JOURNAL OF COMPUTER AND SYSTEM SCIENCES 17, 65–80 (1978)

A Representation of Strongly Connected Automata and Its Applications

MASAMI ITO

Faculty of Science, Kyoto Sangyo University, Kyoto, 603 Japan

Received September 3, 1976; revised May 5, 1977

A new type of representation of strongly connected automata is introduced. And some new results about automorphism groups of strongly connected automata are obtained by making use of this representation.

INTRODUCTION

In the present paper, we deal with a method to determine the structures of strongly connected automata whose automorphism groups are isomorphic to a given finite group. For this purpose, we propose a new type of representation of strongly connected automata, called regular group-matrix type automata. In the first four sections, we shall deal with correlations between strongly connected automata and regular group-matrix type automata. The last section contains applications of related results to the theory of automorphism groups of automata.

As to input sets of automata, we shall avoid an abstract treatment. That is, we shall restrict them to finite alphabets instead of general semigroups. However, our theory will be easily transferred into the general case.

1. INTRODUCTORY CONCEPTS AND SOME RESULTS

In the present section, we provide some introductory concept about automata and their automorphism groups, and present some fundamental results without proof. For the proofs, see [4].

DEFINITION 1.1. An *automaton* A is a triple, $A = (S, \Sigma, M)$, where S is a nonempty finite set of states, Σ is a nonempty finite set of inputs and M is a next state function, called state transition function, such that $M(s, xy) = M(M(s, x), y)$ and $M(s, \epsilon) = s$ for all $s \in S$ and all $x, y \in \Sigma^*$. Here Σ^* is the free semigroup generated by the elements of Σ, and ϵ is its identity.

DEFINITION 1.2. Let $A = (S, \Sigma, M)$ be an automaton. A permutation ρ on S is called an *automorphism* of the automaton A if $\rho(M(s, x)) = M(\rho(s), x)$ for all $s \in S$ and

0022-0000/78/0171–0065$02.0/00

$x \in \Sigma^*$. Then, the set of all automorphisms of A forms a group, denoted $G(A)$, and we call it the automorphism group of A. Here the product $gh \in G(A)$ of $g, h \in G(A)$ means $gh(s) = g(h(s))$ for all $s \in S$.

DEFINITION 1.3. An automaton $A = (S, \Sigma, M)$ is called *strongly connected*, if for any pair of states $s, t \in S$ there exists an element $x \in \Sigma^*$ such that $M(s, x) = t$.

THEOREM 1.1. *If $A = (S, \Sigma, M)$ is a strongly connected automaton and g, h are elements in $G(A)$ such that $g(s_0) = h(s_0)$ for some $s_0 \in S$, then $g(s) = h(s)$ for all $s \in S$.*

THEOREM 1.2. *If $A = (S, \Sigma, M)$ is a strongly connected automaton, then $|G(A)|$ divides $|S|$, where $|K|$ denotes the cardinality of the set K.*

DEFINITION 1.4. An automaton $A = (S, \Sigma, M)$ is called a *permutation automaton*, if $M(s, \sigma)$ is a permutation on S for all $\sigma \in \Sigma$.

DEFINITION 1.5. Automata $A = (S, \Sigma, M)$ and $B = (T, \Gamma, N)$ are called to be isomorphic to each other, denoted $A \approx B$, if there exist two one-to-one and onto mappings $\rho: S \to T$ and $\xi: \Sigma \to \Gamma$ such that $\rho(M(s, \sigma)) = N(\rho(s), \xi(\sigma))$ for all $s \in S$ and all $\sigma \in \Sigma$.

THEOREM 1.3. *If A and B are automata such that $A \approx B$, then $G(A)$ is isomorphic to $G(B)$, also denoted $G(A) \approx G(B)$.*

DEFINITION 1.6. An automaton $A = (S, \Sigma, M)$ is called *simplified*, if for any pair of inputs $\sigma, \tau \in \Sigma$ $(\sigma \neq \tau)$ there exists an element $s \in S$ such that $M(s, \sigma) \neq M(s, \tau)$.

DEFINITION 1.7. Let $A = (S, \Sigma, M)$ be an automaton and $G(A)$ be its automorphism group. Furthermore, assume that H is a subgroup of $G(A)$. Then, the *factor automaton* A/H is the automaton $A/H = (\bar{S}_H, \Sigma, \bar{M}_H)$, where $\bar{S}_H = \{\bar{s};\ s \in S\}$ $(\bar{s} = \{t;\ t \in S$ and there exists some $h \in H$ such that $t = h(s)\})$ and $\bar{M}_H(\bar{s}, \sigma) = \overline{M(s, \sigma)}$ for all $\bar{s} \in \bar{S}_H$ and all $\sigma \in \Sigma$.

2. GROUP-MATRIX TYPE AUTOMATA

In Section 3, we shall give a representation of strongly connected automata. We prepare, in this section, for this goal.

DEFINITION 2.1. Let G be a finite group. Then G^0 is the set $G \cup \{0\}$ in which we introduce two operations $(\cdot)$ and $(+)$ as follows:

(1) For all $g, h \in G$, we define $g \cdot h$ as the group operation in G.

(2) For all $g \in G$, we define $g \cdot 0 = 0 \cdot g = 0$ and $0 \cdot 0 = 0$.

(3) For all $g \in G$, we define $g + 0 = 0 + g = g$ and $0 + 0 = 0$.

(4) For any $g, h \in G$, we do not define $g + h$.

We shall sometimes use the notations gh and $\sum_{i=1}^{s} g_i$ instead of $g \cdot h$ and $g_1 + g_2 + \cdots + g_s$. Notice that the sum $\sum_{i=1}^{s} g_i$ is defined only if at most one of g_i $(1 \leqslant i \leqslant s)$ is nonzero.

DEFINITION 2.2. Let G be a finite group and n be a positive integer. We consider an $n \times n$ matrix (f_{pq}) $(1 \leqslant p \leqslant n,\ 1 \leqslant q \leqslant n,\ f_{pq} \in G^0)$. If an $n \times n$ matrix (f_{pq}) satisfies the following conditions, then (f_{pq}) is called a *group-matrix of order n on G*:

For each p' $(1 \leqslant p' \leqslant n)$, there exists a unique number q' $(1 \leqslant q' \leqslant n)$ such that $f_{p'q'} \neq 0$.

We denote by $\tilde{G}_n$ the set of all group-matrices of order n on G. Then, $\tilde{G}_n$ forms a semigroup under the following operation:

$$(f_{pq})(g_{pq}) = \left(\sum_{k=1}^{n} f_{pk} g_{kq} \right).$$

DEFINITION 2.3. Let G be a finite group and n be a positive integer. We consider a vector (f_p) $(1 \leqslant p \leqslant n, f_p \in G^0)$. A vector (f_p) is called a *group-vector of order n on G*, if there exists a unique number p' $(1 \leqslant p' \leqslant n)$ such that $f_{p'} \neq 0$. We denote by $\hat{G}_n$ the set of all group-vectors of order n on G. For all $(f_p) \in \hat{G}_n$ and all $(g_{pq}) \in \tilde{G}_n$, we define the following multiplication:

$$(f_p)(g_{pq}) = \left(\sum_{k=1}^{n} f_k g_{kp} \right).$$

Under this operation, we get $(f_p)(g_{pq}) \in \hat{G}_n$.

DEFINITION 2.4. Let G be a finite group and n be a positive integer. An automaton $A = (\hat{G}_n, \Sigma, M_\Psi)$ is called a *group-matrix type automaton of order n on G*, or simply an *(n, G)-automaton*, if the following conditions are satisfied:

(1) $\hat{G}_n$ is the set of states.

(2) Σ is a set of inputs.

(3) M_Ψ is a state transition function and it is defined by $M_\Psi(\hat{g}, \sigma) = \hat{g}\Psi(\sigma)$ $(\hat{g} \in \hat{G}_n, \sigma \in \Sigma)$, where Ψ is a mapping of Σ into $\tilde{G}_n$.

Remark 2.1. The mapping Ψ can be extended to the mapping of Σ^* into $\tilde{G}_n$ as follows:

$\Psi(\epsilon) = (e_{pq})$ $(e_{pq} = 0$ if $p \neq q$, and $e_{pp} = e$, where e is the identity of $G)$, and $\Psi(xy) = \Psi(x)\Psi(y)$ for all $x, y \in \Sigma^*$.

In this case, we can see easily that $M_\Psi(\hat{g}, x) = \hat{g}\Psi(x)$ holds for all $x \in \Sigma^*$.

We can easily prove the following:

PROPOSITION 2.1. *Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be an (n, G)-automaton. Then, A is simplified if and only if Ψ is a one-to-one mapping of Σ into $\hat{G}_n$.*

THEOREM 2.1. *Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be an (n, G)-automaton. Then, G is isomorphic to a subgroup of $G(A)$.*

Proof. For all $g \in G$, we shall define the following mapping ρ_g of $\hat{G}_n$ onto itself: $\rho_g(\hat{h}) = (gh_p)$ $(1 \leqslant p \leqslant n)$ for all $\hat{h} \in \hat{G}_n$, where $\hat{h} = (h_p)$ $(1 \leqslant p \leqslant n,\ h_p \in G^0)$. Then, it is not difficult to prove that ρ_g is an automorphism of A and that the mapping $g \to \rho_g$ is an isomorphism of G onto a subgroup of $G(A)$. Q.E.D.

