COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 29, No. 1, 1980

On the Group of Automorphisms of Cyclic Automata

by

Genjiro TANAKA

(Received April 22, 1980)

This paper is a continuation of the studies by Fleck, Trauth and the others. One of the methods used in the study of algebraic structures of automata is the consideration of automorphism groups of automata. Fleck [4], Weeg [15] investigated the class of perfect automata and Trauth [14] generalized Fleck's results, introducing the class of quasi-perfect automata. Masunaga *et al.* [10] introduced the class of quasi-state-independent automata and generalized Trauth's results. In this paper, we introduce a new class of cyclic automata which are called quasi-regular. The class of quasi-regular automata contains the class of quasi-perfect automata as a proper subclass.

In Section 1 of this paper, for the purpose of studying automorphism groups of automata, we consider basic properties of centralizer semigroups of permutation groups. Quasi-perfect automata are essentially "the automaton representations" of finite groups and are, in a certain sense, the regular representations of finite groups. Quasi-regular automata are also closely related to quasi-regular permutation groups (Proposition 2.1). The properties of centralizers of permutation groups are shown in terms of mapping matrix (Theorems 1.1 and 1.2). In this case, the notion of reducer matrix of a permutation group plays a fundamental role. Thus Section 1 contains reducers of permutation groups, quasi-regular permutation groups, $G\bar{C}$-matrices and $\bar{A}G$-matrices. All definitions for permutation groups, used but not explained here, can be found in Wielandt [16].

In Section 2, the relationships between the structure of a cyclic automaton A and the structure of its automorphism group $G(A)$ are mainly investigated. By the notion of reducers of permutation groups we can obtain an interpretation of a relationship between inputs of an automaton A and constituents of the automorphism group $G(A)$ (Theorem 2.2). We pay our attention to Bavel's result [2] that any automorphism of a cyclic automaton is completely determined by its action on the set of generators of the automaton, and for a cyclic automaton A we define the automaton A^* on the set of generators of A. A cyclic automaton A is called quasi-regular if $G(A)$ is transitive on the set of all generators of A. It is shown that if A is a quasi-regular automaton such that $G(A) \neq \{1\}$, then the input-set of A has a certain partition and A^* is a quasi-perfect automaton such that $G(A^*)$ is isomorphic to $G(A)$ (Theorem 2.3). We give an example of a construction of a quasi-regular automaton by using $\bar{A}G$-matrices (Example 2.2). In the latter half of this section, the relationships between A^* and the factor automaton of a cyclic automaton A are studied and, by our Theorem 2.5, Ito's

result [8] is extended easily to cyclic automata (Proposition 2.7).

1. Centralizers of permutation groups

Let $f: S_1 \to S_2$ and $g: S_2 \to S_3$ be mappings of S_1 and S_2, respectively. We read a product fg from left to right;

$$(s)(fg)=((s)f)g\,, \qquad s\in S_1\,.$$

And $((s)f)g$ is denoted simply by $(s)fg$.

Let $X=(x_{ij})$ be an $m\times n$ matrix. If for each i $(i=1, \cdots, m)$, there is a unique number k such that x_{ik} is 1 and other (i, j)-th entries are 0, then X is called a mapping matrix. An $m\times m$ mapping matrix X is called a permutation matrix if all column vectors of X are not the zero vector. Let B_1 and B_2 be two finite sets and α be a mapping from B_1 into B_2. To α we assign the mapping matrix $P(\alpha)$ which is a $|B_1|\times|B_2|$ matrix whose entry in position (i, j) is 1 if $(a_i)\alpha=b_j$ and zero otherwise, where $a_i\in B_1$ and $b_j\in B_2$. If α is one-to-one and onto, then $P(\alpha)$ is a permutation matrix. Note that if X is an $m\times n$ mapping matrix such that each column of X is not the zero vector and if P is an $n\times n$ permutation matrix such that $XP=X$, then P is the identity matrix.

Definition 1.1. Let G_i $(i=1, 2)$ be two groups and Δ be a subset of $G_1\times G_2$. Δ is called a δ-pair of $G_1\times G_2$, if

$$G_1=\{x\in G_1 \mid (x, y)\in\Delta\} \quad \text{and} \quad G_2=\{y\in G_2 \mid (x, y)\in\Delta\}\,.$$

Example 1.1.

(1) $G_1\times G_2$ is a δ-pair of $G_1\times G_2$.

(2) If $\alpha: G_1\to G_2$ is an onto mapping, then $\{(x, (x)\alpha) \mid x\in G_1\}$ is a δ-pair of $G_1\times G_2$.

Notice that if Δ is a δ-apir of $G_1\times G_2$, then the following two subsets are δ-pairs, respectively, of $G_1\times G_2$ and $G_2\times G_1$;

$$\Delta^{-1}=\{(x^{-1}, y^{-1}) \mid (x, y)\in\Delta\} \quad \text{and} \quad {}^t\Delta=\{(y, x) \mid (x, y)\in\Delta\}\,.$$

When G is a permutation group (or a transformation semigroup) on a finite set B, we shall write G more concretely as (G, B).

LEMMA 1.1. *Let (G_1, B_1) and (G_2, B_2) be two transitive permutation groups and Δ be a δ-pair of $G_1\times G_2$. In addition, let X be a $|B_1|\times|B_2|$ matrix such that $P(g_1)X=XP(g_2)$ for all $(g_1, g_2)\in\Delta$. Then we have*

(1) *If some row of X is a zero vector, then $X=0$.*

(2) *If some column of X is a zero vector, then $X=0$.*

(3) *If X is an $m\times n$ mapping matrix, then $m\geqq n$.*

(4) *If (x, y), $(u, v)\in\Delta$, then $P(xu)X=XP(yv)$.*

Proof. Suppose that the k-th row of X is a zero vector. Since G_1 is transitive, for each entry x_{ij} of X it is possible to find some $g\in G_1$ such that (k, i)-th entry of $P(g)$ is 1.

