数理解析研究所講究録
第 296 巻 1977 年 198-206

Input Sets of Strongly Connected Automata

Masami ITO

Faculty of Science, Kyoto Sangyo University

0. Introduction

We shall deal with the input sets of strongly connected automata whose automorphism groups are isomorphic to a given finite group G. As is well known, the cardinalities of state sets of such automata are multiples of the order of G. Hence, we cannot find, in general, an automaton having a small size of state set among the strongly connected automata whose automorphism groups are isomorphic to G. However, an automaton, whose size of input set is small and whose automorphism group is isomorphic to G, may be found. We may not admit it as a simple automaton from the engineering point of view. Because, the size of its state set is not necessarily small. Nevertheless, from the graph theoretical point of view, in which the behavior of an automaton is described in a state transition diagram, the small size of input set may be a standard for an automaton to be simple in its structure.

1. Introductory Concepts and Some Results

In this section, we provide some introductory concepts about automata and their automorphism groups, and present some fundamental results without proof. For the proofs, see (1).

DEFINITION 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 $M(s, \Lambda) = s$ for all $x,y \in \Sigma^*$. Here Σ^* is the free semigroup generated by Σ, and Λ is its identity.

DEFINITION 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 $x \in \Sigma^*$. 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 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. 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 4. Automata $A = (S, \Sigma, M)$ and $B = (T, \quad , N)$ 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 2. If A and B are automata such that $A \approx B$, then G(A) is isomorphic to G(B), also denoted $G(A) \approx G(B)$.

2. Group-Matrix Type Automata

In this section, we introduce the definition of group-matrix type automata and present some results concerning these automata. For the proofs, see (3).

DEFINITION 5. Let G be a finite group. Then G^o 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 use sometimes the notations gh and $\Sigma_{i=1}^{s} g_i$ instead of $g\cdot h$ and $g_1+g_2+ \dots +g_s$. Notice that the sum $\Sigma_{i=1}^{s} g_i$ is defined only if at most one of $g_i (1 \leq i \leq s)$ is non-zero.

DEFINITION 6. Let G be a finite group and n be a positive integer. We consider an $n \times n$ matrix $(f_{pq})(1 \leq p,q \leq n,\ f_{pq} \in G^o)$. 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 $i(1 \leq i \leq n)$, there exists a unique number $j(1 \leq j \leq n)$ such that $f_{ij} \neq 0$.

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 : $(f_{pq})(g_{pq}) = (\Sigma_{k=1}^{n} f_{pk} g_{kq})$.

DEFINITION 7. Let G be a finite group and n be a positive integer. We consider a vector $(f_p)(1 \leq p \leq n,\ f_p \in G^o)$. A vector (f_p) is called a group-vector of order n on G, if there exists a unique number $i(1 \leq i \leq n)$ such that $f_i \neq 0$. 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 : $(f_p)(g_{pq}) = (\Sigma_{k=1}^{n} f_k g_{kp})$.

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

DEFINITION 8. 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 1. The mapping Ψ can be extended to the mapping of Σ^* into $\tilde{G}_n$ as follows : $\Psi(\Lambda) = (e_{pq})(e_{pq} = 0$ 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 $x \in \Sigma^*$.

THEOREM 3. Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be an (n, G)-automaton. Then, G is isomorphic to a subgroup of G(A).

DEFINITION 9. An (n, G)-automaton A is called regular, if A is strongly connected and $G(A) \approx G$ holds.

THEOREM 4. 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 $i,j(1 \leq i,j \leq n)$ and all $g \in G$, there exists some element x in Σ^* such that $\phi_{ij}(x) = g$, where we put $\Psi(x) = (\phi_{pq}(x))$.

THEOREM 5. Let $A = (\hat{G}_1, \Sigma, M_\Psi)$ be a (1, G)-automaton. Then if A is strongly connected, A is regular.

THEOREM 6. 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 $(\Gamma \neq \emptyset)$ of G such that $\phi(k) = k$, $\phi^2(g) = kgk^{-1}$ for all $g \in G$, and $\Psi(\Sigma) = \{ \Psi(\sigma) ; \sigma \in \Sigma \}$ $= \{ \begin{pmatrix} g & 0 \\ 0 & \phi(g) \end{pmatrix}, \begin{pmatrix} 0 & h \\ \phi(h) & 0 \end{pmatrix} ; g \in \Lambda, h \in \Gamma \}$.