In particular, the case where G is isomorphic to $G(A)$ is important.

DEFINITION 2.5. An (n, G)-automaton A is called *regular*, if A is strongly connected and $G(A) \approx G$ holds.

Concerning the strong connectedness, we have the following result:

THEOREM 2.2. *An (n, G)-automaton $A = (\hat{G}_n, \Sigma, M_\Psi)$ is strongly connected if and only if the following condition is satisfied:*

For all p', q' $(1 \leqslant p' \leqslant n,\ 1 \leqslant q' \leqslant n)$ and all $g \in G$, there exists some element x in Σ^* such that $\psi_{p'q'}(x) = g$, where we put $\Psi(x) = (\psi_{pq}(x))$.

Proof. First, assume that A is strongly connected. Put $\hat{e}_{p'} = (e_{pp'}) \in \hat{G}_n$, where e is the identity of G (for the notation, see Remark 2.1).

Now, we put $\hat{g}_{q'} = (ge_{pq'}) \in \hat{G}_n$ for all $g \in G$. Since A is strongly connected, there exists some element $x \in \Sigma^*$ such that $M_\Psi(\hat{e}_{p'}, x) = \hat{g}_{q'}$. Thus, we have $\psi_{p'q'}(x) = g$.

Conversely, assume that the condition is satisfied. For any pair of elements $\hat{g}, \hat{h} \in \hat{G}_n$, there exist some elements $g', h' \in G$ and some numbers p', q' $(1 \leqslant p' \leqslant n,\ 1 \leqslant q' \leqslant n)$ such that $\hat{g} = (g'e_{pp'})$ and $\hat{h} = (h'e_{pq'})$.

By the assumption, there exists some element $x \in \Sigma^*$ such that $\psi_{p'q'}(x) = g'^{-1}h'$. In this case, $M_\Psi(\hat{g}, x) = \hat{g}\Psi(x) = \hat{h}$ holds. Therefore, A is strongly connected. Q.E.D.

It seems very difficult to give a necessary and sufficient condition about $\Psi(\Sigma)$ or $\Psi(\Sigma^*)$ in order that a group-matrix type automaton $A = (\hat{G}_n, \Sigma, M_\Psi)$ may be regular, though we have the following results in the cases $n = 1$ and $n = 2$.

THEOREM 2.3. *Let $A = (\hat{G}_1, \Sigma, M_\Psi)$ be a $(1, G)$-automaton. Then if A is strongly connected, A is regular.*

Proof. We have to prove $G(A) \approx G$. For this purpose, it is enough to say that for all $\rho \in G(A)$ there exists some element $g \in G$ such that $\rho = \rho_g$ (for the reason and the notation, see the proof of Theorem 2.1).

Now, assume that $\rho \in G(A)$. Then, we have $\rho(M_\Psi(\hat{h}, x)) = M_\Psi(\rho(\hat{h}), x)$ for all $\hat{h} = (h) \in \hat{G}_1$ $(h \in G)$ and all $x \in \Sigma^*$. This means that $\rho(\hat{h}\Psi(x)) = \rho(\hat{h})\,\Psi(x)$ holds for all $\hat{h} = (h) \in \hat{G}_1$ $(h \in G)$ and all $x \in \Sigma^*$. Note that for $\hat{e} = (e) \in \hat{G}_1$ there exists some element $g \in G$ such that $\rho(\hat{e}) = (g) \in \hat{G}_1$, where e is the identity of G. By the strong connectedness of A, for all $h \in G$ there exists some element $x \in \Sigma^*$ such that $\Psi(x) = (h)$. Thus, for all $\hat{h} = (h) \in \hat{G}_1$, we have the following:

$$\rho(\hat{h}) = \rho(\hat{e}\Psi(x)) = \rho(\hat{e})\,\Psi(x) = (g)(h) = \rho_g(\hat{h}).$$

Therefore, we get $\rho = \rho_g$. Q.E.D.

THEOREM 2.4. *Let $A = (\hat{G}_2, \Sigma, M_\Psi)$ be a strongly connected $(2, G)$-automaton. Then, A is not regular if and only if there exist some automorphism φ of G, some element k in G, and two subsets Λ, Γ ($\Gamma \neq \varnothing$) of G such that $\varphi(k) = k$, $\varphi^2(g) = kgk^{-1}$ for all $g \in G$, and $\Psi(\Sigma) = \{\left(\begin{smallmatrix} g & 0 \\ 0 & \varphi(g)\end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & h \\ \varphi(h)k & 0\end{smallmatrix}\right); g \in \Lambda, h \in \Gamma\}$.*

Proof. Assume that A is not regular. Then, there exists some element $\rho \in G(A)$ such that $\rho \neq \rho_g$ for all $g \in G$. Furthermore, there exist two transformations ρ_1, ρ_2 on G such that $\rho((g, 0)) = (0, \rho_2(g))$ and $\rho((0, h)) = (\rho_1(h), 0)$ for all $g, h \in G$. Because, if it is not true, there exist some elements $g', h' \in G$ such that either $\rho((g', 0)) = (h', 0)$ or $\rho((0, g')) = (0, h')$ holds.

Let us consider the former case. In this case, since $\rho(M_\Psi((g', 0), x) = M_\Psi(\rho((g', 0)), x)$ holds, we have $\rho((g', 0)\,\Psi(x)) = \rho((g', 0))\,\Psi(x) = (h', 0)\,\Psi(x)$ for all $x \in \Sigma^*$. By the strong connectedness of A, we can find an element $x' \in \Sigma^*$ such that

$$\Psi(x') = \begin{pmatrix} g'^{-1}g & 0 \\ u & v\end{pmatrix} \qquad (u, v \in G^0,\ u + v \in G) \text{ for all } g \in G.$$

Substituting this value into the equality $\rho((g', 0)\,\Psi(x')) = (h', 0)\,\Psi(x')$, we get $\rho((g, 0)) = (h'g'^{-1}g, 0)$ for all $g \in G$.

In the same manner, we can find an element $x'' \in \Sigma^*$ such that

$$\Psi(x'') = \begin{pmatrix} 0 & g'^{-1}h \\ u' & v'\end{pmatrix} \qquad (u', v' \in G^0,\ u' + v' \in G) \text{ for all } h \in G.$$

By the equality $\rho((g', 0)\,\Psi(x'')) = (h', 0)\,\Psi(x'')$, we have $\rho((0, h)) = (0, h'g'^{-1}h)$ for all $h \in G$. Thus, ρ must be equal to $\rho_{h'g'^{-1}}$. This is a contradiction. Hence, there exist two transformations ρ_1, ρ_2 on G.

Next, let us consider an element in $\Psi(\Sigma^*)$ of the form $\left(\begin{smallmatrix} g & 0 \\ u & v\end{smallmatrix}\right)$ $(u, v \in G^0, g, u + v \in G)$. By the fact that $(e, 0)\left(\begin{smallmatrix} g & 0 \\ u & v\end{smallmatrix}\right) = (g, 0)$ and that $\rho((e, 0)\left(\begin{smallmatrix} g & 0 \\ u & v\end{smallmatrix}\right)) = \rho((e, 0))\left(\begin{smallmatrix} g & 0 \\ u & v\end{smallmatrix}\right)$, we have $(0, \rho_2(g)) = (0, \rho_2(e))\left(\begin{smallmatrix} g & 0 \\ u & v\end{smallmatrix}\right) = (\rho_2(e)u, \rho_2(e)v)$. Therefore, $u = 0$ and $v = \rho_2(e)^{-1}\rho_2(g)$ hold. This means that, if $\left(\begin{smallmatrix} g & 0 \\ u & v\end{smallmatrix}\right) \in \Psi(\Sigma^*)$ holds, then we have

$$\begin{pmatrix} g & 0 \\ u & v\end{pmatrix} = \begin{pmatrix} g & 0 \\ 0 & \rho_2(e)^{-1}\rho_2(g)\end{pmatrix}.$$

Further, let us consider an element in $\Psi(\Sigma^*)$ of the form $\left(\begin{smallmatrix} 0 & g \\ u & v\end{smallmatrix}\right)$$(u, v \in G^0, g, u + v \in G)$. By the fact that $(e, 0)\left(\begin{smallmatrix} 0 & g \\ u & v\end{smallmatrix}\right) = (0, g)$ and that $\rho((e, 0)\left(\begin{smallmatrix} 0 & g \\ u & v\end{smallmatrix}\right)) = \rho((e, 0))\left(\begin{smallmatrix} 0 & g \\ u & v\end{smallmatrix}\right)$, we have

$(\rho_1(g), 0) = (0, \rho_2(e))\begin{pmatrix} 0 & g \\ u & v \end{pmatrix} = (\rho_2(e)u, \rho_2(e)v)$. Therefore, $u = \rho_2(e)^{-1}\rho_1(g)$ and $v = 0$ hold. This means that, if $\begin{pmatrix} 0 & g \\ u & v \end{pmatrix} \in \Psi(\Sigma^*)$ holds, then we have

$$\begin{pmatrix} 0 & g \\ u & v \end{pmatrix} = \begin{pmatrix} 0 & g \\ \rho_2(e)^{-1}\rho_1(g) & 0 \end{pmatrix}.$$

From these facts and the strong connectedness of A, we have the following:

There exist two permutations φ, ξ on G such that for all $g, h \in G$ we have $\begin{pmatrix} g & 0 \\ 0 & \varphi(g) \end{pmatrix}$, $\begin{pmatrix} 0 & h \\ \xi(h) & 0 \end{pmatrix} \in \Psi(\Sigma^*)$ and that conversely all elements in $\Psi(\Sigma^*)$ can be represented in the above form.