If $(g, h) \in \Delta$, then $P(g)X = XP(h)$. The k-th row of $XP(h)$ is a zero vector and the (k, j)-th entry of $P(g)X$ is x_{ij}. Hence we have $x_{ij}=0$ and (1) holds. For (2), consider the transpose of matrix. By the hypothesis, some row of ${}^tX$ is a zero vector. Since ${}^tP(g_2){}^tX = {}^tX{}^tP(g_1)$ for all $(g_2, g_1) \in {}^t\Delta$ and ${}^tP(g) = P(g^{-1})$ for an arbitrary permutation g, we have ${}^tX = 0$ from (1). This proves (2). It is clear that (2) implies (3). Finally, if $(x, y), (u, v) \in \Delta$, then

$$P(xu)X = P(x)(P(u)X) = P(x)XP(v) = XP(y)P(v) = XP(yv).$$

Q.E.D.

PROPOSITION 1.1. *Let (G_i, B_i) $(i=1, 2)$ be two transitive permutation groups and Δ be a δ-pair of $G_1 \times G_2$. In addition, let X be a mapping matrix such that $P(g_1)X = XP(g_2)$ for all $(g_1, g_2) \in \Delta$. Then we have*

(1) *α: $G_1 \to G_2$, which is defined by $(g_1)\alpha = g_2$ if $(g_1, g_2) \in \Delta$, is well-defined and α is a homomorphism from G_1 onto G_2.*

(2) *If $|B_1| = |B_2|$, then X is a permutation matrix and α* is an isomorphism from *G_1 onto G_2.*

Proof. (1) Let $(x, y), (x, z) \in \Delta$, then $XP(y) = XP(z)$. Hence $XP(yz^{-1}) = X$ and this implies that $P(yz^{-1})$ is the identity matrix. Thus $y = z$ and α is well-defined. From the definition of δ-pair it follows that α is an onto mapping. Δ can be written in the form

$$\Delta = \{(x, (x)\alpha) \mid x \in G_1\}.$$

For any $(x, (x)\alpha), (y, (y)\alpha) \in \Delta$, by Lemma 1.1, we have $P(xy)X = XP((x)\alpha(y)\alpha)$. On the other hand, $P(xy)X = XP((xy)\alpha)$ since $(xy, (xy)\alpha) \in \Delta$. Thus we conclude that $(xy)\alpha = (x)\alpha(y)\alpha$ for all $x, y \in G_1$.

(2) Since $|B_1| = |B_2|$, X is a square mapping matrix such that all column vectors of X are not the zero vector. This means that X is a permutation matrix. If $(x, z), (y, z) \in \Delta$, then $P(x)X = P(y)X$. It implies $P(x) = P(y)$ because there exists the inverse of X. Thus α is one-to-one. Q.E.D.

Definition 1.2. Let (G_i, B_i) $(i=1, 2)$ be two permutation groups. If there exist two mappings α and ξ which satisfy the following conditions, then (G_2, B_2) is called a reduction of (G_1, B_1) and (α, ξ) is called a reducer of (G_1, B_1) onto (G_2, B_2):

(1) α is a homomorphism from G_1 onto G_2 and ξ is a mapping from B_1 onto B_2.

(2) For all $b \in B_1$ and $g \in G_1$, $(b)g\xi = (b)\xi(g)\alpha$.

If, in addition, α is an isomorphism and ξ is one-to-one, then (G_1, B_1) and (G_2, B_2) are said to be equivalent to each other, and denoted as $(G_1, B_1) \cong_p (G_2, B_2)$.

If (α, ξ) is a reducer of (G_1, B_1) onto (G_2, B_2), then we have that $P(g)P(\xi) = P(\xi)P((g)\alpha)$ for all $g \in G_1$ and also we have the commutative diagram

$$\begin{array}{ccc} B_1 & \xrightarrow{\xi} & B_2 \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle (g)\alpha} \\ B_1 & \xrightarrow[\xi]{} & B_2 \end{array} \quad \text{, where } g \in G_1.$$

Example 1.2. Let (G, B) be a permutation group and H be a subgroup of G. For each $x \in G$, ξ_x: $H \to x^{-1}Hx$ is defined by $(y)\xi_x = x^{-1}yx$ for all $y \in H$. Then $(b)yx = (b)x(y)\xi_x$ for all $b \in B$ and $y \in H$. Hence (ξ_x, x) is a reducer of (H, B) onto $(x^{-1}Hx, B)$.

Definition 1.3. Let (G, B) be a permutation group. A mapping matrix X is called a reducer matrix of (G, B) if there exists some reducer (α, ξ) of (G, B) such that $P(\xi) = X$.

PROPOSITION 1.2. *Let (α, ξ) be a reducer of (G, B) onto itself. Then, α is the identity mapping if and only if ξ is a permutation in the centralizer of G in $\mathfrak{S}_B$, where $\mathfrak{S}_B$ is the symmetric group on B.*

Proof. If $\alpha = 1$, then $g\xi = \xi g$ for all $g \in G$. Since ξ is an onto mapping and B is a finite set, the mapping ξ is a permutation in the centralizer of G in $\mathfrak{S}_B$.

