On Complexity of Finite Moore Automata

By Masashi Katsura

The concept of complexity of finite Moore automata is introduced by Ádám [1]. In this paper, we obtain relationships among complexity and cardinalities of state set, input set and output set of a Moore automaton.

1.

For a finite set Z, the cardinality of Z is denoted by $|Z|$. Z^* is the free monoid generated by Z. $\mathbf{N}$ is the set of positive integers and $\mathbf{N}^\circ$ is the set of nonnegative integers. For $t, k, \in \mathbf{N}^\circ$, we set $[t: k]=\{i \in \mathbf{N}^\circ | t \leqq i \leqq k\}$.

By a *Moore automaton*, we mean a 5-tuple $\mathbf{A}=(A, X, Y, \delta, \lambda)$, where A, X, Y are finite nonempty sets called a state set, an input set and an output set, respectively. δ is a mapping of $A \times X$ into A called a state transition function (δ is extended as usual to a mapping of $A \times X^*$ into A). λ is a mapping of A *onto* Y called an output function.

Let $\mathbf{A}=(A, X, Y, \delta, \lambda)$ be a Moore automaton. If $\lambda(\delta(a, p)) \neq \lambda(\delta(b, p))$ holds for $a, b \in A$ and $p \in X^*$, then we say that p distinguishes between a and b. $\omega_{\mathbf{A}}(a, b)$ is the minimal length of p which distinguishes between a and b. If there is no word which distinguishes between a and b, then we write $\omega_{\mathbf{A}}(a, b)=\infty$. *The complexity* $\Omega(\mathbf{A})$ of the Moore automaton $\mathbf{A}$ is defined by $\Omega(\mathbf{A})=\max \{\omega_{\mathbf{A}}(a, b) | a, b \in A, a \neq b\}$. If $|A|=1$ then $\Omega(\mathbf{A})=0$.

A Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$ is said to be *initially connected* if a distinguished state $a_0 \in A$, called the *initial state* of A, is given and the following condition is satisfied: For any $a \in A$, there exists a $p \in X^*$ such that $\delta(a_0, p)=a$.

Let $v, n \in \mathbf{N}$ and $w \in \mathbf{N}^\circ \cup \{\infty\}$. If there exists an (initially connected) Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$ such that $|A|=v$, $|X|=n$ and $\Omega(\mathbf{A})=w$, then the triple (v, n, w) is said to be *realizable* by (initially connected) Moore automata.

We have the following theorem by summarizing the results of Ádám in [2], [3], [4].

Theorem 1. For any $v, n \in \mathbf{N}$ and $w \in \mathbf{N}^\circ \cup \{\infty\}$, the following three statements are equivalent:

(1) (v, n, w) is realizable by Moore automata.

(2) (v, n, w) is realizable by initially connected Moore automata.

(3) (3.1) $w \leqq v-2$, or

(3.2) $v = 1, \quad w = 0,$ or

(3.3) $v \geqq 2, \quad w = \infty.$ □

When we realize a triple (v, n, w) for a small w, a large output set is needed, and vice versa. We wish to take consideration on cardinalities of output sets, too.

Let $v, n, m \in \mathbf{N}$ and $w \in \mathbf{N}^\circ \cup \{\infty\}$. If there exists an (initially connected) Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$ such that $|A|=v$, $|X|=n$, $|Y|=m$ and $\Omega(\mathbf{A})=w$, then the 4-tuple (v, n, m, w) is said to be *realizable* by (initially connected) Moore automata.

In this paper, all realizable 4-tuples are completely determined. Section 2 gives a sufficient condition. Section 4 is a preparation to show that the sufficient condition given in Section 2 is necessary. In Section 5, the main result is stated and proved. Section 6 illustrates some examples. In Section 3, we prove a conjecture posed in [3].

2.

Let X and Y be finite nonempty sets and let $t \in \mathbf{N}^\circ$. By $F_t(X, Y)$ we denote the set of all mappings of $\bigcup_{k=0}^{t} X^k$ into Y.

The following lemma is evident.

Lemma 1. $|F_t(X, Y)| = |Y|^{1+|X|+|X|^2+\cdots+|X|^t}$ for any $t \in \mathbf{N}^\circ$. □

Let $\mathbf{A}=(A, X, Y, \delta, \lambda)$ be a Moore automaton. For each $a \in A$, let $\lambda^*(a)$ be a mapping of X^* into Y defined by

$$(\lambda^*(a))(p) = \lambda(\delta(a, p)).$$

For $t \in \mathbf{N}^\circ$, $\lambda^{(t)}(a)$ is an element of $F_t(X, Y)$ which is the restriction of $\lambda^*(a)$ to $\bigcup_{k=0}^{t} X^k$. Hence $\lambda^{(0)}=\lambda$ if we identify $F_0(X, Y)$ with Y.

For each $t \in \mathbf{N}^\circ$, let $\eta_t(\mathbf{A})$ be a partition of A defined as follows: a and b are congruent modulo $\eta_t(\mathbf{A})$ iff $\omega_{\mathbf{A}}(a, b) \geqq t$. $\eta_t(\mathbf{A})$ is introduced and investigated in [2], [4]. The number of $\eta_t(\mathbf{A})$-classes is denoted by $|\eta_t(\mathbf{A})|$. The following three lemmas indicate fundamental properties of the partition $\eta_t(\mathbf{A})$.