By the fact that $\Psi(\Sigma^*)$ is a semigroup, we have the following four equalities.

By

$$\begin{pmatrix} g & 0 \\ 0 & \varphi(g) \end{pmatrix}\begin{pmatrix} h & 0 \\ 0 & \varphi(h) \end{pmatrix} \quad \begin{pmatrix} gh & 0 \\ 0 & \varphi(g)\,\varphi(h) \end{pmatrix},$$

(A) $\quad \varphi(gh) = \varphi(g)\,\varphi(h)$ for all $g, h \in G$.

By

$$\begin{pmatrix} g & 0 \\ 0 & \varphi(g) \end{pmatrix}\begin{pmatrix} 0 & h \\ \xi(h) & 0 \end{pmatrix} = \begin{pmatrix} 0 & gh \\ \varphi(g)\,\xi(h) & 0 \end{pmatrix},$$

(B) $\quad \xi(gh) = \varphi(g)\,\xi(h)$ for all $g, h \in G$.

By

$$\begin{pmatrix} 0 & g \\ \xi(g) & 0 \end{pmatrix}\begin{pmatrix} h & 0 \\ 0 & \varphi(h) \end{pmatrix} = \begin{pmatrix} 0 & g\varphi(h) \\ \xi(g)h & 0 \end{pmatrix},$$

(C) $\quad \xi(g)h = \xi(g\varphi(h))$ for all $g, h \in G$.

By

$$\begin{pmatrix} 0 & g \\ \xi(g) & 0 \end{pmatrix}\begin{pmatrix} 0 & h \\ \xi(h) & 0 \end{pmatrix} = \begin{pmatrix} g\xi(h) & 0 \\ 0 & \xi(g)h \end{pmatrix},$$

(D) $\quad \xi(g)h = \varphi(g\xi(h))$ for all $g, h \in G$.

By these equalities, we can see easily that there exist φ, k, Λ, and Γ which satisfy the conditions mentioned in the theorem. For example, φ is an automorphism of G by (A), and $k = \xi(e)$.

Conversely, assume that there exist φ, k, Λ, and Γ which satisfy the conditions in the theorem. Put $\rho((g, 0)) = (0, \varphi(g))$ and $\rho((0, h)) = (\varphi(h)k, 0)$ for all $g, h \in G$. Then, it is not difficult to prove that $\rho \in G(A)$. But, since $\rho \neq \rho_g$ for all $g \in G$, A is not regular.

Q.E.D.

The following corollary is immediate.

COROLLARY 2.1. *Let $A = (\hat{G}_2, \Sigma, M_\Psi)$ be a strongly connected $(2, G)$-automaton. Then if A is not a permutation automaton, A is regular.*

In the case $n > 2$, we have the following result.

THEOREM 2.5. *Let* $A = (\hat{G}_n, \Sigma, M_\Psi)$ *be a strongly connected* (n, G)-*automaton. Furthermore, assume that there exists some number* i' $(1 \leqslant i' \leqslant n)$ *which satisfies the following condition*:

For all i $(1 \leqslant i \leqslant n,\ i \neq i')$, *there exist some elements* $x, y \in \Sigma^*$ *and number* q' $(1 \leqslant q' \leqslant n)$ *such that* $\psi_{i'q}(x) = \psi_{i'q}(y)$ *for all* q $(1 \leqslant q \leqslant n)$ *and that* $\psi_{iq'}(x) \neq \psi_{iq'}(y)$, *where* $\Psi(x) = (\psi_{pq}(x))$ *and* $\Psi(y) = (\psi_{pq}(y))$.

Then, A *is regular*.

Proof. It is enough to prove that for all $\rho \in G(A)$ there exists some element $g \in G$ such that $\rho = \rho_g$. Therefore, we assume that $\rho \in G(A)$. Hence, for all $\hat{h} \in \hat{G}_n$ and all $x \in \Sigma^*$, $\rho(\hat{h})\,\Psi(x) = \rho(\hat{h}\Psi(x))$ holds. Now, put $\hat{h} = (e_{pi'})$. Then, there exist some element $k \in G$ and number i $(1 \leqslant i \leqslant n)$ such that $\rho(\hat{h}) = (ke_{pi})$.

In the case $i = i'$, we can prove that there exists some element $g \in G$ such that $\rho = \rho_g$, in a manner similar to that of the first part of the proof of Theorem 2.4.

Now, assume that $i \neq i'$. Then, by a condition in the theorem, there exist some elements $x, y \in \Sigma^*$ and number q' $(1 \leqslant q' \leqslant n)$ such that $\psi_{i'q}(x) = \psi_{i'q}(y)$ for all q $(1 \leqslant q \leqslant n)$ and $\psi_{iq'}(x) \neq \psi_{iq'}(y)$.

By the above relationship and by the equalities $\rho(\hat{h})\,\Psi(x) = \rho(\hat{h}\Psi(x))$, $\rho(\hat{h})\,\Psi(y) = \rho(\hat{h}\Psi(y))$, $\hat{h} = (e_{pi'})$ and $\rho(\hat{h}) = (ke_{pi})$ $(i \neq i')$, the following contradiction follows: $\rho(\hat{h}\Psi(x)) \neq \rho(\hat{h}\Psi(y))$, although $\hat{h}\Psi(x) = \hat{h}\Psi(y)$. Therefore, $i = i'$ must hold and thus A is regular. Q.E.D.

3. REPRESENTATION OF STRONGLY CONNECTED AUTOMATA

In this section, we give a representation of strongly connected automata by group-matrix type automata. In preparation, the following lemma is given:

LEMMA 3.1. *Let* G *and* G' *be two isomorphic groups. Furthermore, assume that* $A = (\hat{G}_n, \Sigma, M_\Psi)$ *is an* (n, G)-*automaton. Then, there exists some* (n, G')-*automaton* $A' = (\hat{G}'_n, \Sigma', M_{\Psi'})$ *such that* $A \approx A'$. *If, in addition,* A *is regular, then* A' *is also regular*.

Proof. Put $\Sigma' = \{\sigma'; \sigma \in \Sigma\}$. Let Φ be an isomorphism of G onto G'. We define $\Psi'(\sigma') = (\tilde{\Phi}(\psi_{pq}(\sigma)))$, where $\tilde{\Phi}$ is the extension of Φ on G^0 with $\tilde{\Phi}(0) = 0$ and $\Psi(\sigma) = (\psi_{pq}(\sigma))$. With the above Σ' and Ψ', we define $A' = (\hat{G}'_n, \Sigma', M_{\Psi'})$.

First, we shall prove that $A \approx A'$. For this purpose, we put $\xi(\sigma) = \sigma'$ for all $\sigma \in \Sigma$ and $\rho(\hat{g}) = (\tilde{\Phi}(g_p))$ for all $\hat{g} = (g_p) \in \hat{G}_n$. Then, ξ and ρ are one-to-one mappings, of Σ onto Σ' and of $\hat{G}_n$ onto $\hat{G}'_n$, respectively. By the definition of Ψ' and the fact that Φ is an isomorphism of G onto G', we can prove easily that $\rho(M_\Psi(\hat{g}, \sigma)) = M_{\Psi'}(\rho(g), \xi(\sigma))$. This means that $A \approx A'$.

Next, assume that A is regular. Then, $G(A) \approx G$ holds. By Theorem 1.3, we have $G(A) \approx G(A')$. On the other hand, $G \approx G'$ holds by the assumption. Therefore, we have $G(A') \approx G'$. This means that A' is regular. Q.E.D.

THEOREM 3.1. *Let $A = (S, \Sigma, M)$ be a strongly connected automaton such that $|S| = n|G(A)|$, where n is a positive integer (the existence of such a number n is warranted by Theorem 1.2). Furthermore, assume that G is a finite group such that $G \approx G(A)$. Then, there exists a regular (n, G)-automaton isomorphic to A.*

Proof. By Lemma 3.1, it is enough to say that A is isomorphic to some regular $(n, G(A))$-automaton. For a preparation for proving this, we define the following relation on S:

For $s, t \in S$, $s \leftrightarrow t$ means that there exists some element $g \in G(A)$ such that $t = g(s)$. Then, it is easy to see that $\leftrightarrow$ defines an equivalence relation on S and it induces n equivalence classes.