Conversely, if ξ is an element in the centralizer of G in $\mathfrak{S}_B$, then $\xi g = g\xi = \xi(g)\alpha$ for all $g \in G$. Thus $(g)\alpha = g$ for all $g \in G$. Q.E.D.

PROPOSITION 1.3. *Let (G_1, B_1) and (G_2, B_2) be two transitive permutation groups, and let Δ be a δ-pair of $G_1 \times G_2$. If there exists a mapping matrix X such that $P(g_1)X = XP(g_2)$ for all $(g_1, g_2) \in \Delta$, then (G_2, B_2) is a reduction of (G_1, B_1) and X is a reducer matrix of (G_1, B_1).*

Proof. By Proposition 1.1, α: $G_1 \to G_2$, which is defined by $(g_1)\alpha = g_2$ if $(g_1, g_2) \in \Delta$, is a homomorphism from G_1 onto G_2. Define the mapping ξ: $B_1 \to B_2$ by $(s_i)\xi = t_j$ if the (i, j) entry of X is 1, where $s_i \in B_1$ and $t_j \in B_2$. Then $X = P(\xi)$ and $(s)g_1\xi = (s)\xi(g_1)\alpha$ for all $s \in B_1$ and $g_1 \in G_1$. Q.E.D.

Let G be a group with a subgroup H and let $G\backslash H = \{Hx_1, \cdots, Hx_n\}$ be the set of all right cosets of H in G. Then we have a homomorphism π_H from G into the symmetric group on $G\backslash H$ given by

$$\pi_H : g \longrightarrow \begin{pmatrix} \cdots & Hx_i & \cdots \\ & Hx_ig & \end{pmatrix}.$$

A homomorphism α from G into the symmetric group on a set B is called a permutation representation of G on B. We say α is transitive if $(G)\alpha$ is transitive on B.

PROPOSITION 1.4. *Let α: $G \to (K, B)$ be a transitive permutation representation. Then there exists a subgroup H of G such that*

$$((G)\pi_H, G\backslash H) \cong_p (K, B).$$

For the proof, see Huppert [7], p. 29.

A permutation group (G, B) is called semiregular if for each $b \in B$, $G_b = \{1\}$, where $G_b = \{g \in G | (b)g = b\}$ (the stabilizer of b). A permutation group G is called regular if it is semiregular and transitive.

PROPOSITION 1.5. *Let (G, B) be a regular permutation group and let $\mathfrak{T}_B$ be the*

full transformation semigroup on B. Then

$$G^+ = \{f \in \mathfrak{T}_B \mid fg = gf \quad \text{for all} \quad g \in G\}$$

is a regular permutation group on B.

For the proof, see Dörfler [3] (Folgerung 3).

PROPOSITION 1.6. *If a transitive permutation group (G, B) is abelian, then G is its own centralizer in* $\mathfrak{S}_B$.

For the proof, see Wielandt [16], p. 9 or Huppert [7], p. 29.

Let G be a group. To each $g \in G$ we assign the permutations

$$g^* = \begin{pmatrix} \cdots & x & \cdots \\ & xg & \end{pmatrix} \quad \text{and} \quad {}^*g = \begin{pmatrix} \cdots & x & \cdots \\ & g^{-1}x & \end{pmatrix}, \quad x \in G .$$

Then $G^* = \{g^* \mid g \in G\}$ and ${}^*G = \{{}^*g \mid g \in G\}$ are regular on G. G^* and ${}^*G$ are called the right regular and left regular representations of G, respectively. $({}^*G, G)$ is the centralizer of (G^*, G) in $\mathfrak{T}_G$.

Remark 1.1. Let S be a semigroup with a left identity. To each $t \in S$ we assign the transformations

$$t^* : s \to st \quad \text{and} \quad {}^*t : s \to ts, \quad s \in S .$$

Then $({}^*S, S)$ is the centralizer of (S^*, S) in $\mathfrak{T}_S$.

Let G be a group and consider the two mappings

$$\alpha : {}^*G \to G^*({}^*x \to x^*) \quad \text{and} \quad \xi : G \to G(g^{-1} \to g) .$$

Then (α, ξ) is a reducer of $({}^*G, G)$ onto (G^*, G), and $({}^*G, G)$ is equivalent to (G^*, G).

If (G, B) is a regular permutation group and $b_1 \in B$, then for each $b_i \in B$ there exists a unique element $g_i \in G$ such that $(b_1)g_i = b_i$. Therefore the operation $*$ on B defined by

$$b_i * b_j = (b_1)g_i g_j$$

is well-defined. It is easy to see that B forms a group under the operation $*$ and the group $B = (B, *)$ is isomorphic to G. Thus we may regard the regular permutation (G, B) as the right regular representation of G. From Proposition 1.2, we have the following immediately.

PROPOSITION 1.7. *Let G be a group and* (α, ξ) *be a reducer of* (G^*, G) *onto itself. Then* α *is the identity mapping if and only if* $\xi \in {}^*G$.

PROPOSITION 1.8. *Let G be a group and H be a subgroup of G. Define the two mappings* ξ *and* π'_H *as follows*:

$$\pi'_H : G^* \to (G)\pi_H \qquad (x^* \to (x)\pi_H)$$

and

$$\xi : G \to G \backslash H \qquad (g \to Hg) .$$

Then (π'_H, ξ) *is a reducer of* (G^*, G) *onto* $((G)\pi_H, G\backslash H)$.