Lemma 2 [4]. $\eta_0(\mathbf{A}) \supseteq \eta_1(\mathbf{A}) \supseteq \eta_2(\mathbf{A}) \supseteq \cdots$. □

Lemma 3 [4]. If $\eta_{t-1}(\mathbf{A})=\eta_t(\mathbf{A})$ then $\eta_t(\mathbf{A})=\eta_{t+1}(\mathbf{A})$. □

Lemma 4. Let $w \in \mathbf{N}^\circ$. Then $\Omega(\mathbf{A})=w$ iff $\eta_w(\mathbf{A}) \supsetneqq \eta_{w+1}(\mathbf{A})$ and $|\eta_{w+1}(\mathbf{A})| = |A|$. □

By using the mapping $\lambda^{(t)}(a)$, the partition $\eta_t(A)$ is characterized as follows:

Lemma 5. a and b are congruent modulo $\eta_{t+1}(\mathbf{A})$ iff $\lambda^{(t)}(a)=\lambda^{(t)}(b)$. □

Hence we have:

Lemma 6. $|\eta_{t+1}(\mathbf{A})| = |\{\lambda^{(t)}(a) \in F_t(X, Y) | a \in A\}|$ for any $t \in \mathbf{N}^\circ$. □

Expecially, we have:

Lemma 7. $|\eta_{t+1}(\mathbf{A})| \leqq |Y|^{1+|X|+|X|^2+\cdots+|X|^t}$ for any $t \in \mathbf{N}^\circ$. □

On the other hand, a lower bound of the number of $\eta_t(\mathbf{A})$-classes is given as follows:

Lemma 8. Let $t \in \mathbf{N}^\circ$. If $t \leqq \Omega(\mathbf{A})$ then $|\eta_{t+1}(\mathbf{A})| \geqq |Y|+t$.

Proof. By Lemmas 2, 3 and 4, we have $\eta_1(\mathbf{A}) \supsetneqq \eta_2(\mathbf{A}) \supsetneqq \ldots \supsetneqq \eta_t(\mathbf{A}) \supsetneqq \eta_{t+1}(\mathbf{A})$, i.e., $|\eta_1(\mathbf{A})| < |\eta_2(\mathbf{A})| < \ldots < |\eta_t(\mathbf{A})| < |\eta_{t+1}(\mathbf{A})|$. Hence $|\eta_{t+1}(\mathbf{A})| \geqq |\eta_1(\mathbf{A})|+t$. By Lemma 6, we have $|\eta_1(\mathbf{A})| = |Y|$. □

Now, we have the following desired result.

Proposition 1. Let $v, n, m \in \mathbf{N}$ and $w \in \mathbf{N}^\circ$. If the 4-tuple (v, n, m, w) is realizable by Moore automata then $m+w \leqq v \leqq m^{1+n+n^2+\cdots+n^w}$.

Proof. Let $\mathbf{A}=(A, X, Y, \delta, \lambda)$ be a Moore automaton such that $|A|=v$, $|X|=n$, $|Y|=m$ and $\Omega(\mathbf{A})=w$. By Lemma 4, $|\eta_{w+1}(\mathbf{A})|=v$. By Lemmas 7 and 8, we have $m+w \leqq |\eta_{w+1}(\mathbf{A})| \leqq m^{1+n+n^2+\cdots+n^w}$. □

3.

Ádám posed three conjectures in [3]. Conjectures 1 and 2 are solved in Theorem 1. However, Conjecture 3 is not yet solved. In this section, we settle this conjecture. (This result is not used in what follows).

Let $\mathbf{A}=(A, X, Y, \delta, \lambda)$ be a Moore automaton such that $1 \leqq \Omega(\mathbf{A}) < \infty$. Put $\Omega(\mathbf{A})=w$. Take $a, b \in A$ such that $\omega_{\mathbf{A}}(a, b)=w$. Then there exists a $q \in X^w$ such that $\lambda(\delta(a, q)) \neq \lambda(\delta(b, q))$. Let $q=q'x$ with $q' \in X^{w-1}$ and $x \in X$. Let B be the $\eta_2(\mathbf{A})$-class containing $\delta(a, q')$, i.e., $B=\{c \in A \mid \lambda(\delta(c, p))=\lambda(\delta(a, q'p))$ for any $p \in X \cup \{e\}\}$, where e is the identity of X^*.

Define $\mathbf{A}'=(A, X, Y', \delta, \lambda')$ as follows:

(i) $Y'=Y \cup \{y\}$ where y is not in Y.
(ii) $\lambda'(c)=y$ for any $c \in B$.
(iii) $\lambda'(c)=\lambda(c)$ for any $c \in A-B$.

Since $\lambda(\delta(a, q'x)) \neq \lambda(\delta(b, q'x))$, we have $\delta(b, q') \notin B$. Hence $\lambda'(\delta(b, q')) = \lambda(\delta(b, q')) = \lambda(\delta(a, q'))$. Consequently, λ' is surjective. Moreover, we have:

Lemma 9. (1) $\eta_t(\mathbf{A}) \supseteq \eta_t(\mathbf{A}')$ for any $t \in \mathbf{N}^\circ$.
(2) $\eta_w(\mathbf{A}) \supsetneqq \eta_w(\mathbf{A}')$.
(3) $\eta_{w-1}(\mathbf{A}')$ is not the identity partition.

Proof. (1) It is obvious that for any $c, d \in A$, if $\lambda(c) \neq \lambda(d)$, then $\lambda'(c) \neq \lambda'(d)$. It follows from this fact that $\omega_{\mathbf{A}'}(c, d) \leqq \omega_{\mathbf{A}}(c, d)$ for any $c, d \in A$.

(2) Since $\lambda'(\delta(a, q')) \neq \lambda(\delta(a, q')) = \lambda(\delta(b, q')) = \lambda'(\delta(b, q'))$, we have $\omega_{\mathbf{A}'}(a, b) \leqq w-1$. Hence a and b are congruent modulo $\eta_w(\mathbf{A})$, but not congruent modulo $\eta_w(\mathbf{A}')$.