THEOREM 7. Let $A = (\hat{G}_n, \Sigma, M_\Psi)$ be a strongly connected (n, G)-automaton. Furthermore, assume that there exists some number $i'(1 \leq i' \leq n)$ which satisfies the following condition : For all $i(1 \leq i \leq n, i \neq i')$, there exist some elements $x,y \in \Sigma^*$ and number $q'(1 \leq q' \leq n)$ such that

$\phi_{i'q}(x) = \phi_{i'q}(y)$ for all $q(1 \leq q \leq n)$ and that $\phi_{iq'}(x) \neq \phi_{iq'}(y)$, where $\Psi(x) = (\phi_{pq}(x))$ and $\Psi(y) = (\phi_{pq}(y))$.

Under this assumption, A is regular.

THEOREM 8. Let $A = (S, \Sigma, M)$ be a strongly connected automaton such that $|S| = n|G(A)|$, where n is a positive integer. 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.

3. Input Sets of Strongly Connected Automata

In the present section, the input sets of strongly connected automata are considered.

THEOREM 9. Let $A = (S, \Sigma, M)$ be a strongly connected automaton whose automorphism group is isomorphic to a finite group G. Then, we have $|S||\Sigma| \geq I(G)|G|$, where $I(G) = \min\{ |H| ; H \subset G, [H] = G \}$($[K]$ is the subgroup of G generated by 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 $n|G||\Sigma| \geq I(G)|G|$.

Let $\Psi(\sigma)^{\#}$ be the set of all non-zero component of $\Psi(\sigma)$, where $\sigma \in \Sigma$. Then, obviously $|\Psi(\sigma)^{\#}| \leq n$ holds. By the strong connectedness of A, we obtain immediately $[\bigcup_{\sigma \in \Sigma} \Psi(\sigma)^{\#}] = G$.
Thus, we have $| \bigcup_{\sigma \in \Sigma} \Psi(\sigma)^{\#} | \geq I(G)$.

On the other hand, $n|\Sigma| \geq |\bigcup_{\sigma \in \Sigma} \Psi(\sigma)^{\#}|$ holds. Therefore, we have $n|G||\Sigma| \geq I(G)|G|$. Q.E.D.

From the above theorem, we can see that there is no strongly connected automaton $A = (S, \Sigma, M)$ such that $|\Sigma| < I(G)/n$, where $n = |S|/|G(A)|$ 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 this question, for any finite group G and any positive integer n, we define the number J(n, G) as follows :

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

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

THEOREM 10. Let G be a finite group and n be a positive integer. Then, we have $\langle I(G)/n \rangle \le J(n, G) \le \langle I(G)/n \rangle + p(n)$, where $p(1) = 0$ and $p(n) = 1$ for $n \ge 2$.

Proof. We can prove immediately the theorem for the case $n = 1$. Therefore, we consider the case $n \ge 2$.

The inequality $\langle I(G)/n \rangle \le J(n, G)$ is immediate from THEOREM 9. Hence, we have to prove the inequality $J(n, G) \le \langle I(G)/n \rangle + p(n)$. By the definition of I(G), there exists a set of generators H of G, i.e., $[H] = G$, such that $H = \{\ h_i\ ;\ h_i \in G,\ 1 \le i \le I(G)\ \}$.
Now, put $\Sigma = \Gamma \cup \{\delta\}$, where $\Gamma = \{\ \gamma_i\ ;\ 1 \le i \le \langle I(G)/n \rangle\ \}$.
Moreover, for each $i (1 \le i \le \langle I(G)/n \rangle\ )$ we can define $\Psi(\gamma_i) \in \tilde{G}_n$ such that all elements of $\Psi(\gamma_i)^{\#}$ are gathered only into the first column of $\Psi(\gamma_i)$, $\Psi(\gamma_i) \ne \Psi(\gamma_j) (i \ne j)$ and $H = \bigcup_{i=1}^{\langle I(G)/n \rangle} \Psi(\gamma_i)^{\#}$.
Put $\tau = (123\ \ldots\ n) \in S(n)$, where S(n) denotes the symmetric group on $\{1,2,3,\ \ldots\ ,n\}$. Furthermore, we assign $\Psi(\delta) = (e_{p\tau(q)}) \in \tilde{G}_n$, where e is the identity of G. Thus, we can define an (n, G)-automaton $A = (\ \hat{G}_n, \Sigma, M_\Psi\ )$.

Now, we prove that A is regular. Proof of the strong connectedness of A : First, we prove that, for all $i, j (1 \le i, j \le n)$ and all $h \in H$, there exists an element $x \in \Sigma^*$ such that the $(i,\ j)$-component of $\Psi(x)$ is equal to h.