Proof. For all $g\in G$ and $x^*\in G^*$,

$$(g)x^*\xi=(gx)\xi=Hgx=(Hg)(x)\pi_H=(g)\xi(x^*)\pi'_H\,.$$

Q.E.D.

Definition 1.4. Let (G, B) be a permutation group and $\{B_i|\, i=1, \cdots, r\}$ be the set of all G-orbits, where $|B_j|\geqq|B_{j+1}|$ for all $j=1, \cdots, r-1$. If $|G|=|B_1|$, then (G, B) is called quasi-regular.

Let (G, B) be a quasi-regular permutation group and (G_i, B_i) $(1\leqq i\leqq r)$ be the constituent of G on B_i. Then (G_1, B_1) is regular and each $g\in G$ can be written in the form $g=g_1\cdots g_i\cdots g_r$, where g_i is an element of G_i. The mapping $\alpha_i: G\to G_i$ defined by $(g)\alpha_i=g_i$ is a homomorphism from G onto G_i. Thus we have $|G_i|\,||\,G|$ and $|B_i|\,||\,B_1|$ for all $i=1, \cdots, r$. If $|B_i|=|B_1|$ for all $i=1, \cdots, r$, then G is semiregular. If $r=1$, then G is regular. We notice that in general $|B_i|>|B_j|$ does not imply $|G_i|>|G_j|$.

PROPOSITION 1.9. *Let* (G, B) *be a quasi-regular permutation group and* (G_i, B_i) $(1\leqq i\leqq r)$ *be constituents of* G *on* G*-orbits. If* G *is abelian, then* (G_i, B_i) *is regular for all* i.

Proof. It follows easily from Proposition 1.6. Q.E.D.

In the case that a quasi-regular permutation group G is not abelian, its constituent on some G-orbit B is not necessarily regular on B. For instance, see the constituent G_2 in Example 2.2.

Definition 1.5. Let (G, B) be a permutation group and (G_i, B_i), where $i=1, \cdots, r$, be all constituents of G on G-orbits. The δ-pair Δ_{ij} of $G_i\times G_j$ is defined by $(g_i, g_j)\in\Delta_{ij}$ if there exists $g\in G$ such that $g=g_1\cdots g_i\cdots g_j\cdots g_r$ $(g_k\in G_k)$.

In the above notations, the set M_{ij} of matrices is defined by

$$M_{ij}=\{X\,|\,X \text{ is a mapping matrix such that } P(g_i)X=XP(g_j) \quad \text{for all} \quad (g_i, g_j)\in\Delta_{ij}\}\,.$$

Definition 1.6. Let (G, B) be a permutation group and let

$$\bar{C}=\{(G_i, B_i)\,|\,1\leqq i\leqq r,\ |B_j|\geqq|B_{j+1}|,\ 1\leqq j\leqq r-1\}$$

be the set of all constituents of G on G-orbits. If the set of matrices $\{X_{pq}\,|\,1\leqq p, q\leqq r\}$ satisfies the following conditions, then the matrix $X=(X_{pq})$ is called a $G\bar{C}$-matrix:

(1) X_{pq} is a $|B_p|\times|B_q|$ matrix for all p and q $(1\leqq p, q\leqq r)$.

(2) For each p $(1\leqq p\leqq r)$, there exists a unique number k such that $X_{pk}\neq 0$ and if $X_{pk}\neq 0$, then $X_{pk}\in M_{pk}$.

THEOREM 1.1. *Let* (G, B) *be a permutation group and let*

$$\bar{C}=\{(G_i, B_i)|\ 1\leqq i\leqq r,\ |B_j|\geqq|B_{j+1}|,\ 1\leqq j\leqq r-1\}$$

be the set of all constituents of G *on* G*-orbits. Then* X *is a mapping matrix such that*

$P(g)X=XP(g)$ for all $g\in G$ if and only if X is a $G\bar{C}$-matrix.

Proof. Let

$$P(g)=\begin{bmatrix} P(g_1) & & & \\ & P(g_2) & & \\ & & \ddots & \\ & & & P(g_r) \end{bmatrix} \quad X=\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1r} \\ X_{21} & X_{22} & \cdots & X_{2r} \\ & & \cdots & \\ & & \cdots & \\ X_{r1} & X_{r2} & \cdots & X_{rr} \end{bmatrix},$$

where $g=g_1g_2\cdots g_r\in G(g_i\in G_i)$ and X_{ij} is a $|B_i|\times|B_j|$ matrix. Since X is a mapping matrix, every entry of X_{ij} is equal to 0 or 1. Comparing the (i, j) block of $P(g)X$ with the (i, j) block of $XP(g)$, we have $P(g_i)X_{ij}=X_{ij}P(g_j)$ for all $(g_i, g_j)\in\Delta_{ij}$. If $X_{ij}\neq 0$, then all rows of X_{ij} are not the zero vector by Lemma 1.1. Thus X_{ij} is a mapping matrix and $X_{ij}\in M_{ij}$.

Conversely, if X is a $G\bar{C}$-matrix, then $X_{ij}=0$ or $X_{ij}\in M_{ij}$. Therefore $P(g_i)X_{ij}=X_{ij}P(g_j)$ for all $(g_i, g_j)\in\Delta_{ij}$. Thus we have $P(g)X=XP(g)$ for all $g\in G$. Q.E.D.