(3) It suffices to show that $\omega_{\mathbf{A}'}(a, b)=w-1$. When $w=1$, the conclusion is obvious. Assume $w \geqq 2$ and $\omega_{\mathbf{A}'}(a, b) \leqq w-2$. Then there exists a $p \in \bigcup_{k=0}^{w-2} X^k$ such that $\lambda'(\delta(a, p)) \neq \lambda'(\delta(b, p))$. Since $\lambda(\delta(a, p)) = \lambda(\delta(b, p))$, we have $\delta(a, p) \in B$

and $\delta(b,p)\notin B$, or vice versa. In other words, $\delta(a,p)$ and $\delta(b,p)$ are not congruent modulo $\eta_2(A)$. For any $p'\in X\cup\{e\}$, we have $pp'\in\bigcup_{k=0}^{w-1}X^k$. Hence $\lambda(\delta(a,pp'))=\lambda(\delta(b,pp'))$ for any $p'\in X\cup\{e\}$. This means that $\delta(a,p)$ and $\delta(b,p)$ are congruent modulo $\eta_2(\mathbf{A})$. This is a contradiction. Hence we have $\omega_{\mathbf{A}'}(a,b)=w-1$. □

Proposition 2 ([3] Conjecture 3). Let $\mathbf{A}=(A,X,Y,\delta,\lambda)$ be a Moore automaton such that $1\leqq\Omega(\mathbf{A})<\infty$. Then there exists a Moore automaton $\mathbf{A}'=(A,X,Y',\delta,\lambda')$ such that $|Y'|=|Y|+1$ and $\Omega(\mathbf{A})-1\leqq\Omega(\mathbf{A}')\leqq\Omega(\mathbf{A})$.

Proof. Let $\mathbf{A}'$ be the Moore automaton constructed as above. Lemma 9 (1) implies that $\Omega(\mathbf{A}')\leqq\Omega(\mathbf{A})$. Lemma 9 (3) means that $\Omega(\mathbf{A}')\geqq\Omega(\mathbf{A})-1$. □

As pointed out in [3], we get an automaton of complexity 0 by at most $|A|-|Y|$ times application of Proposition 2. Hence we have another proof of the left hand side inequality of Proposition 1.

4.

In this section, we prepare for showing the converse of Proposition 1. Throughout this section, we assume that $X=\{x_1,\ldots,x_n\}$, $Y=\{y_1,\ldots,y_m\}$ and $m\geqq 2$. $F_t(X,Y)$ is simply denoted by F_t. F_{-1} means the singleton set consisting of the empty mapping, i.e., the mapping whose definition domain is the empty set.

Let $t\in\mathbf{N}^\circ$ and $f\in F_t$. We define $f_l, f_{r,1},\ldots,f_{r,n}\in F_{t-1}$ as follows:

$$f_l \text{ is the restriction of } f \text{ to } \bigcup_{k=0}^{t-1}X^k,$$

$$f_{r,j}(p)=f(x_jp) \text{ for any } p\in\bigcup_{k=0}^{t-1}X^k \quad (j\in[1:n]).$$

Hence for $f\in F_0$, f_l and $f_{r,j}$ are the empty mappings. f_l is said to be the *left factor* of f, and $f_{r,j}$ is its *j-th right factor*.

The following lemma can be shown by a straightforward verification.

Lemma 10. Let $t\in\mathbf{N}^\circ$ and $g\in F_{t-1}$. Then $|\{f\in F_t|f_l=g\}|=|\{f\in F_t|f_{r,j}=g\}|=|F_t|/|F_{t-1}|=m^{n^t}$. □

Let $\mathbf{A}=(A,X,Y,\delta,\lambda)$ be a Moore automaton. Consider the mapping $\lambda^{(t)}$ of A into F_t. The assumption that λ is surjective is equivalent to:

(i) For any $j\in[1:n]$, there exists an $a\in A$ such that $(\lambda^{(t)}(a))(e)=y_j$, where e is the identity of X^*.

If $\delta(a,x_j)=b$, then $(\lambda^{(t)}(a))_{r,j}=(\lambda^{(t)}(b))_l$. Hence we have:

(ii) For any $a\in A$ and $j\in[1:n]$, there exists a $b\in A$ such that $(\lambda^{(t)}(a))_{r,j}=(\lambda^{(t)}(b))_l$.

$\Omega(\mathbf{A})=t$ is equivalent to:

(iii) $\lambda^{(t)}$ is injective, and $(\lambda^{(t)}(a))_l=(\lambda^{(t)}(b))_l$ for some $a,b\in A$ with $a\neq b$.

Conversely, assume that a mapping τ of A into F_t which satisfies (i) and (ii) is given. Define a Moore automaton $\mathbf{A}_\tau=(A,X,Y,\delta,\lambda)$ as follows:

(iv) $\lambda(a)=(\tau(a))(e)$ for any $a\in A$.

(v) Let $a\in A$ and $j\in[1:n]$. By (ii), there exists a $b\in A$ such that $\tau(a)_{r,j}=\tau(b)_l$. Set $\delta(a, x_j)=b$.

Then it can easily be seen that $\lambda^{(t)}(a)=\tau(a)$ holds for any $a\in A$. $\mathbf{A}_\tau$ is not unique in general. The collection of all $\mathbf{A}_\tau$ coincides with all Moore automata $\mathbf{A}=(A, X, Y, \delta, \lambda)$ which satisfy $\lambda^{(t)}=\tau$. The partitions $\eta_0(\mathbf{A}_\tau), \eta_1(\mathbf{A}_\tau), \ldots, \eta_{t+1}(\mathbf{A}_\tau)$ are independent of the choice of b in (v), i.e., they depend only on the mapping τ.

To show the converse of Proposition 1, it suffices to give a mapping τ of A into F_t which satisfies (i), (ii) and (iii) for each finite set A with $m+t\leqq|A|\leqq m^{1+n+n^2+\cdots+n^t}$. However, we wish to prove the converse of Proposition 1 in case of initially connected Moore automata. Related problem is:

Let τ be a mapping satisfying (i) and (ii) (and (iii)). What conditions are required so that we can make $\mathbf{A}_\tau$ to be initially connected? What is a method to construct an initially connected $\mathbf{A}_\tau$, when it exists?

In general, this problem seems to be difficult. In what follows, we construct a special type of mapping τ, and construct a special type of initially connected Moore automaton $\mathbf{A}_\tau$.