Let S_i $(1 \leqslant i \leqslant n)$ be an equivalence class by the relation $\leftrightarrow$ on S. We choose $s_i \in S_i$ $(1 \leqslant i \leqslant n)$ and put $T = \{s_1, s_2, \ldots, s_n\}$. Then, for all $\sigma \in \Sigma$ and all $s_p \in T$ $(1 \leqslant p \leqslant n)$, there exists a unique pair $s_{p'} \in T$, $h \in G(A)$ such that $M(s_p, \sigma) = h(s_{p'})$. Note, here, that the uniqueness of $h \in G(A)$ is guaranteed by Theorem 1.1. Making use of these p, p' and h, we define the following mapping Ψ of Σ into $\widetilde{G(A)}_n$:

$\Psi(\sigma) = (\psi_{pq}(\sigma))$ for $\sigma \in \Sigma$, where $\psi_{pp'}(\sigma) = h$ and $\psi_{pq}(\sigma) = 0$ $(q \neq p')$.

Thus, we can obtain an $(n, G(A))$-automaton $A' = (\widehat{G(A)}_n, \Sigma, M_\Psi)$.

Now, we shall prove that $A \approx A'$. For this, we first define ξ as the identity mapping on Σ, i.e., $\xi(\sigma) = \sigma$ for all $\sigma \in \Sigma$. Next, we define the mapping ρ as follows:

$\rho(s) = (he_{pi})$ for $s \in S$, where e is the identity of $G(A)$, i and h are, respectively, a number and an element in $G(A)$ uniquely determined such that $s_i \in T$ and $s = h(s_i)$. Then, it is easy to see that $\rho(s) \in \widehat{\hat{G}(A)}_n$ and ρ is a one-to-one mapping of S onto $\widehat{\hat{G}(A)}_n$. Now, we shall prove that for all $s \in S$ and all $\sigma \in \Sigma$ we have $\rho(M(s, \sigma)) = M_\Psi(\rho(s), \xi(\sigma))$ Put $s = h(s_i)$ $(h \in G(A))$. Then, we have $\rho(s) = (he_{pi})$. On the other hand, we have the following equality:

$$M_\Psi(\rho(s), \xi(\sigma)) = M_\Psi(\rho(s), \sigma) = \rho(s)\,\Psi(\sigma) = (he_{pi})(\psi_{pq}(\sigma))$$
$$= \left(\sum_{k=1}^{n} he_{ki}\psi_{kp}(\sigma)\right) = (h\psi_{ip}(\sigma)).$$

Assume that $\psi_{ip'}(\sigma) \in G(A)$ and $\psi_{ip}(\sigma) = 0$ $(p \neq p')$. Then, by the definition of $\Psi(\sigma)$, we have $M(s_i, \sigma) = \psi_{ip'}(\sigma)(s_{p'})$. Therefore, we have $M(s, \sigma) = M(h(s_i), \sigma) = h(M(s_i, \sigma)) = h(\psi_{ip'}(\sigma)(s_{p'})) = (h\psi_{ip'}(\sigma))(s_{p'})$. Consequently, if we put $\rho(M(s, \sigma)) = (\eta_p)$, then $\eta_{p'} = h\psi_{ip'}(\sigma)$ and $\eta_p = 0$ $(p \neq p')$ hold by the definition of ρ. Thus, we have $M_\Psi(\rho(s), \xi(\sigma)) = \rho(M(s, \sigma))$. Therefore, $A \approx A'$ holds and also A' is strongly connected. Furthermore, by Theorem 1.3, $G(A) \approx G(A')$ holds. This means that A' is regular. Q.E.D.

Remark 3.1. Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be a regular (n, G)-automaton. Then, $|\hat{G}_n| = n|G|$ and $G(A) \approx G$ hold. Consequently, we have the following result:

To determine all distinct strongly connected automata whose automorphism groups are isomorphic to a given finite group G, is equivalent to determine all distinct regular group-matrix type automata of each order of positive integer on G.

Note that here we do not consider two isomorphic automata as distinct ones. Thus, the following problem will be induced: What conditions are required in order that two group-matrix type automata may be isomorphic to each other? This problem will be treated in the following section.

4. Equivalence of Regular Systems

In this section, we shall deal with the problem as noted at the end of the previous section.

Definition 4.1. Let G be a finite group, n be a positive integer and E be a subset of $\tilde{G}_n$. Then, E is called *a regular system in* $\tilde{G}_n$ if there exists some regular (n, G)-automaton $A = (\hat{G}_n, \Sigma, M_\Psi)$ such that $E = \Psi(\Sigma)$.

Definition 4.2. Let E and F be two regular systems in $\tilde{G}_n$. Then, we say that E and F are *equivalent*, denoted $E \sim F$, if there exist some permutation Θ on $\hat{G}_n$ and isomorphism Φ of E^* onto F^* such that the following two conditions are satisfied:

(a) $F = \Phi(E)$.

(b) $\Theta(\hat{g}X) = \Theta(\hat{g})\,\Phi(X)$ for all $\hat{g} \in \hat{G}_n$ and all $X \in E$.

Here, $K^*(K \subseteq \tilde{G}_n)$ denotes the semigroup generated by the elements of $K \cup \{(e_{pq})\}$ (e is the identity of G). Note that, in this case, $\sim$ induces an equivalence relation on the set of all regular systems in $\tilde{G}_n$.

Now, let us consider the problem about isomorphism relation of automata. As easily seen, to discuss this sort of problem, it is sufficient to deal only with the case of simplified automata; thus we have:

Theorem 4.1. *Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ and $A' = (\hat{G}_m, \Sigma', M_{\Psi'})$ be simplified regular (n, G)-, and (m, G)-automaton, respectively. Then, A and A' are isomorphic if and only if two regular systems $\Psi(\Sigma)$ and $\Psi'(\Sigma')$ are equivalent.*

Proof. Assume that $A \approx A'$. Then, $n = m$ holds by $|\hat{G}_n| = |\hat{G}_m|$. Therefore, $\Psi(\Sigma)$ and $\Psi'(\Sigma')$ are regular systems in the same $\tilde{G}_n$. Furthermore, since $A \approx A'$, there exist some permutation ρ on $\hat{G}_n$ and a one-to-one mapping ξ of Σ onto Σ' such that $\rho(M_\Psi(\hat{g}, \sigma)) = M_{\Psi'}(\rho(\hat{g}), \xi(\sigma))$ for all $\hat{g} \in \hat{G}_n$ and all $\sigma \in \Sigma$. By this fact, we can see easily that $\rho(\hat{g}\Psi(\sigma_1)\,\Psi(\sigma_2) \cdots \Psi(\sigma_l)) = \rho(\hat{g})\,\Psi'(\xi(\sigma_1))\,\Psi'(\xi(\sigma_2)) \cdots \Psi'(\xi(\sigma_l))$ holds for all $\sigma_i \in \Sigma$ $(1 \leqslant i \leqslant l,\ l \geqslant 1)$.

Now, let us consider the following mapping:

(1) $\Phi(\Psi(\sigma)) = \Psi'(\xi(\sigma))$ for all $\sigma \in \Sigma$.

(2) $\Phi(X) = \Phi(\Psi(\sigma_1)\,\Psi(\sigma_2) \cdots \Psi(\sigma_l)) = \Psi'(\xi(\sigma_1))\,\Psi'(\xi(\sigma_2)) \cdots \Psi'(\xi(\sigma_l))$ for all $X = \Psi(\sigma_1)\,\Psi(\sigma_2) \cdots \Psi(\sigma_l)$ $(\sigma_i \in \Sigma,\ 1 \leqslant i \leqslant l,\ l \geqslant 1)$.

(3) $\Phi((e_{pq})) = (e_{pq})$.

First, we shall show that the above Φ can be well defined as a mapping. That is, we must say that if $\Psi(\sigma_1)\Psi(\sigma_2)\cdots\Psi(\sigma_l) = \Psi(\tau_1)\Psi(\tau_2)\cdots\Psi(\tau_r)$ $(\sigma_i, \tau_j \in \Sigma,\ 1 \leqslant i \leqslant l,\ 1 \leqslant j \leqslant r,\ l, r \geqslant 1)$ holds, then we have $\Psi'(\xi(\sigma_1))\Psi'(\xi(\sigma_2))\cdots\Psi'(\xi(\sigma_l)) = \Psi'(\xi(\tau_1))\Psi'(\xi(\tau_2))\cdots\Psi'(\xi(\tau_r))$, and that if $\Psi(\sigma_1)\Psi(\sigma_2)\cdots\Psi(\sigma_l) = (e_{pq})$ $(\sigma_i \in \Sigma, 1 \leqslant i \leqslant l, l \geqslant 1)$ holds, then we have $\Psi'(\xi(\sigma_1))\Psi'(\xi(\sigma_2))\cdots\Psi'(\xi(\sigma_l)) = (e_{pq})$.