From the form of $G\bar{C}$-matrix we have

COROLLARY 1.1. *Let (G, B) be a permutation group and let G^+ be the centralizer of G in $\mathfrak{T}_B$. If $f\in G^+$ and B' is a G-orbit, then $\{(b)f \mid b\in B'\}$ is also a G-orbit, and thus f maps any orbit of G onto an orbit of G.*

Definition 1.7. Let (G_1, B_1) be a transitive permutation group and let

$$\bar{\Delta}=\{(G_i, B_i) \mid 1\leqq i\leqq r, |B_j|\geqq|B_{j+1}|, 1\leqq j\leqq r-1\}$$

be a set of reductions of (G_1, B_1). If the matrix $X=(X_{pq})$, where $1\leqq p, q\leqq r$, satisfies the following conditions, then X is called a $\bar{\Delta}G_1$-matrix:

(1) X_{pq} is a $|B_p|\times|B_q|$ matrix for all p and q $(1\leqq p, q\leqq r)$.

(2) For each p $(1\leqq p\leqq r)$, there exists a unique number k such that $X_{pk}\neq 0$ and if $X_{pk}\neq 0$, then X_{pk} is a reducer matrix of (G_p, B_p) onto (G_k, B_k).

Example 1.3. Let $G=\langle x\rangle\times\langle y\rangle$ be an elementary abelian group of order 4 and let e be the identity of G. Put

$$x_1=\begin{pmatrix} e & x & y & xy \\ x & e & xy & y \end{pmatrix}, \qquad y_1=\begin{pmatrix} e & x & y & xy \\ y & xy & e & x \end{pmatrix}$$

$$e_1=x_1^2, \qquad G_1=\langle x_1, y_1\rangle \quad \text{and} \quad B_1=\{e, x, y, xy\}.$$

Then (G_1, B_1) is the right regular representation of G. Let $H=\langle x\rangle$. Then $G\backslash H=\{H, Hy\}$ and

$$(e)\pi_H=\begin{pmatrix} H & Hy \\ H & Hy \end{pmatrix}, \qquad (y)\pi_H=\begin{pmatrix} H & Hy \\ Hy & H \end{pmatrix}.$$

Set $e_2=(e)\pi_H$, $y_2=(y)\pi_H$, $B_2=G\backslash H$ and $G_2=\langle y_2\rangle$. For two permutation groups G_1 and G_2, we consider the following reducer (Proposition 1.8):

$$\alpha=\begin{pmatrix} e_1 & x_1 & y_1 & x_1y_1 \\ e_2 & e_2 & y_2 & y_2 \end{pmatrix}, \qquad \xi=\begin{pmatrix} e & x & y & xy \\ H & H & Hy & Hy \end{pmatrix}.$$

And also consider the reducer of G_2 onto itself as follows (Proposition 1.2):

$$\beta=\begin{pmatrix} e_2 & y_2 \\ e_2 & y_2 \end{pmatrix}, \qquad \mu=\begin{pmatrix} H & Hy \\ Hy & H \end{pmatrix}.$$

Put $\bar{\Delta}=\{G_1, G_2\}$, then the following matrix X is a $\bar{\Delta}G_1$-matrix.

$$X=\begin{bmatrix} 0 & P(\xi) \\ 0 & P(\mu) \end{bmatrix}=\begin{array}{c} \\ e \\ x \\ y \\ xy \\ H \\ Hy \end{array}\begin{array}{c} \begin{array}{cccccc} e & x & y & xy & H & Hy \end{array} \\ \left[\begin{array}{cccc|cc} 0 & 0 & 0 & 0 & 1 & 0 \\ & & & & 1 & 0 \\ & & & & 0 & 1 \\ & & & & 0 & 1 \\ \hline & & & & 0 & 1 \\ & & & & 1 & 0 \end{array}\right] \end{array}.$$

In the following diagram, let (α_i, ξ_i) $(i=1, 2)$ be reducers of (G_i, B_i) $(i=1, 2)$, respectively. Then $(\alpha_1\alpha_2, \xi_1\xi_2)$ is a reducer of (G_1, B_1) onto (G_3, B_3):

$$(G_1, B_1) \xrightarrow{(\alpha_1, \xi_1)} (G_2, B_2) \xrightarrow{(\alpha_2, \xi_2)} (G_3, B_3).$$

Thus, if X and Y are $\bar{\Delta}G_1$-matrices, then XY is also a $\bar{\Delta}G_1$-matrix.

THEOREM 1.2. *Let (G, B) be a quasi-regular permutation group and let*

$$\bar{\Delta}=\{(G_i, B_i) \mid 1\leqq i\leqq r, \ |B_j|\geqq|B_{j+1}|, \ 1\leqq j\leqq r-1\}$$

be the set of all constituents of G on G-orbits. If X is a mapping matrix such that $P(g)X=XP(g)$ for all $g\in G$, then X is a $\bar{\Delta}G_1$-matrix.

Proof. Owing to the quasi-regularity of G, the mapping $\alpha_i: G_1\to G_i$, which is defined by $(g_1)\alpha_i=g_i$ if $g=g_1\cdots g_i\cdots g_r\in G(g_i\in G_i)$, is a homomorphism from G_1 onto G_i. Since α_i is a permutation representation of the group G_1, by Proposition 1.4 there is a subgroup H_1 of G_1 such that

$$((G_1)\pi_{H_1}, G_1\backslash H_1)\cong_p(G_i, B_i).$$

By Proposition 1.8, there exists some reducer of (G_1^*, G_1) onto $((G_1)\pi_{H_1}, G_1\backslash H_1)$. Since (G, B) is quasi-regular, (G_1, B_1) is a regular permutation group. Therefore (G_1, B_1) is equivalent to (G_1^*, G_1). It follows that (G_i, B_i) is a reduction of (G_1, B_1), so that all (G_i, B_i) $(1\leqq i\leqq r)$ are reductions of (G_1, B_1). Using the proof of Theorem 1.1, we have Theorem 1.2. Q.E.D.