Let $t\in\mathbf{N}^\circ$, $s\in\mathbf{N}$ and let π be an injection of $[1:s]$ into F_t. If the following four conditions are satisfied then π is called an *op-mapping* of *degree* (t, s) (with respect to X and Y).

(a) For any $g\in F_{t-1}$, there exists an $i\in[1:s]$ such that $\pi(i)_l=g$.

(b) For any $j\in[1:m]$, there exists an $i\in[1:s]$ such that $(\pi(i))(e)=y_j$.

(c) $\pi(i)_{r,1}=\pi(i+1)_l$ for any $i\in[1:s-1]$.

(d) There exists an $i_\pi\in[1:s-1]$ such that $(\pi(i_\pi))(p)=y_1$ for any $p\in\bigcup_{k=0}^{t} X^k$.

(Since π is injective, i_π is uniquely determined).

When $t\geqq 1$, the assertion (b) is implied by (a). When $t=0$, the assertions (a) and (c) are always satisfied, and the assertion (b) means that π is surjective. Hence an op-mapping π of degree $(0, s)$ is considered as a bijection of $[1:s]$ onto Y such that $\pi(i)=y_1$ for some $i\in[1:s-1]$. Thus we have:

Lemma 11. There exists an op-mapping of degree $(0, s)$ iff $s=m$. □

Lemma 12. Let $t, s\in\mathbf{N}$. If there exists an op-mapping π of degree (t, s) then $m^{1+n+n^2+\cdots+n^{t-1}}+1\leqq s\leqq m^{1+n+n^2+\cdots+n^t}$.

Proof. Since π is injective, we have $s\leqq|F_t|$. We have $\pi(i_\pi)_l=\pi(i_\pi)_{r,1}$. Since $i_\pi\in[1:s-1]$, we have $i_\pi+1\in[1:s]$ and $\pi(i_\pi+1)_l=\pi(i_\pi)_{r,1}=\pi(i_\pi)_l$. From this fact and by the assertion (a), it follows that $s\geqq|F_{t-1}|+1$. □

Now we shall construct an op-mapping of degree (t, s) for any $t, s\in\mathbf{N}$ with $m^{1+n+n^2+\cdots+n^{t-1}}+1\leqq s\leqq m^{1+n+n^2+\cdots+n^t}$. To this end, we provide the following two lemmas.

Lemma 13. Let π be an op-mapping of degree (t, s). Then the following statements are equivalent:

(1) There exists an op-mapping π' of degree $(t, s+1)$ which is an extension of π.

(2) There exists an $f\in F_t-\{\pi(i)\mid i\in[1:s]\}$ such that $f_l=\pi(s)_{r,1}$.

Proof. (1)⇒(2). By the assertion (c), we have $\pi'(s+1)_l=\pi'(s)_{r,1}=\pi(s)_{r,1}$. Since π' is injective, $\pi'(s+1)\in F_t-\{\pi(i)\,|\,i\in[1:s]\}$.
(2)⇒(1). Let $\pi'(s+1)=f$ and $\pi'(i)=\pi(i)$ for any $i\in[1:s]$. Then π' is an op-mapping of degree $(t, s+1)$. □

Lemma 14. Let π be an op-mapping of degree (t, s). Assume that there exists no op-mapping π' of degree $(t, s+1)$ which is an extension of π. Then $\pi(s)_{r,1}=\pi(1)_l$.

Proof. If $t=0$ then $\pi(s)_{r,1}$ and $\pi(1)_l$ are the empty mappings. Hence the conclusion holds obviously. Assume that $t\in\mathbf{N}$. Let

$$I=\{i\in[1:s]\,|\,\pi(i)_l=\pi(s)_{r,1}\} \quad \text{and}$$

$$J=\{j\in[1:s]\,|\,\pi(j)_{r,1}=\pi(s)_{r,1}\}.$$

Suppose that $|I|<m^{n^t}$. Then, by Lemma 10, there exists an $f\in F_t-\{\pi(i)|i\in[1:s]\}$ such that $f_l=\pi(s)_{r,1}$. It contradicts the assumption by Lemma 13. Hence we have $|I|=m^{n^t}$. By Lemma 10, we have $|J|\leqq|I|$. By the assertion (c), we have:

If $i\in I-\{1\}$, then $i-1\in J$.

If $j\in J-\{s\}$, then $j+1\in I$.

Hence $|I-\{1\}|=|J-\{s\}|$. Since $s\in J$, we have

$$|I|\geqq|J|=|J-\{s\}|+1=|I-\{1\}|+1.$$

Thus, we have $1\in I$, i.e., $\pi(1)_l=\pi(s)_{r,1}$. □

There exists an op-mapping of degree $(0, m)$ (Lemma 11). Hence to construct an op-mapping of degree (t, s) for each $t,s\in\mathbf{N}$ with $m^{1+n+n^2+\cdots+n^{t-1}}+1\leqq s\leqq m^{1+n+n^2+\cdots+n^t}$, it suffices to give construction methods for the following two cases:

(I) Let $t\in\mathbf{N}$ and $s=m^{1+n+n^2+\cdots+n^{t-1}}+1$. Assume that an op-mapping π of degree $(t-1, s-1)$ is given. Construct an op-mapping π' of degree (t, s).

(II) Let $t, s\in\mathbf{N}$ and $m^{1+n+n^2+\cdots+n^{t-1}}+2\leqq s\leqq m^{1+n+n^2+\cdots+n^t}$. Assume that an op-mapping π of degree $(t, s-1)$ is given. Construct an op-mapping π' of degree (t, s).

Case (II) is divided into the following two subcases:

(II.1) There exists an $f\in F_t-\{\pi(i)\,|\,i\in[1:s-1]\}$ such that $f_l=\pi(s-1)_{r,1}$.
(II.2) There exists no $f\in F_t-\{\pi(i)\,|\,i\in[1:s-1]\}$ such that $f_l=\pi(s-1)_{r,1}$.