For this, we assume that $\Psi(\sigma_1)\Psi(\sigma_2)\cdots\Psi(\sigma_l) = \Psi(\tau_1)\Psi(\tau_2)\cdots\Psi(\tau_r)$ $(\sigma_i, \tau_j \in \Sigma,\ 1 \leqslant i \leqslant l,\ 1 \leqslant j \leqslant r,\ l, r \geqslant 1)$ holds. Then, we have $\hat{g}\Psi(\sigma_1)\Psi(\sigma_2)\cdots\Psi(\sigma_l) = \hat{g}\Psi(\tau_1)\Psi(\tau_2)\cdots\Psi(\tau_r)$ for all $\hat{g} \in \hat{G}_n$. By the application of the mapping ρ to the above equality, we have $\rho(\hat{g})\Psi'(\xi(\sigma_1))\Psi'(\xi(\sigma_2))\cdots\Psi'(\xi(\sigma_l)) = \rho(\hat{g})\Psi'(\xi(\tau_1))\Psi'(\xi(\tau_2))\cdots\Psi'(\xi(\tau_r))$ for all $\hat{g} \in \hat{G}_n$. Since ρ is a one-to-one mapping of $\hat{G}_n$ onto $\hat{G}_m$ $(=\hat{G}_n)$ and we can choose an arbitrary element $\hat{g} \in \hat{G}_n$, $\Psi'(\xi(\sigma_1))\Psi'(\xi(\sigma_2))\cdots\Psi'(\xi(\sigma_l)) = \Psi'(\xi(\tau_1))\Psi'(\xi(\tau_2))\cdots\Psi'(\xi(\tau_r))$ must hold.

Thus, we obtain the first part. As to second part, we can prove it in a similar way. Consequently, Φ is well defined.

Next, we can prove easily that Φ is a one-to-one mapping of $\Psi(\Sigma)^*$ $(=\Psi(\Sigma^*))$ onto $\Psi'(\Sigma')^*$ $(=\Psi'(\Sigma'^*))$. Furthermore, it is easily seen that Φ is a homomorphism. Thus, Φ is an isomorphism of $\Psi(\Sigma)^*$ onto $\Psi'(\Sigma')^*$ such that $\Psi'(\Sigma') = \Phi(\Psi(\Sigma))$. Therefore, we have condition (a) in Definition 4.2.

Now, put $\Theta = \rho$. Furthermore, note that $\Phi(\Psi(\sigma)) = \Psi'(\xi(\sigma))$ holds for all $\sigma \in \Sigma$. Then, we have $\Theta(\hat{g}\Psi(\sigma)) = \rho(\hat{g}\Psi(\sigma)) = \rho(M_\Psi(\hat{g}, \sigma))$. On the other hand, $\Theta(\hat{g})\,\Phi(\Psi(\sigma)) = \rho(\hat{g})\,\Psi'(\xi(\sigma)) = M_{\Psi'}(\rho(\hat{g}), \xi(\sigma))$ holds. Since $A \approx A'$, we have $\Theta(\hat{g}\Psi(\sigma)) = \Theta(\hat{g})\,\Phi(\Psi(\sigma))$ for all $\hat{g} \in \hat{G}_n$. This means that we get condition (b). Thus, $\Psi(\Sigma)$ and $\Psi'(\Sigma')$ are equivalent.

Conversely, assume that $\Psi(\Sigma)$ and $\Psi'(\Sigma')$ are equivalent. Then, obviously we have $n = m$. Remember that Ψ and Ψ' are one-to-one by Proposition 2.1. Furthermore, let Φ be an isomorphism of $\Psi(\Sigma)^*$ onto $\Psi'(\Sigma')^*$ which satisfies condition (a).

Now, let us consider the mapping ξ which is defined as follows:

$$\Psi'(\xi(\sigma)) = \Phi(\Psi(\sigma)) \qquad \text{for all } \sigma \in \Sigma.$$

In this case, we can see that $\xi(\sigma)$ is determined uniquely for each $\sigma \in \Sigma$, from the fact that Φ satisfies condition (a) and that Ψ, Ψ' are one-to-one mappings. We can also see that ξ is a one-to-one mapping of Σ onto Σ'. Next, we put $\rho = \Theta$. Obviously, ρ is a one-to-one mapping of $\hat{G}_n$ onto $\hat{G}_m$ $(=\hat{G}_n)$. Then, we have the following result:

For all $\hat{g} \in \hat{G}_n$ and all $\sigma \in \Sigma$, $\rho(M_\Psi(\hat{g}, \sigma)) = \rho(\hat{g}\Psi(\sigma)) = \Theta(\hat{g}\Psi(\sigma)) = \Theta(\hat{g})\,\Phi(\Psi(\sigma)) = \rho(g)\,\Psi'(\xi(\sigma)) = M_{\Psi'}(\rho(g), \xi(\sigma))$ holds. Therefore, we have $A \approx A'$. Q.E.D.

The condition for two regular systems to be equivalent is not so concrete. However, we can give a criterion for the equivalence of regular systems in a more concrete form.

First, we give the following lemmas:

LEMMA 4.1. *Let $A = (S, \Sigma, M)$ and $B = (T, \Gamma, N)$ be two isomorphic automata. Furthermore, assume that ρ and ξ are one-to-one mappings of S onto T, and of Σ onto Γ, respectively, such that $\rho(M(s, \sigma)) = N(\rho(s), \xi(\sigma))$ for all $s \in S$ and all $\sigma \in \Sigma$. Then if $\eta \in G(A)$, we have $\rho\eta\rho^{-1} \in G(B)$.*

Proof. Put $\delta = \rho\eta\rho^{-1}$. Then for all $\gamma \in \Gamma$ and all $t \in T$, we can find some $\sigma \in \Sigma$ and $s \in S$ such that $\gamma = \xi(\sigma)$ and $t = \rho(s)$. Consequently, we have $\delta(N(t, \gamma)) = \delta(N(\rho(s), \xi(\sigma)) = \delta(\rho(M(s, \sigma))) = \rho\eta\rho^{-1}(\rho(M(s, \sigma))) = \rho\eta(M(s, \sigma)) = \rho(M(\eta(s), \sigma)) = N(\rho\eta(s), \xi(\sigma)) = N(\rho\eta\rho^{-1}(\rho(s)), \xi(\sigma)) = N(\delta(t), \gamma)$. Therefore, we have $\delta = \rho\eta\rho^{-1} \in G(B)$. Q.E.D.

LEMMA 4.2. *Let E and F be two equivalent regular systems in $\tilde{G}_n$, i.e., $E \sim F$. Furthermore, assume that Θ and Φ are a permutation on $\hat{G}_n$ and an isomorphism of E^* onto F^*, respectively, which satisfy conditions* (a) *and* (b) *in Definition* 4.2. *Then, there exist a permutation τ on $\{1, 2, 3,..., n\}$ and n permutations θ_i $(1 \leqslant i \leqslant n)$ on G such that for all $\hat{g} = (g_1, g_2, ..., g_n) \in \hat{G}_n$ we have $\Theta(\hat{g}) = (\tilde{\theta}_1(g_{\tau(1)}), \tilde{\theta}_2(g_{\tau(2)}), ..., \tilde{\theta}_n(g_{\tau(n)}))$, where each $\tilde{\theta}_i$ $(1 \leqslant i \leqslant n)$ is the extension of θ_i on G^0 with $\tilde{\theta}_i(0) = 0$.*

Proof. Assume that the above is not true. Then, it is easily seen that there exist some elements $g, g', h, h' \in G$ $(g \neq h)$ and numbers i, j, k $(1 \leqslant i, j, k \leqslant n, j \neq k)$ such that $\Theta((ge_{pi})) = (g'e_{pj})$ and $\Theta((he_{pi})) = (h'e_{pk})$. On the other hand, by Definition 4.1 and by the proof of Theorem 4.1, there exist two regular (n, G)-automata $A = (\hat{G}_n, \Sigma, M_\Psi)$ and $A' = (\hat{G}_n, \Sigma, M_{\Psi'})$, and a permutation ξ on Σ such that $\Psi(\Sigma) = E$, $\Psi'(\Sigma) = F$ and $\Theta(M_\Psi(\hat{g}, \sigma)) = M_{\Psi'}(\Theta(\hat{g}), \xi(\sigma))$ for all $\hat{g} \in \hat{G}_n$ and all $\sigma \in \Sigma$. Then, by Lemma 4.1, for all $\eta \in G(A)$ we have $\Theta\eta\Theta^{-1} \in G(A')$. Now, put $\eta = \rho_{hg^{-1}} \in G(A)$. Here, let us compute the value $\Theta\eta\Theta^{-1}((g'e_{pj}))$. We have $\Theta\eta\Theta^{-1}((g'e_{pj})) = \Theta\eta((ge_{pi})) = \Theta\rho_{hg^{-1}}((ge_{pi})) = \Theta((he_{pi})) = (h'e_{pk})$. Then, it is easily seen that $\Theta\eta\Theta^{-1} \in G(A')$ is not represented by the form $\Theta\eta\Theta^{-1} = \rho_g$ for any $g \in G$. However, this is inconsistent with the fact that A' is regular. Thus, the assertion of the lemma must be true. Q.E.D.