Let $S=\{1, \cdots, r\}$ and G be a group. To each $g\in G$, we assign a permutation $(g)\theta$ on $G\times S$;

$$(g)\theta=\begin{pmatrix} \cdots & (h, i) & \cdots \\ & (hg, i) & \end{pmatrix}, \text{ where } \quad h\in G \quad \text{and} \quad i\in S.$$

Denote the set of all such permutations by $(G)\theta$. Then $((G)\theta, G\times S)$ is a semiregular permutation group which has r orbits. Conversely, if (G, B) is a semiregular permutation group with r orbits, then (G, B) is equivalent to $((G)\theta, G\times S)$.

If $(g)\theta\in((G)\theta, G\times S)$, then $P((g)\theta)$ is a matrix whose (i, i)-th blocks, where $i=1, \cdots, r$, are equal to $P(g^*)$, $g^*\in G^*$. If X is a mapping matrix such that $P(g^*)X=XP(g^*)$ for all $g^*\in G^*$, then, by Proposition 1.7, there exists some $^*h\in{}^*G$ such that $X=P(^*h)$. Therefore we have the following result from Theorem 1.1.

PROPOSITION 1.10. *Let G be a group and $S=\{1, \cdots, r\}$, and let X be a mapping matrix. Then $P((g)\theta)X=XP((g)\theta)$ for all $g\in G$ if and only if X satisfies the following conditions*:

(1) *$X=(X_{ij})$ $(1\leqq i, j\leqq r)$, where all X_{ij} are $|G|\times|G|$ matrices.*

(2) *For each i $(1\leqq i\leqq r)$, there exists a unique number k such that $X_{ik}\neq 0$.*

(3) *If $X_{ik}\neq 0$, then $X_{ik}=P(^*h)$ for some $^*h\in{}^*G$.*

Let $C((G)\theta, G\times S)$ be the set of all mapping matrices which commute with all $P((g)\theta)$, $g\in G$. From Proposition 1.10 and the fact $|{}^*G|=|G|$, we have $|C((G)\theta, G\times S)|=|G|^r\cdot r^r$. $C((G)\theta, G\times S)$ froms a semigroup under the multiplication of matrices. The preimage W of $C((G)\theta, G\times S)$ under P is a transformation semigroup on $G\times S$. The centralizer of W in $\mathfrak{S}_{G\times S}$ is $((G)\theta, G\times S)$ (see (2) of Lemma of [12]). For a subsemigroup J of W, we put

$$C(J)=\{g\in\mathfrak{S}_{G\times S}\mid gf=fg \quad \text{for all} \quad f\in J\}\,.$$

Then it is obvious that $((G)\theta, G\times S)\subseteq C(J)$. However we do not have a necessary and sufficient condition about J in order that $C(J)$ is equal to $((G)\theta, G\times S)$, where $|S|>1$. This is clearly a difficult problem.

Definition 1.8. Let H be a group and (K, S) be a transformation semigroup on S. The wreath product $H\wr K$ of H and K is the set

$$\{(f, \lambda)\mid \lambda\in K, f \text{ is a mapping from } S \text{ into } H\}$$

which has the multiplication

$$(f_1, \lambda)(f_2, \mu)=(f_3, \lambda\mu)\,,$$

where $(i)f_3=(i)f_1((i)\lambda)f_2$ for all $i\in S$.

$H\wr K$ forms a semigroup and if K is a permutation group, then $H\wr K$ forms a group (see [7], p. 95).

PROPOSITION 1.11. *Let G be a group and $\mathfrak{T}_S$ be the full transformation semigroup on S. Then $C((G)\theta, G\times S)$ is isomorphic to $G\wr\mathfrak{T}_S$.*

Proof. $F=\{f\mid f \text{ is a mapping from } S \text{ into } G\}$ forms a group under the operation $\circ$, where (i) $(f\circ f')=(i)f(i)f'$ for all $i\in S$. To each $i\in S$, we set $D_i=\{(f_{ix}, e)\mid x\in G\}$, where e is the identity permutation on S and

$$(j)f_{ix}=\begin{cases}x & \text{if } j=i\,,\\ 1_G \ \text{(the identity of } G) & \text{if } j\neq i\,.\end{cases}$$

Then D_i is isomorphic to G as group and $f \in F$ is written in the form

$$f = f_{1x_1} \circ f_{2x_2} \circ \cdots \circ f_{rx_r},\ f_{ix_i} \in D_i\,,$$

where $r = |S|$ and $i = 1, \cdots, r$. If $v, w \in G \wr \mathfrak{T}_S$ and

$$v = (f_{1x_1} \circ \cdots \circ f_{rx_r},\ \lambda), \qquad w = (f_{1y_1} \circ \cdots \circ f_{ry_r},\ \mu)\,,$$

then $vw = (f',\ \lambda\mu)$ where $(i)f' = x_i y_{(i)\lambda}$ for all $i \in S$. We define the mapping P: $G \wr \mathfrak{T}_S \to C((G)\theta,\ G \times S)$ as follows;

If $v = (f_{1x_1} \circ \cdots \circ f_{ix_i} \circ \cdots \circ f_{rx_r},\ \lambda) \in G \wr \mathfrak{T}_S$, then $P(v)$ is a matrix whose $(i, (i)\lambda)$ block is $P(^*x_i)$.