Construction (I). (i) Define a mapping σ of $[2:s]$ into F_{t-1} as follows:

$$\sigma(2)=\pi(i_\pi),\ \sigma(3)=\pi(i_\pi+1),\ \ldots,\ \sigma(s-i_\pi+1)=\pi(s-1),$$

$$\sigma(s-i_\pi+2)=\pi(1),\ \sigma(s-i_\pi+3)=\pi(2),\ \ldots,\ \sigma(s)=\pi(i_\pi-1)$$

where i_π is determined in the assertion (d). (By Lemmas 11 and 12, π satisfies the assumption of Lemma 14. Hence $\pi(s-1)_{r,1}=\pi(1)_l$. Thus, we have $\sigma(i)_{r,1}=\sigma(i+1)_l$ for any $i\in[2:s-1]$.)
(ii) Define a mapping π' of $[1:s]$ into F_t as follows:

$$(\pi'(1))(p)=y_1 \quad \text{for any } p\in\bigcup_{k=0}^{t}X^k.$$

Let $i\in[2: s-1]$. Take an $f\in F_t$ such that $f_l=\sigma(i)$ and $f_{r,1}=\sigma(i+1)$. (The existence of such an f follows from $\sigma(i)_{r,1}=\sigma(i+1)_l$). Set $\pi'(i)=f$.

Take an $f\in F_t$ such that $f_l=\sigma(s)$. (The existence of such an f is evident.) Set $\pi'(s)=f$.

Then it is not difficult to verify that π' is an op-mapping of degree (t, s).

Construction (II.1). Take an $f\in F_t-\{\pi(i)\mid i\in[1: s-1]\}$ such that $f_l=\pi(s-1)_{r,1}$. Set $\pi'(s)=f$ and $\pi'(i)=\pi(i)$ for any $i\in[1: s-1]$. Then $g\pi'$ is an op-mappin of degree (t, s).

Construction (II.2). (i) Take an $f\in F_t-\{\pi(i)\mid i\in[1: s-1]\}$.
(ii) Take an $i_0\in[1: s-1]$ such that $f_l=\pi(i_0)_l$. (The existence of such an i_0 follows from the assertion (a). If $i_0=1$, then $f_l=\pi(1)_l=\pi(s-1)_{r,1}$ which contradicts the assumption. Hence we have $i_0\in[2: s-1]$.)
(iii) Define a mapping π' of $[1: s]$ into F_t by

$$\pi'(1)=\pi(i_0),\ \pi'(2)=\pi(i_0+1),\ \ldots,\ \pi'(s-i_0)=\pi(s-1),$$

$$\pi'(s-i_0+1)=\pi(1),\ \ldots,\ \pi'(s-1)=\pi(i_0-1)\quad\text{and}\quad\pi'(s)=f.$$

By Lemmas 13 and 14, we have $\pi'(s-i_0)_{r,1}=\pi(s-1)_{r,1}=\pi(1)_l=\pi'(s-i_0+1)_l$. By the assertion (c), we have $\pi'(s-1)_{r,1}=\pi(i_0-1)_{r,1}=\pi(i_0)_l=f_l=\pi'(s)_l$. It can easily be seen that π' satisfies the other assertions for an op-mapping of degree (t, s).

We have shown the following.

Proposition 3. Let $t, s\in\mathbf{N}$. Then there exists an op-mapping of degree (t, s) iff $m^{1+n+n^2+\cdots+n^{t-1}}+1\leqq s\leqq m^{1+n+n^2+\cdots+n^t}$. □

Remark. Ito and Duske [5] shows the following:

Let Y be a finite nonempty set and let $t\in\mathbf{N}$. Then there exists a $p\in Y^*$ whose length is $|Y|^t+t-1$, and which contains every element of Y^t as a subword (such a word p is called a *merged word* of Y^t).

With a little change of the proof, we have Proposition 3 in case $|X|=1$. Our above constructions are done along the line of Ito and Duske. □

Let π be an op-mapping of degree (t, s) and let $r\in\mathbf{N}^\circ$. Define an automaton $\mathbf{A}(\pi, r)=(A, X, Y, \delta, \lambda)$ as follows:

(e) $A=\{a_1, \ldots, a_s, b_1, \ldots, b_r\}$. Put $b_0=a_{i_\pi}$ and $b_{r+1}=a_{i_\pi+1}$.
(f) $\lambda(a_i)=(\pi(i))(e)$ for any $i\in[1: s]$.
(g) $\lambda(b_i)=y_1$ for any $i\in[1: r]$.
(h) $\delta(a_i, x_1)=a_{i+1}$ for any $i\in[1: s-1]-\{i_\pi\}$.
(i) $\delta(b_i, x_j)=b_{i+1}$ for any $i\in[0: r]$ and $j\in[1: n]$.
(j) Let $(i, j)\in([1: s]-\{i_\pi\})\times[2: n]\cup\{(s, 1)\}$. By the assertion (a), there exists a $k\in[1: s]$ such that $\pi(i)_{r,j}=\pi(k)_l$. Set $\delta(a_i, x_j)=a_k$.

$\mathbf{A}(\pi, r)$ is not unique in general. (If we take the least k in (j), then $\mathbf{A}(\pi, r)$ is uniquely determined.)

It follows from the assertions (b) and (f) that λ is surjective. For any $c\in A$, there exists a $u\in\mathbf{N}^\circ$ such that $\delta(a_1, x_1^u)=c$. Hence $\mathbf{A}(\pi, r)$ is an initially connected Moore automaton with initial state a_1.

Lemma 15. $\lambda^{(t)}(a_i)=\pi(i)$ for any $i\in[1:s]$, and $(\lambda^{(t)}(b_i))(p)=y_1$ for any $i\in[1:r]$ and $p\in\bigcup_{k=0}^{t} X^k$.