Making use of the above lemma, we can obtain the following result:

THEOREM 4.2. *Let E and F be regular systems in $\tilde{G}_n$. Then, E and F are equivalent if and only if there exist $n - 1$ elements k_i $(2 \leqslant i \leqslant n)$ in G, an automorphism φ of G and a permutation τ on $\{1, 2, 3,..., n\}$ such that $F = \{(k_p^{-1}\tilde{\varphi}(x_{\tau(p)\tau(q)})k_q); (x_{pq}) \in E\}$, where $\tilde{\varphi}$ is the extension of φ on G^0 with $\tilde{\varphi}(0) = 0$ and $k_1 = e$.*

Proof. Proof of the "only if" part. Let Θ and Φ be a permutation on $\hat{G}_n$ and an isomorphism of E^* onto F^*, respectively, which satisfy conditions (a) and (b) in Definition 4.2. Then there exist a permutation τ on $\{1, 2, 3,..., n\}$ and n permutations θ_i $(1 \leqslant i \leqslant n)$ on G satisfying the conditions of Lemma 4.2.

Now, put $X = (x_{pq}) \in E^*$ and $\Phi(X) = (y_{pq}) \in F^*$. Note that $\hat{g}X = (g_1, g_2, ..., g_n)(x_{pq}) = (\sum_{k=1}^n g_kx_{k1}, \sum_{k=1}^n g_kx_{k2}, ..., \sum_{k=1}^n g_kx_{kn})$ holds for all $\hat{g} = (g_1, g_2, ..., g_n) \in \hat{G}_n$. Applying the mapping Θ to the above equality, we have $\Theta((g_1, g_2, ..., g_n))\ \Phi((x_{pq})) = \Theta((\sum_{k=1}^n g_kx_{k1}, \sum_{k=1}^n g_kx_{k2}, ..., \sum_{k=1}^n g_kx_{kn}))$. Thus, we obtain $(\theta_1(g_{\tau(1)}), \theta_2(g_{\tau(2)}), ..., \theta_n(g_{\tau(n)}))(y_{pq}) = (\tilde{\theta}_1(\sum_{k=1}^n g_kx_{k\tau(1)}), \tilde{\theta}_2(\sum_{k=1}^n g_kx_{k\tau(2)}), ..., \tilde{\theta}_n(\sum_{k=1}^n g_kx_{k\tau(n)}))$. This equality implies $\tilde{\theta}_j(\sum_{k=1}^n g_kx_{k\tau(j)}) = \sum_{k=1}^n \tilde{\theta}_k(g_{\tau(k)})y_{kj}$ for each j $(1 \leqslant j \leqslant n)$. Note that $\tilde{\theta}_j(\sum_{k=1}^n g_kx_{k\tau(j)}) = \tilde{\theta}_j(\sum_{k=1}^n g_{\tau(k)}x_{\tau(k)\tau(j)})$ holds for each j $(1 \leqslant j \leqslant n)$. By the fact that E is a regular system in $\tilde{G}_n$, we can choose $g_{\tau(i)} = e$ for all i $(1 \leqslant i \leqslant n)$. Then, we have $g_{\tau(u)} = 0$ for all u $(u \neq i)$. From this, we obtain $\tilde{\theta}_i(e)y_{ij} = \tilde{\theta}_j(x_{\tau(i)\tau(j)})$ for all i, j $(1 \leqslant i, j \leqslant n)$. That is,

$y_{ij} = \theta_i(e)^{-1}\,\tilde{\theta}_j(x_{\tau(i)\tau(j)})$ holds for all i, j $(1 \leqslant i, j \leqslant n)$. Thus, we can conclude as follows: $\Phi((x_{pq})) = (h_p^{-1}\tilde{\theta}_q(x_{\tau(p)\tau(q)}))$ for all $(x_{pq}) \in E^*$, where $h_i = \theta_i(e) \in G$ $(1 \leqslant i \leqslant n)$.

Let (x_{pq}) and (x'_{pq}) be elements in E^*. Then, we have $(x_{pq})(x'_{pq}) = (\sum_{k=1}^{n} x_{pk}x'_{kq}) \in E^*$. Since Φ is an isomorphism of E^* onto F^*, we obtain

$$\Phi((x_{pq}))\,\Phi((x'_{pq})) = \Phi\left(\left(\sum_{k=1}^{n} x_{pk}x'_{kq}\right)\right).$$

Therefore, $(h_p^{-1}\tilde{\theta}_q(x_{\tau(p)\tau(q)}))(h_p^{-1}\tilde{\theta}_q(x'_{\tau(p)\tau(q)})) = (h_p^{-1}\tilde{\theta}_q(\sum_{k=1}^{n} x_{\tau(p)k}x'_{k\tau(q)}))$ holds. From this, we have $\sum_{k=1}^{n} \tilde{\theta}_k(x_{\tau(i)\tau(k)})\,h_k^{-1}\tilde{\theta}_j(x'_{\tau(k)\tau(j)}) = \sum_{k=1}^{n} \tilde{\theta}_j(x_{\tau(i)k}x'_{k\tau(j)})$ for all i, j $(1 \leqslant i, j \leqslant n)$. By the fact that E is a regular system in $\hat{G}_n$, we can see that for any $x \in G$ there exist some group-matrices (x_{pq}), $(x'_{pq}) \in E^*$ such that $x_{\tau(i)\tau(i)} = x$ and $x'_{\tau(i)\tau(j)} = e$. Thus, we have $\theta_i(x)\,h_i^{-1}h_j = \theta_j(x)$ for all $x \in G$ and i, j $(1 \leqslant i, j \leqslant n)$. In fact, as easily seen, $\tilde{\theta}_i(x)\,h_i^{-1}h_j = \tilde{\theta}_j(x)$ holds for all $x \in G^0$ and i, j $(1 \leqslant i, j \leqslant n)$. From this, we have $\tilde{\theta}_j(x) = \tilde{\theta}_1(x)\,h_1^{-1}h_j$ for all $x \in G^0$ and j $(1 \leqslant j \leqslant n)$.

Put $\varphi(x) = h_1^{-1}\theta_1(x)$ $(x \in G)$ and $k_i = h_1^{-1}h_i \in G$ $(1 \leqslant i \leqslant n)$. Then, we have $h_i^{-1}\tilde{\theta}_j(x) = h_i^{-1}\tilde{\theta}_1(x)\,h_1^{-1}h_j = k_i^{-1}\tilde{\varphi}(x)k_j$ for all $x \in G^0$ and i, j $(1 \leqslant i, j \leqslant n)$. On the other hand, it is not difficult to verify that φ is an automorphism of G. Furthermore, we have $F = \Phi(E) = \{\Phi((x_{pq}));\ (x_{pq}) \in E\} = \{(h_p^{-1}\tilde{\theta}_q(x_{\tau(p)\tau(q)}));\ (x_{pq}) \in E\} = \{(k_p^{-1}\tilde{\varphi}(x_{\tau(p)\tau(q)})k_q);\ (x_{pq}) \in E\}$.

This completes the proof of the "only if" part.

Proof of the "if" part. Assume that there exist φ, k_i $(2 \leqslant i \leqslant n)$ and τ as in the theorem statement. Then, we put first $\Theta((g_1, g_2, \ldots, g_n)) = (\tilde{\varphi}(g_{\tau(1)}), \tilde{\varphi}(g_{\tau(2)})k_2, \tilde{\varphi}(g_{\tau(3)})k_3, \ldots, \tilde{\varphi}(g_{\tau(n)})k_n)$ $((g_1, g_2, \ldots, g_n) \in \hat{G}_n)$. It is easily seen that Θ is a permutation on $\hat{G}_n$. Next, we put $\Phi(X) = (k_p^{-1}\tilde{\varphi}(x_{\tau(p)\tau(q)})k_q)$ for all $X = (x_{pq}) \in E$, $\Phi((e_{pq})) = (e_{pq})$ and $\Phi(X_1X_2 \cdots X_t) = \Phi(X_1)\,\Phi(X_2) \cdots \Phi(X_t)$ $(X_i \in E,\ 1 \leqslant i \leqslant t,\ t \geqslant 1)$. Then, it is easy to show that Φ is well defined as a mapping. Furthermore, we can prove that Φ is an isomorphism of E^* onto F^* such that $\Theta(\hat{g}X) = \Theta(\hat{g})\,\Phi(X)$ for all $\hat{g} \in \hat{G}_n$ and all $X \in E^*$. This means that E and F are equivalent.

Thus, the "if" part is proved. Q.E.D.