Then we can easily prove that P is an isomorphism from $G \wr \mathfrak{T}_S$ onto $F((G)\theta,\ G \times S)$. Q.E.D.

2. Automorphism groups of automata

In this section we deal with the groups of automorphisms of automata.

Definition 2.1. An automaton A is a triple, $A = (S, I, M)$, where S is a nonempty finite set of states, I is a nonempty finite set of inputs and $M: S \times \tilde{I} \to S$ is a next state function, called state transition function, such that $M(s, xy) = M(M(s, x), y)$ and $M(s, \varepsilon) = s$ for all $s \in S$ and all $x, y \in I$. Here $\tilde{I}$ is the free semigroup generated by the elements of I and ε is the identity of $\tilde{I}$.

Definition 2.2. Let $A = (S, I, M)$ be an automaton. A permutation g on S is called an automorphism of the automaton A if $M((s)g, x) = (M(s, x))g$ for all $s \in S$ and all $x \in \tilde{I}$.

Fleck [4] has shown that the set of all automorphisms of an automaton A forms a group, denoted by $G(A)$. Let $A = (S, I, M)$ be an automaton. The reachability set of $s \in S$ is defined by $r(s) = \{M(s, x) \mid x \in \tilde{I}\}$.

Definition 2.3. An automaton $A = (S, I, M)$ is called a cyclic automaton if there is an $s \in S$ such that $r(s) = S$. Such an element s is called a generator of A. If an automaton A is cyclic and if every element of S is a generator, then A is called strongly connected ([4], [11], [15]).

In this paper, by S_A we denote the set of all generators of an automaton $A = (S, I, M)$.

Definition 2.4. An automaton $A = (S, I, M)$ is called quasi-perfect if A is strongly connected and if $G(A)$ is transitive on S. If $M(s, xy) = M(s, yx)$ for all $s \in S$ and $x, y \in \tilde{I}$, then A is called abelian. An automaton A is called perfect if A is abelian and quasi-perfect ([4], [14]).

THEOREM 2.1 (Bavel [2]). *If $A = (S, I, M)$ is a cyclic automaton, then the restriction of $G(A)$ on S_A is a semiregular permutation group and $|G(A)|$ divides $|S_A|$.*

For the proof, see Corollary 1 and Theorem 6 of Bavel [2].

COROLLARY 2.1 (Fleck [4]). *If $A=(S, I, M)$ is a strongly connected automaton, then $G(A)$ is a semiregular permutation group on S and $|G(A)|$ divides $|S|$.*

Remark 2.1. In the case that $A=(S, I, M)$ is strongly connected and $G(A)$ has r orbits, the permutation group $(G(A), S)$ is equivalent to $((G)\theta, G\times B)$, where $G=G(A)$ and $B=\{1, \cdots, r\}$. If $x\in I$, then $\bar{x}$: $S\to M(s, x)$, $s\in S$, is a mapping from S into itself. If we regard $G(A)$ as the permutation group $((G)\theta, G\times B)$, then $\bar{x}$ is regarded as a transformation on $G\times B$ and $\langle P(\bar{x})\mid x\in I\rangle$ is a subsemigroup of $C((G)\theta, G\times B)$. For the computation of those matrices it is a convenience to remove "P" from matrices in $C((G)\theta, G\times B)$. For instance

$$X=\begin{bmatrix}0 & P(g_1)\\ P(g_2) & 0\end{bmatrix}\longrightarrow X=\begin{bmatrix}0 & g_1\\ g_2 & 0\end{bmatrix}.$$

The right-hand matrix is called a group-matrix (of order 2). Ito [8], [9] has shown that the semigroup which consists of group-matrices is a useful tool for the study of automorphism groups of automata.

Definition 2.5. An automaton $A=(S, I, M)$ is called a permutation automaton if for every $x\in I$ the mapping

$$\bar{x}\colon s\to M(s, x), \qquad s\in S,$$

is a permutation on S([13]).

Let $A=(S, I, M)$ be a quasi-perfect automaton, then $G(A)$ is transitive on S and $|G(A)|=|S|$ by Corollary 2.1. This means that $(G(A), S)$ is a regular permutation group. If $x\in\tilde{I}$, then the transformation $\bar{x}$ on S is a semiregular permutation by Proposition 1.5. Therefore, a quasi-perfect automaton is a permutation automaton.

Now we present relationships between an input of an automaton A and constituents of $G(A)$.

THEOREM 2.2. *Let $A=(S, I, M)$ be an automaton, and let G_i and G_j be constituents of $G(A)$ on orbits B_i and B_j, respectively. If $x\in\tilde{I}$ and $M(s_0, x)\in B_j$ for some $s_0\in B_i$, then ξ_x: $s\to M(s, x)$, $s\in B_i$, is a mapping from B_i onto B_j and for ξ_x there exists some reducer (α, ξ_x) of (G_i, B_i) onto (G_j, B_j).*

Proof. Since $M((s_0)g, x)=(M(s_0, x))g\in(B_i)g$ for all $g\in G(A)$ and both B_i and B_j are $G(A)$-orbits, ξ_x is a mapping from B_i onto B_j. Let G_k, $k=1, \cdots, r$, be constituents of $G(A)$ on $G(A)$-orbits and let $g=g_1\cdots g_i\cdots g_j\cdots g_r$ ($g_k\in G_k$) be an arbitrary element in $G(A)$, then for $s\in B_i$ we have

$$\begin{aligned}M((s)g_i, x)&=M((s)g, x)\\ &=(M(s, x))g=(M(s, x))g_j\end{aligned}$$

It implies that $(s)g_i\xi_x=(s)\xi_x g_j$ for all $s\in B_i$ and $(g_i, g_j)\in\Delta_{ij}$, so that $P(g_i)P(\xi_x)=P(\xi_x)P(g_j)$ for all $(g_i, g_j)\in\Delta_{ij}$. By Proposition 1.1, the mapping α: $G_i\to G_j$, given by $(g_i)\alpha=g_j$ if $(g_i, g_j)\in\Delta_{ij}$, is a homomorphism from G_i onto G_j. Therefore (α, ξ_x) is a reducer of G_i onto G_j. Q.E.D.