Proof. For each: $u\in[0:t]$, we consider the following two conditions:

$(\mathscr{C}_u)$ $(\lambda^{(t)}(a_i))(p)=(\pi(i))(p)$ for any $i\in[1:s]-\{i_\pi\}$ and $p\in\bigcup_{k=0}^{u} X^k$.

$(\mathscr{D}_u)$ $(\lambda^{(t)}(b_i))(p)=y_1$ for any $i\in[0:r]$ and $p\in\bigcup_{k=0}^{u} X^k$.

$(\mathscr{C}_0)$ and $(\mathscr{D}_0)$ follow directly from (f) and (g). Let $u\in[1:t]$ and assume that $(\mathscr{C}_{u-1})$, $(\mathscr{D}_{u-1})$ hold. Let $p\in X^u$. Then $p=x_jq$ for some $j\in[1:n]$ and $q\in X^{u-1}$. Let $i\in[1:s]-\{i_\pi\}$ and $\delta(a_i, x_j)=a_k$. Then $\pi(k)_l=\pi(i)_{r,j}$ by (h), (c) and (j). We have

$$(\lambda^{(t)}(a_i))(p)=\lambda(\delta(a_i, p))=\lambda(\delta(a_k, q))=(\lambda^{(t)}(a_k))(q)=(\pi(k)_l)(q)=(\pi(i)_{r,j})(q)=$$
$$=(\pi(i))(x_jq)=(\pi(i))(p).$$

Hence we have $(\mathscr{C}_u)$. Let $i\in[0:r]$. Then $\lambda(\delta(b_i, p))=\lambda(\delta(b_{i+1}, q))=$ $=(\lambda^{(t)}(b_{i+1}))(q)=y_1$. Hence we have $(\mathscr{D}_u)$. Consequently, we have $(\mathscr{C}_t)$ and $(\mathscr{D}_t)$ by induction. □

Lemma 16. Let π be an op-mapping of degree (t, s) and let $r\in\mathbf{N}^\circ$. For a Moore automaton $\mathbf{A}(\pi, r)=(A, X, Y, \delta, \lambda)$, we have:

$$|\eta_0(\mathbf{A}(\pi, r))| = 1,$$
$$|\eta_1(\mathbf{A}(\pi, r))| = m,$$
$$|\eta_2(\mathbf{A}(\pi, r))| = m^{1+n},$$
$$\cdots$$
$$|\eta_t(\mathbf{A}(\pi, r))| = m^{1+n+n^2+\ldots+n^{t-1}},$$
$$|\eta_{t+1}(\mathbf{A}(\pi, r))| = s = |A|-r,$$
$$|\eta_{t+2}(\mathbf{A}(\pi, r))| = |A|-(r-1),$$
$$\cdots$$
$$|\eta_{t+r}(\mathbf{A}(\pi,r))| = |A|-1,$$
$$|\eta_{t+r+1}(\mathbf{A}(\pi,r))| = |A|.$$

Proof. $|\eta_0(\mathbf{A}(\pi, r))|=1$ is evident. Let $u\in[1:t]$. By the assertion (a) and by Lemma 15, for any $g\in F_{u-1}$, there exists an $i\in[1:s]$ such that $\lambda^{(u-1)}(a_i)=g$. Hence by Lemmas 6 and 1, we have

$$|\eta_u(\mathbf{A}(\pi, r))| = |F_{u-1}| = m^{1+n+n^2+\ldots+n^{u-1}}.$$

Since π is injective, it follows from Lemmas 15 and 5 that any two elements of $\{a_1, \ldots, a_s\}$ are not congruent modulo $\eta_{t+1}(\mathbf{A}(\pi, r))$. Moreover by Lemmas 15 and 5, any two elements of $\{b_0, b_1, \ldots, b_r\}$ are congruent modulo $\eta_{t+1}(\mathbf{A}(\pi, r))$. Thus we have $|\eta_{t+1}(\mathbf{A}(\pi, r))|=s$.

Next let $u \in [2: r+1]$. By the assertions (c) and (d), we have $(\pi(i_\pi+1))(p)=y_1$ for any $p \in \bigcup_{k=0}^{t-1} X^k$. Since an op-mapping is injective, we have $\pi(i_\pi+1) \neq \pi(i_\pi)$. Hence $(\pi(i_\pi+1))(q) \neq y_1$ for some $q \in X^t$. Notice that $b_{r+1}=a_{i_\pi+1}$. By the first part of Lemma 15, we have $\lambda(\delta(b_{r+1}, p))=(\lambda^{(t)}(b_{r+1}))(p)=\pi(i_\pi+1)(p)=y_1$ for any $p \in \bigcup_{k=0}^{t-1} X^k$, and $\lambda(\delta(b_{r+1}, q))=(\lambda^{(t)}(b_{r+1}))(q)=\pi(i_\pi+1)(q) \neq y_1$ for some $q \in X^t$. Hence for any $i \in [0: r+1]$, $\lambda(\delta(b_i, p'))=y_1$ for any $p' \in \bigcup_{k=0}^{t+r-i} X^k$ and $\lambda(\delta(b_i, q')) \neq y_1$ for some $q' \in X^{t+r+1-i}$. It follows easily from this fact that $\{b_0, \ldots, b_{r+1-u}\}$ is an $\eta_{t+u}(\mathbf{A}(\pi, r))$-class, and any other element of A is congruent only to itself. Hence we have $|\eta_{t+u}(\mathbf{A}(\pi, r))|=|A|-(r+1-u)$. □

Proposition 4. Let π be an op-mapping of degree (t, s) and let $r \in \mathbf{N}^\circ$. Then $\mathbf{A}(\pi, r)$ is an initially connected Moore automaton with $\Omega(\mathbf{A}(\pi, r))=t+r$.

Proof. By Lemmas 16 and 4. □

Remark. By Lemmas 7, 8 and 16 we have the following: For every $i \in \mathbf{N}^\circ$, the number of $\eta_i(\mathbf{A}(\pi, r))$-classes takes the maximal value among all Moore automata $\mathbf{A}=(A, X, Y, \delta', \lambda')$ with $\Omega(\mathbf{A})=r+t$. □

5.