5. Applications

This section contains two applications of our method. One is concerned with the input sets of automata, and another with the factor automata of automata and their automorphism groups.

First, we shall consider a relation between the input sets and the state sets of strongly connected automata.

Theorem 5.1. *Let $A = (S, \Sigma, M)$ be a strongly connected automaton whose automorphism group is isomorphic to a finite group G. Then, we have:*

$|S|\,|\Sigma| \geqslant I(G)\,|G|$, *where* $I(G) = \min\{|H|;\ H \subseteq G,\ [H] = G\}$ ($[K]$ *is the subgroup of G generated by the elements of K*).

Proof. We can assume that A is of the form $A = (\hat{G}_n, \Sigma, M_\Psi)$, i.e., A is a regular (n, G)-automaton. Then, it suffices to prove that $n \mid G \mid \mid \Sigma \mid \geqslant I(G) \mid G \mid$.

Let $\Psi(\sigma)^{\#}$ be the set of all nonzero components of $\Psi(\sigma)$, where $\sigma \in \Sigma$. Then, obviously $\mid \Psi(\sigma)^{\#} \mid \leqslant n$ holds. Since A is strongly connected, by Theorem 2.2 $[\bigcup_{\sigma\in\Sigma} \Psi(\sigma)^{\#}] = G$ must hold. Thus, we have $\mid \bigcup_{\sigma\in\Sigma} \Psi(\sigma)^{\#} \mid \geqslant I(G)$. On the other hand, $n \mid \Sigma \mid \geqslant \mid \bigcup_{\sigma\in\Sigma} \Psi(\sigma)^{\#} \mid$ holds. Therefore, we have $n \mid G \mid \mid \Sigma \mid \geqslant I(G) \mid G \mid$. Q.E.D.

From the above theorem, we can see that there is no strongly connected automaton $A = (S, \Sigma, M)$ such that $\mid \Sigma \mid < I(G)/n$, where $n = \mid S \mid / \mid G(A) \mid$ and $G(A) \approx G$. Thus, we may have the following question:

Can we construct an automaton with the smallest cardinality of input set among the strongly connected automata whose automorphism groups are isomorphic to a given finite group?

In response to such a question, for any finite group G and any positive integer n, we define the number $J(n, G)$ as follows:

$J(n, G) = \min\{\mid \Sigma \mid; A = (S, \Sigma, M)$: strongly connected automaton such that $G(A) \approx G$ and $\mid S \mid = n \mid G(A) \mid\}$.

Furthermore, by $\langle r \rangle$ we denote the positive integer m such that $m - 1 < r \leqslant m$. Then, we have the following result:

THEOREM 5.2. *Let G be a finite group and n be a positive integer. Then, we have:* $\langle I(G)/n \rangle \leqslant J(n, G) \leqslant \langle I(G)/n \rangle + p(n)$, *where* $p(1) = 0$, $p(2) = 1$ *and* $p(n) = 2$ *for* $n > 2$.

Proof. We have immediately the theorem for the case $n = 1$. Thus, we consider the case $n \geqslant 2$. The inequality $\langle I(G)/n \rangle \leqslant J(n, G)$ is immediate from Theorem 5.1. Therefore, we have to prove the inequality $J(n, G) \leqslant \langle I(G)/n \rangle + p(n)$. By the definition of $I(G)$, there exists a set of generators H of G, i.e., $[H] = G$, such that $H = \{h_i ; h_i \in G, 1 \leqslant i \leqslant I(G)\}$. Now, put $\Sigma = \Gamma \cup \Delta$, where $\Gamma = \{\gamma_i ; 1 \leqslant i \leqslant \langle I(G)/n \rangle\}$ and $\Delta = \{\delta_i ; 1 \leqslant i \leqslant p(n)\}$. Moreover, for each i $(1 \leqslant i \leqslant \langle I(G)/n \rangle)$ we can define $\Psi(\gamma_i) \in \tilde{G}_n$ such that $\Psi(\gamma_i) \neq \Psi(\gamma_j)$ $(i \neq j)$ and $H = \bigcup_{i=1}^{\langle I(G)/n \rangle} \Psi(\gamma_i)^{\#}$. Let $\{\tau_i ; 1 \leqslant i \leqslant p(n)\}$ be a set of generators of the symmetric group $S(n)$ on $\{1, 2,..., n\}$, e.g., $\{(12)\}$ for $n = 2$ and $\{(12), (123 \cdots n)\}$ for $n > 2$. Furthermore, for each i $(1 \leqslant i \leqslant p(n))$ we assign $\Psi(\delta_i) = (e_{p\tau_i(q)}) \in \tilde{G}_n$, where e is the identity of G. Thus, we can define an (n, G)-automaton $A = (\hat{G}_n, \Sigma, M_\Psi)$.

Now, we shall prove that A is regular.

Proof of the strong connectedness of A: Since $\{\tau_i ; 1 \leqslant i \leqslant p(n)\}$ is a set of generators of $S(n)$, for any pair of numbers p', q' $(1 \leqslant p', q' \leqslant n)$ there exist some numbers $i_1, i_2, ..., i_k$ such that $p' = \tau_{i_1}\tau_{i_2} \cdots \tau_{i_k}(q')$. On the other hand, we have the following equality:

$$\begin{aligned}\Psi(\delta_{i_k}\delta_{i_{k-1}} \cdots \delta_{i_2}\delta_{i_1}) &= (e_{p\tau_{i_k}(q)})(e_{p\tau_{i_{k-1}}(q)}) \cdots (e_{p\tau_{i_2}(q)})(e_{p\tau_{i_1}(q)}) \\ &= (\Sigma_{q_k, q_{k-1}, ..., q_3, q_2} e_{p\tau_{i_k}(q_k)} e_{q_k\tau_{i_{k-1}}(q_{k-1})} \cdots e_{q_3\tau_{i_2}(q_2)} e_{q_2\tau_{i_1}(q)}) \qquad (*) \\ &= (e_{p\tau_{i_1}\tau_{i_2}\cdots\tau_{i_{k-1}}\tau_{i_k}(q)}).\end{aligned}$$

By this equality and the relation between p' and q', we can see that the (p', q')-component of $\Psi(\delta_{i_k}\delta_{i_{k-1}} \cdots \delta_{i_1})$ is equal to e. Next, note that for all $h \in H$ there exist some numbers t, l, m $(1 \leqslant t \leqslant \langle I(G)/n \rangle,\ 1 \leqslant l,\ m \leqslant n)$ such that (l, m)-component of $\Psi(\gamma_t)$ is equal to h. As mentioned, for any pair of numbers p', q' $(1 \leqslant p',\ q' \leqslant n)$ there exist some group-matrices $M, N \in \Psi(\Sigma^*)$ such that the (p', l)-component of M and the (m, q')-component of N are equal to e, respectively. Thus, the (p', q')-component of $M\Psi(\gamma_t)N \in \Psi(\Sigma^*)$ becomes h. By these facts, we can see easily the strong connectedness of A.

Proof of the regularity of A: In the case $n = 2$, we can easily see the regularity of A. Because, by Theorem 2.4, it is enough to put, for example, $\left(\begin{smallmatrix} g & 0 \\ h & 0 \end{smallmatrix}\right) \in \Psi(\Gamma)$ $(g, h \in H)$, and so forth. Consequently, assume $n > 2$. By Theorem 2.5, it suffices to show the following:

For all i $(1 < i \leqslant n)$ there exist some pair of elements $x, y \in \Sigma^*$ and number i' $(1 \leqslant i' \leqslant n)$ such that $\psi_{11}(x) = \psi_{11}(y) \in G$ and $\psi_{ii'}(x) \neq \psi_{ii'}(y)$, where we put $\Psi(z) = (\psi_{pq}(z))$ for all $z \in \Sigma^*$.

By equality (*), for all $\tau \in S(n)$ there exists some element $z \in \Sigma^*$ such that $\Psi(z) = (e_{p\tau(q)})$. Let i' be a positive integer such that $1 < i' \neq i$. Put $\tau' = (i, i') \in S(n)$. Then, there exists some element $y \in \Sigma^*$ such that $\Psi(y) = (e_{p\tau'(q)})$. Now, we put $x = \epsilon \in \Sigma^*$. Then, obviously we have $\psi_{11}(x) = \psi_{11}(y) = e \in G$. But, since $\psi_{ii'}(x) = 0$ and $\psi_{ii'}(y) = e_{i\tau'(i')} = e_{ii} = e$, $\psi_{ii'}(x) = \psi_{ii'}(y)$ does not hold. Thus, A is regular. Therefore, we have $J(n, G) \leqslant \langle I(G)/n \rangle + p(n)$. Q.E.D.

COROLLARY 5.1. *Let G be a finite group. Then, there exists a strongly connected automaton $A = (S, \Sigma, M)$ such that $G(A) \approx G$ and $|\Sigma| \leqslant 3$.*

Proof. It suffices to prove that $\min\{J(n, G); n \geqslant 1\} \leqslant 3$. This is immediate from the fact that $J(n, G) \leqslant \langle I(G)/n \rangle + p(n)$ and $\min\{\langle I(G)/n \rangle + p(n); n \geqslant 1\} \leqslant 3$. Q.E.D.