By the assignment of $\Psi(\Gamma)$, for each $h \in H$ there exist some integer $s (1 \leq s \leq n)$ and $t (1 \leq t \leq \langle I(G)/n \rangle)$ such that the $(s,\ 1)$-component of $\Psi(\gamma_t)$ is equal to h. Now, we put $x = \delta^u \gamma_t \delta^{n-j+1}$, where $u \equiv i-s \pmod{n}$ and $u > 0$. Here, by $\delta^k (k \geq 1)$ we denote $\delta^{k-1}\delta (\delta^o = \Lambda)$.
Then, it is not difficult to verify that the $(i,\ j)$-component of $\Psi(x)$ is equal to h.

From this fact, we can prove easily that, for all $i, j (1 \leq i, j \leq n)$ and all $g \in G$, there exists an element $x \in \Sigma^*$ such that the $(i,\ j)$-component of $\Psi(x)$ is equal to g. By THEOREM 4, this indicates the strong connectedness of A.

Proof of the regularity of A : Let γ be an arbitrary element in Γ, g be the $(1,\ 1)$-component of $\Psi(\gamma)$ and k be the order of g. Then, the $(1,\ 1)$-component of $\Psi(\gamma^k)$ is equal to e. On the other hand, the $(1,\ 1)$-component of $\Psi(\delta^n)$ is also equal to e. By a comparison of these two group-matrices and by THEOREM 6 and 7, the regularity of A can be proved.

Thus, the existence of an automaton $A = (\ S,\ \Sigma,\ M\ )$ such that $G(A) \approx G$, $|S| = n|G(A)|$ and $|\Sigma| = \langle I(G)/n \rangle + 1$ could be shown. And this completes the proof of the theorem. Q.E.D.

REMARK 2. There is the case $J(n,\ G) = \langle I(G)/n \rangle$. For instance, we shall consider the following case.

Let G be the permutation group $[\{a,\ b,\ c\}]$ on $\{1,2,3,\ \ldots\ ,9\}$, where $a = (123)$, $b = (456)$ and $c = (789)$. Then, obviously we have $I(G) = 3$ and thus $\langle I(G)/2 \rangle = 2$. Now, put $\Sigma = \{\gamma,\ \delta\}$, $\Psi(\gamma) = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ and $\Psi(\delta) = \begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}$.

Then, it is easily seen that the automaton $A = (\hat{G}_2, \Sigma, M_\Psi)$ is a regular $(2, G)$-automaton. Thus, we have $J(2, G) = \langle I(G)/2 \rangle = 2$.
In the proof of the above, notice a role of the input δ, i.e.,

$$\Psi(\delta^3) = \begin{pmatrix} 0 & c^3 \\ c^3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix}.$$

In a manner similar to the above, we have :

THEOREM 11. Let n and k be positive integers which are relatively prime, and G be a finite group such that $I(G) \equiv 1 (\mathrm{mod}\ n)$. Furthermore, assume that there exist a set of generators H of G and an element $h \in H$ such that $|H| = I(G)$ and $o(h) \equiv k (\mathrm{mod}\ n)$, where $o(h)$ means the order of h. Then, we have $J(n, G) = \langle I(G)/n \rangle$.

COROLLARY. Let G be a finite group such that $I(G)|G|$ is an odd number. Then, we have $J(2, G) = \langle I(G)/2 \rangle$.

Proof. This is the case where we put, in the above theorem, $n = 2$, $k = 1$, $I(G) \equiv 1 (\mathrm{mod}\ 2)$ and $o(h) \equiv 1 (\mathrm{mod}\ 2)$. Here, h is an arbitrary element in H. Q.E.D.

THEOREM 12. Let G be a finite group. Then, there exists a strongly connected automaton $A = (S, \Sigma, M)$ such that $G(A) \approx G$ and $|\Sigma| \leq 2$.

Proof. It suffices to prove that $\min\{ J(n, G) \ ; \ n \geq 1 \} \leq 2$. However, this is immediate from the fact that $J(n, G) \leq \langle I(G)/n \rangle + p(n)$ and $\min\{ \langle I(G)/n \rangle + p(n) \ ; \ n \geq 1 \} \leq 2$. Q.E.D.

4. Conclusion

Let G be a non-cyclic finite group. Since the automorphism group of a one-input strongly connected automaton is always cyclic, we cannot find a one-input strongly connected automaton whose sutomorphism group is isomorphic to G. Consequently, THEOREM 12 gives the best estimation for the bound of cardinalities of input sets.

Acknowledgement

The author warmly thanks Mr. K.Uemura of Nagasaki University for his valuable suggestion.

References

(1) A.C. Fleck, Isomorphism Groups of Automata, J.ACM 9 (1962), p.469

(2) A.C. Fleck, On the Automorphism Group of an Automaton, J.ACM 12 (1965), p.566

(3) M. Ito, Representations of Strongly Connected Automata, Trans. IECE Japan J59-D (1976), p.33