Now we can determine all realizable 4-tuples.

Theorem 2. Let $v, n, m \in \mathbf{N}$ and $w \in \mathbf{N}^\circ \cup \{\infty\}$. The following three assertions are equivalent:

(1) (v, n, m, w) is realizable by Moore automata.

(2) (v, n, m, w) is realizable by initially connected Moore automata.

(3) (3.1) $m+w \leqq v \leqq m^{1+n+n^2+\ldots+n^w}$, or

(3.2) $w=\infty$, $m \leqq v-1$.

Proof. (2)⇒(1). Obvious.

(1)⇒(3). If $w<\infty$, then we have (3.1) by Proposition 1. If $|A|=|Y|$ in a Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$, then it is evident that $\Omega(\mathbf{A})=0$. Hence we have (3.2).

(3.1)⇒(2). If $m=1$ then (3.1) implies that $v=1$ and $w=0$. For any $n \in \mathbf{N}$, there actually exists a Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$ such that $|A|=|Y|=1$ and $|X|=n$. Obviously, $\mathbf{A}$ is initially connected and $\Omega(\mathbf{A})=0$.

Next assume that $m \geqq 2$. Put $\alpha(-1)=m-1$ and $\alpha(k)=m^{1+n+n^2+\cdots+n^k}-k$ for any $k \in \mathbf{N}^\circ$. Our assumption is

(i) $m \leqq v-w \leqq \alpha(w)$.

Since $m=\alpha(0)<\alpha(1)<\alpha(2)<\ldots$, there exists a unique $t \in \mathbf{N}^\circ$ such that

(ii) $\alpha(t-1)+1 \leqq v-w \leqq \alpha(t)$.

Let $X=\{x_1, \ldots, x_n\}$ and $Y=\{y_1, \ldots, y_m\}$. If $t=0$ then (ii) means that $v-w=m$. Hence $(t, v-w+t)=(0, m)$. By Lemma 11, there exists an op-mapping π of degree $(t, v-w+t)$ with respect to X and Y. If $t\geqq 1$ then (ii) means that

$$m^{1+n+n^2+\ldots+n^{t-1}}+2 \leqq v-w+t \leqq m^{1+n+n^2+\ldots+n^t}.$$

Hence by Proposition 3, there exists an op-mapping π of degree $(t, v-w+t)$ with respect to X and Y. By (i) and (ii), it can easily be seen that $t\leqq w$. Consider an initially connected Moore automaton $\mathbf{A}(\pi, w-t)=(A, X, Y, \delta, \lambda)$. We have $|A|=(v-w+t)+(w-t)=v$, $|X|=n$, $|Y|=m$ and, by Proposition 4, $\Omega(\mathbf{A}(\pi, w-t))=t+(w-t)=w$.

(3.2)$\Rightarrow$(2). Define a Moore automaton $\mathbf{A}=(A, X, Y, \delta, \lambda)$ as follows:

(i) $A=\{a_1, \ldots, a_v\}$, $X=\{x_1, \ldots, x_n\}$ and $Y=\{y_1, \ldots, y_m\}$.

(ii) $\lambda(a_i)=y_i (i\in[1: m-1])$ and $\lambda(a_i)=y_m (i\in[m: v])$.

(iii) $\delta(a_i, x_j)=a_{i+1} (i\in[1: v-1])$ and $\delta(a_v, x_j)=a_v$ for any $j\in[1: n]$.

Then it can easily be seen that $\mathbf{A}$ is initially connected and $\omega_{\mathbf{A}}(a_{v-1}, a_v)=\infty$. Hence $\Omega(\mathbf{A})=\infty$, and thus we have (2). □

6.

Let $X=\{x_1, x_2\}$ and $Y=\{1, 2\}$. (Instead of $Y=\{y_1, y_2\}$, we use $Y=\{1, 2\}$ for simplicity). We shall construct op-mappings according to the Constructions (I) and (II) in Section 4. An op-mapping of degree (t, s) is denoted by $\pi_{t,s}$.

For $t=0$, $\pi_{0,2}$ is uniquely determined by $(\pi_{0,2}(1))(e)=1$ and $(\pi_{0,2}(2))(e)=2$. For $t=1$, $\pi_{1,s}$ exist for $2+1\leqq s\leqq 2^{1+2}$. To obtain $\pi_{1,3}$ we use Construction (I). σ is given by $(\sigma(2))(e)=1$ and $(\sigma(3))(e)=2$. $\pi_{1,3}$ is obtained (for example) by the first three rows of Table 1, and $\pi_{1,4}$, $\pi_{1,5}$, $\pi_{1,6}$ are represented by the first 4, 5, 6 rows of Table 1. These op-mappings are obtained by Construction (II.1), i.e., to satisfy the following conditions:

(i) The x_1-component of the i-th row equals the e-component of the $(i+1)$-th row.

(ii) All rows are distinct.

We can not continue this procedure to give $\pi_{1,7}$. Because two rows, i.e., two elements of $F_1(X, Y)$, which are not yet used are (2, 2, 1) and (2, 2, 2), and we can not determine the 7th row so as to satisfy (i) and (ii). This means that we are in case (II.2). As shown in Lemma 14, the x_1-component of the 6th row is equal to the e-component of the first row. We make a cyclic exchange of 6 rows for example in Table 2. Then we can add the 7th and 8th rows to satisfy (i) and (ii). In this way, we have $\pi_{1,7}$ and $\pi_{1,8}$ which are the first 7 and 8 rows of Table 2.

For $t=2$, $\pi_{2,s}$ exist for $2^{1+2}+1\leqq s\leqq 2^{1+2+4}$. To construct $\pi_{2,9}$, first obtain σ from $\pi_{1,8}$. σ is shown in Table 3 which is derived by cyclic exchange of Table 2 so that the top row is (1, 1, 1). The first 9 rows of Table 4 are constructed as follows:

(i) All components of the first row are 1.