In the rest of this section, we deal with a problem concerning factor automata. Fleck [5] presented the following result:

Let $A = (S, \Sigma, M)$ be a strongly connected automaton such that $|S| = |G(A)|$ and H be a normal subgroup of $G(A)$. Then, $G(A)/H \approx G(A/H)$ holds.

In connection with the above result, we may have the following question:

Is it possible to have $G(A)/H \approx G(A/H)$ in spite of $|S| \neq |G(A)|$?

We shall respond to this question for the case $|S| = 2|G(A)|$. For this purpose, we first give the following:

DEFINITION 5.1. Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be an (n, G)-automaton and ξ be a homomorphism of G onto some group. Then, A_ξ is the $(n, \xi(G))$-automaton $A_\xi = (\widehat{(\xi(G)})_n, \Sigma, M_{\xi[\Psi]})$ such that $\xi[\Psi](\sigma) = (\tilde{\xi}(\psi_{pq}(\sigma))$ for all $\sigma \in \Sigma$, where $\tilde{\xi}$ is the extension of ξ on G^0 with $\tilde{\xi}(0) = 0$, and $\Psi(\sigma) = (\psi_{pq}(\sigma))$.

The following results are immediate:

PROPOSITIION 5.1. *Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be a strongly connected (n, G)-automaton. Then, A_ξ is also strongly connected.*

i.e., $A/H \approx A'/H'$. Hence, by Theorem 1.3, $G(A/H) \approx G(A'/H')$ holds. Now, let η be a homomorphism of $G(A')$ onto some group such that $\mathrm{Ker}(\eta) = H'$. Then, by Theorem 5.3, we have $A'_\eta \approx A'/\mathrm{Ker}(\eta) = A'/H'$. Hence, $G(A'/H') \approx G(A'_\eta)$ holds. Since $A \approx A'$, A' is a regular $(2, G)$-automaton and not a permutation automaton. Thus, by Lemma 5.1, A'_η is regular. Therefore, $G(A'_\eta) \approx \eta(G(A'))$ holds. By the so-called homomorphism theorem, we have $\eta(G(A')) \approx G(A')/H'$. On the other hand, $G(A)/H \approx G(A')/H'$ holds. Consequently, we have $G(A/H) \approx G(A'/H') \approx G(A)/H$. Q.E.D.

6. Conclusion

By virtue of our new representation of strongly connected automata, we have a possibility of describing all strongly connected automata whose automorphism groups are isomorphic to a given finite group. However, to complete this problem, it is necessary to obtain a proper necessary and sufficient condition for the regularity of strongly connected group-matrix type automata. In this paper, we could deal only with special cases. Thus, we shall leave a treatment of the general case as an open problem.

Finally, we shall refer to an advantage of our method. The results in Section 5 are new ones obtained by making use of our representation. Moreover, it seems that there are many problems which are easily solvable only by our method. In fact, by making use of our new representation, we have elegant proofs for known results concerning the theory of automorphism groups of strongly connected automata.

References

1. B. H. Barnes, Groups of automorphisms and sets of equivalence classes of input for automata, *J. ACM* **12** (1965), 561–565.
2. B. H. Barnes, On the group of automorphisms of strongly connected automata, *Math. System Theory* **4** (1970), 289–294.
3. Z. Bavel, Structure and transition-preserving functions of finite automata, *J. ACM* **15** (1968), 135–158.
4. A. C. Fleck, Isomorphism groups of automata, *J. ACM* **9** (1962), 469–476.
5. A. C. Fleck, On the automorphism group of an automaton, *J. ACM* **12** (1965), 566–569.
6. Y. Masunaga, S. Noguchi, and J. Oizumi, A structure theory of automata characterized by group, *J. Comput. System Sci.* **7** (1973), 300–305.
7. G. P. Weeg, The structure of an automaton and its operation-preserving transformation group, *J. ACM* (1962), 345–349.
8. G. P. Weeg, The automorphism group of the direct product of strongly related automata, *J. ACM* **12** (1965), 187–195.

PROPOSITION 5.2. *Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be an (n, G)-automaton. Then if A is not a permutation automaton, A_ξ is neither a permutation automaton.*

Thus, we have:

LEMMA 5.1. *Let $A = (\hat{G}_2, \Sigma, M_\Psi)$ be a regular $(2, G)$-automaton and ξ be a homomorphism of G onto some group. Then if A is not a permutation automaton, A_ξ is regular.*

Proof. This is obvious from the above propositions and Corollary 2.1. Q.E.D.

THEOREM 5.3. *Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be a regular (n, G)-automaton and ξ be a homomorphism of G onto some group. Then, we have $A_\xi \approx A/\mathrm{Ker}(\xi)$, where $\mathrm{Ker}(\xi)$ means the kernel of ξ.*

Remark 5.1. In the above, we identify $G(A)$ with G. That is, we identify $\rho_g \in G(A)$ with $g \in G$ (for the notation, see the proof of Theorem 2.1).

Consequently, $\mathrm{Ker}(\xi)$ is assumed to be a subgroup of $G(A)$. In the sequel, we shall discuss this assumption.

Proof of Theorem 5.3. Put $H = \mathrm{Ker}(\xi) \subseteq G$ and $A/H = (\bar{S}_H, \Sigma, \overline{M}_H)$, where $S = \hat{G}_n$ and $M = M_\Psi$. Then, for $\hat{f} = (f_p) \in \hat{G}_n$, $\hat{k} = (k_p) \in \hat{G}_n$ we have the following: $\bar{\hat{f}} = \bar{\hat{k}} \in \bar{S}_H$ holds if and only if there exists some element $h \in H$ such that $\hat{f} = h(\hat{k}) = \rho_h(\hat{k}) = (hk_p)$. Now, we define the mapping Ξ as follows:

$$\Xi(\bar{\hat{g}}) = (\bar{\xi}(g_p)) \qquad \text{for all} \quad \hat{g} = (g_p) \in \hat{G}_n .$$

It is easily seen that Ξ is well defined as a mapping and it is a one-to-one mapping of $\bar{S}_H$ onto $\widehat{\xi(G)}_n$.

Finally, we shall show that $A_\xi \approx A/H$. Since $\overline{M}_H(\bar{\hat{g}}, \sigma) = \overline{M_\Psi(\hat{g}, \sigma)} = \overline{\hat{g}\Psi(\sigma)}$ holds for all $\hat{g} \in \hat{G}_n$ and all $\sigma \in \Sigma$, we have $\Xi(\overline{M}_H(\bar{\hat{g}}, \sigma)) = \Xi(\overline{\hat{g}\Psi(\sigma)})$. Now, we put $\hat{g} = (g_p) \in \hat{G}_n$ and $\Psi(\sigma) = (\psi_{pq}(\sigma))$. Then, we have $\hat{g}\Psi(\sigma) = (\sum_{k=1}^n g_k\psi_{kp}(\sigma))$. Thus, we have $\Xi(\overline{M}_H(\bar{\hat{g}}, \sigma)) = \Xi(\overline{\hat{g}\Psi(\sigma)}) = (\bar{\xi}(\sum_{k=1}^n g_k\psi_{kp}(\sigma))) = (\sum_{k=1}^n \bar{\xi}(g_k)\ \bar{\xi}(\psi_{kp}(\sigma))) = (\bar{\xi}(g_p))(\bar{\xi}(\psi_{pq}(\sigma))) = \Xi(\bar{\hat{g}})\ \xi[\Psi](\sigma) = M_{\xi[\Psi]}(\Xi(\bar{\hat{g}}), \sigma)$. Therefore, we obtain $A_\xi \approx A/H$. Q.E.D.

Now, we give the final result.

THEOREM 5.4. *Let $A = (S, \Sigma, M)$ be a strongly connected automaton such that $|S| = 2|G(A)|$ and H be a normal subgroup of $G(A)$. Then if A is not a permutation automaton, $G(A)/H \approx G(A/H)$ holds.*

Proof. By Theorem 3.1, there exist some mappings ρ, ξ and Ψ, respectively, of S onto $\widehat{G(A)}_2$, of Σ onto an input set Σ' and of Σ' into $\widetilde{G(A)}_2$, by which A becomes isomorphic to $A' = (\widehat{G(A)}_2, \Sigma', M_\Psi)$. Put $\varphi(g) = \rho g \rho^{-1}$ $(g \in G(A))$. Then, it is easy to see that φ is an isomorphism of $G(A)$ onto $G(A')$. Let $H' = \varphi(H)$. Then, H' is a normal subgroup of $G(A')$. Moreover, it is not difficult to verify that a pair of mappings $\bar{\rho}$ and $\bar{\xi}$ $(\bar{\rho}(\bar{s}) = \overline{\rho(s)}$ $(s \in S)$, $\bar{\xi} = \xi)$ constitutes an isomorphism of A/H onto A'/H',