZ(LG) = LZ(G) = LG \) and \( RZ(RG) = RZ(G) = RG \).

**Theorem 3.** Let \( A = (X, A, \delta) \) be an automaton. Then the following are equivalent:

(1) There exist a subset \( Y \) of \( X \) and an equivalence \( \kappa \) on \( X \) such that \( \im a = Y \) and \( \ker a = \kappa \) for every \( a \in A \) and \( Y \cap x \kappa \neq \emptyset \) for every \( x \in X \).

(2) There exist a subset \( Y \) of \( X \) and an equivalence \( \kappa \) on \( X \) such that \( \im s = Y \) and \( \ker s = \kappa \) for every \( s \in A^+ \),

(3) \( A \) is a group-type.

A semigroup in \( SL(G) \) is called a Cliford semigroup,

**Corollary 3.1.** An automaton \( A = (X, A, \delta) \) is a Cliford smigroup type if and only if \( \im st = \im s \cap \im t \) and \( \ker st = \ker s \vee \ker t \) for every \( s, t \in A^+ \).

**Theorem 4.** Let \( A = (X, A, \delta) \) be an automaton, and Let \( Y = \cup \{ \im a : a \in A \}, \kappa = \cap \{ \ker a : a \in A \} \). Suppose that \( \im s \cap x \ker s \neq \emptyset \) for every \( s \in A^+ , x \in X \). Then the following are equivalent:

(1) \( A \) is a \( LZ \times G \times RZ \)-type.

(2) \( \ker s_\kappa = \ker t_\kappa \) for every \( s, t \in A^+ \).

(3) \( \im s_\kappa = \im t_\kappa \) for every \( s, t \in A^+ \).

**Corollary 4.1.** With the assumption of Theorem 4, the following are equivalent:

(1) \( A \) is a \( SL(LZ \times G \times RZ) \)-type.
(2) \( \ker s_Y t_Y = \ker s_Y \lor \ker t_Y \) for every \( s, t \in A^+ \).
(3) \( \im s_\kappa t_\kappa = \im s_\kappa \cap \im t_\kappa \) for every \( s, t \in A^+ \).

Suppose that an automaton \( A \) is a \( \mathcal{L} \mathcal{Z} \times \mathcal{G} \times \mathcal{R} \mathcal{Z} \)-type. As is seen in the proof of Theorem 4, \( A^+ / \rho = \{(i, g, \mu) : i \in I, g \in G, \mu \in M\} \). For \( i \in I \) and \( \mu \in M \), let \( A_i / \rho = \{(i, g, \mu) : g \in G, \mu \in M\} \) and \( A_\mu = \{(i, g, \mu) : i \in I, g \in G\} \), respectively. Then \( A_i / \rho \in \mathcal{RG} \) and \( A_\mu / \rho \in \mathcal{LG} \). For \( s \rho = (i, g, \nu), t \rho = (j, h, \mu) \), since \( (st) \rho = (i, gh, \mu) \), by Theorems 1 and 2, we have \( \ker st = \ker s \) and \( \im st = \im t \). Thus we obtain:

**Corollary 4.2.** If an automaton \( A \) is a \( \mathcal{L} \mathcal{Z} \times \mathcal{G} \times \mathcal{R} \mathcal{Z} \)-type, then it is a \( \mathcal{R} \mathcal{Z}(\mathcal{L} \mathcal{G}) \)-type. The converse is not true.

There is a simple example that a \( \mathcal{R} \mathcal{Z}(\mathcal{L} \mathcal{G}) \)-type automaton which is not a \( \mathcal{L} \mathcal{Z} \times \mathcal{G} \times \mathcal{R} \mathcal{Z} \)-type.

**References**