(ii) The e-, x_1- and x_2-components from the 2nd to the 9th rows are coincident with those of σ.

(iii) The x_1x_1- and x_1x_2-components of the i-th row are equal to the x_1- and x_2-components of the $(i+1)$-th row ($i\in[2: 8]$).

(iv) The x_2x_1- and x_2x_2-components from the 2nd to the 9th rows are arbitrarily chosen. The x_1x_1- and x_1x_2-components of the 9th row are also arbitrarily chosen.

In this way we have $\pi_{2,9}$ by using Construction (I). To obtain $\pi_{2,s}$ for $s=10, 11, \ldots,$ we add new rows one by one so that the following conditions are satisfied (Construction (II.1)).

(i) The x_1x_1- and x_1x_2-components of the i-th row are equal to the x_1- and x_2-components of the $(i+1)$-th row.

(ii) All rows are distinct.

In the case when we can not continue this procedure (Case (II.2)), we make a cyclic exchange of rows and continue the procedure. In such a way, we can obtain $\pi_{2,s}$ for all $s\in[9: 2^7]$. Table 4 shows $\pi_{2,s}$ for $s\in[9: 16]$.

Table 1

	e	x_1	x_2
1	1	1	1
2	1	2	1
3	2	1	1
4	1	1	2
5	1	2	2
6	2	1	2

Table 2

	e	x_1	x_2
1	2	1	1
2	1	1	2
3	1	2	2
4	2	1	2
5	1	1	1
6	1	2	1
7	2	2	1
8	2	2	2

Table 3

	e	x_1	x_2
2	1	1	1
3	1	2	1
4	2	2	1
5	2	2	2
6	2	1	1
7	1	1	2
8	1	2	2
9	2	1	2

Table 4

	e	x_1	x_2	x_1x_1	x_1x_2	x_2x_1	x_2x_2
1	1	1	1	1	1	1	1
2	1	1	1	2	1	1	1
3	1	2	1	2	1	1	1
4	2	2	1	2	2	2	1
5	2	2	2	1	1	2	2
6	2	1	1	1	2	1	2
7	1	1	2	2	2	1	1
8	1	2	2	1	2	1	2
9	2	1	2	1	1	1	2
10	1	1	1	1	2	1	2
11	1	1	2	2	2	1	2
12	1	2	2	2	2	2	2
13	2	2	2	1	2	1	2
14	2	1	2	2	2	1	2
15	1	2	2	1	1	1	1
16	2	1	1	1	1	1	1

Next we shall see two examples of realization of 4-tuples (v, n, m, w).

Let $(v, n, m, w)=(10, 2, 2, 4)$. Since $2+4\leqq 10\leqq 2^{1+2+2^3+2^4}$, $(10, 2, 2, 4)$ is realizable by initially connected Moore automata. The unique solution of $2^{1+2+\cdots+2^{t-1}}+2\leqq 10-4+t\leqq 2^{1+2+2^2+\cdots+2^t}$ is $t=1$. Hence $\mathrm{A}(\pi_{1,7}, 3)$ realizes $(10, 2, 2, 4)$. In Fig. 1, an example of $\mathrm{A}(\pi_{1,7}, 3)$ is depicted, which is obtained by using Table 2.

Let $(v, n, m, w)=(17, 2, 2, 5)$. Since $2+5 \leqq 17 \leqq 2^{1+2+2^3+2^4+2^5}$, $(17, 2, 2, 5)$ is realizable by initially connected Moore automata. The unique solution of $2^{1+2+\cdots+2^{t-1}}+2 \leqq 17-5+t \leqq 2^{1+2+2^2+\cdots+2^t}$ is $t=2$. Hence $\mathrm{A}(\pi_{2,14}, 3)$ realizes $(17, 2, 2, 5)$. $\mathrm{A}(\pi_{2,14}, 3)$ is illustrated in Fig. 2.

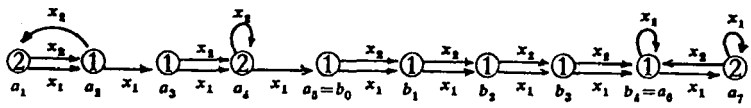

Fig. 1

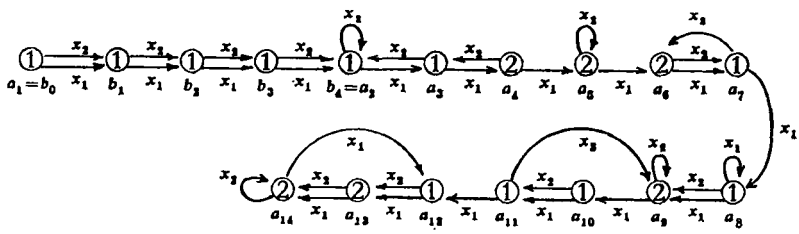

Fig. 2

Acknowledgement

The author would like to thank Professors A. Ádám and M. Ito for their careful readings and comments.

FACULTY OF SCIENCE
KYOTO SANGYO UNIVERSITY
KYOTO 603, JAPAN

References

[1] Ádám, A., On the question of description of the behavior of finite automata, Studia Sci. Math. Hungar. 13 (1978), 105—124.
[2] Ádám, A., On the complexity of codes and pre-codes assigned to finite Moore automata, Acta Cybernet., 5 (1981), 117—133.
[3] Ádám, A., Research problem 29, The connection of state number and the complexity of finite Moore automata, Period. Math. Hungar., 12 (1981), 229—230.
[4] Ádám, A., On certain partitions of finite directed graphs and of finite automata, Acta Cybernet. 6 (1984), 331—346.
[5] Ito, M. and J. Duske, On cofinal and definite automata, Acta Cybernet., 6 (1983), 181—189.

(Received Febr. 1, 1985)