COROLLARY 2.2. *Let $A=(S, I, M)$ be an automaton, and let G_i and G_j be constituents of $G(A)$ on orbits B_i and B_j, respectively. If one of the following conditions holds, then $M(s, x)\notin B_j$ for all $s\in B_i$ and $x\in\tilde{I}$.*

(1) $|B_j|\not>|B_i|$.

(2) $|G_j|\not>|G_i|$.

(3) *The correspondence α: $G_i\to G_j$, given by $(g_i)\alpha=g_j$ if $(g_i, g_j)\in\Delta_{ij}$, is not well-defined as a mapping.*

Proof. (1) If there exist some $s_0\in B_i$ and $x\in\tilde{I}$ such that $M(s_0, x)\in B_j$, then ξ_x: $s\to M(s, x)$ $(s\in B_i)$ is a mapping from B_i onto B_j. Let $B_j=\{t_1, \cdots, t_n\}$ and $D_k=\{s\in B_i\,|\,M(s, x)=t_k\}$, where $k=1, \cdots, n$. Since B_j is a $G(A)$-orbit, for given $t_k\in B_j$ there exists $g_k\in G(A)$ such that $(t_1)g_k=t_k$. If $s\in D_1$, then $(M(s, x))g_k=M((s)g_k, x)=t_k$. Therefore $(s)g_k\in D_k$ for all $s\in D_1$. This means that $|D_1|\leqq|D_k|$. Similarly we obtain $|D_k|\leqq|D_1|$ by considering g_k^{-1}. Hence $|D_1|=|D_k|$ for all $k=1, \cdots, n$. Thus we have that $|B_i|=n|D_1|=|B_j|\cdot|D_1|$.

(2) and (3) follow from the proof of Theorem 2.2. Q.E.D.

Let $A=(S, I, M)$ be an automaton and U be a $G(A)$-orbit. If $|U|=1$, then U is called a one-state orbit. For instance, the set $\{14\}$ in Example 2.2 is a one-state orbit.

COROLLARY 2.3. *Let $A=(S, I, M)$ be an automaton, and let G_i and G_j be constituents of $G(A)$ on orbits B_i and B_j, respectively. If*

$$G_i/N_i\ncong G_j/N_j$$

for any pair of $N_i\lneqq G_i$ and $N_j\lneqq G_j$, then

$$R_{ij}=\left\{\bigcup_{s\in B_i} r(s)\right\}\cap\left\{\bigcup_{t\in B_j} r(t)\right\}$$

is an empty set or the set which is a union of one-state orbits.

Proof. If R_{ij} is not an empty set, then there exists some orbit B_k such that $B_k\cap R_{ij}\neq\varnothing$. By Theorem 2.2, $B_k\subseteqq R_{ij}$ and (G_k, B_k) is a reduction of both (G_i, B_i) and (G_j, B_j). Since G_k on B_k is a transitive permutation representation of G_i and G_j, there exist normal subgroups $N_i\trianglelefteqq G_i$ and $N_j\trianglelefteqq G_j$ such that

$$G_i/N_i\cong G_k\cong G_j/N_j\,.$$

By the hypothesis, $N_i=G_i$ and $N_j=G_j$. Therefore (G_k, B_k) is an identity group and $|B_k|=1$. Q.E.D.

Now we introduce the notion of quasi-regular automata and, in Proposition 2.1 and Theorem 2.3, we establish some of their properties.

Definition 2.6. Let $A=(S, I, M)$ be an automaton. If A is cyclic and $G(A)$ is transitive on S_A, then the automaton A is called quasi-regular.

PROPOSITION 2.1. *If $A=(S, I, M)$ is a quasi-regular automaton, then $G(A)$ is a quasi-regular permutation group.*

Proof. From the definition and Theorem 2.1, we have $|G(A)|=|S_A|$. Let B_i be an arbitrary $G(A)$-orbit and $s\in B_i$, then there exist some $t_0\in S_A$ and $x\in\tilde{I}$ such that $M(t_0, x)=s$. From Theorem 2.2, ξ_x: $t\to M(t, x)$, $t\in S_A$, is a mapping from S_A onto B_i. It implies that $|S_A|\geqq|B_i|$. Q.E.D.

Let $A=(S, I, M)$ be a cyclic automaton. We define the subset I_A of I by

$$I_A=\{x\in I|M(s, x)\in S_A \quad \text{for all} \quad s\in S_A\},$$

and by $\tilde{I}_A$ we denote the free semigroup generated by I_A.

In general there are cyclic automata such that $I_A=\varnothing$ and $G(A)\neq\{1\}$. However we have

LEMMA 2.1. *Let $A=(S, I, M)$ be a quasi-regular automaton. Then*

(1) *If $|S_A|\neq 1$, then I_A is not empty.*

(2) *If x is an element in $\tilde{I}$ such that $x\neq\varepsilon$ and $M(s, x)\in S_A$ for at least one $s\in S_A$, then I_A is not empty and $x\in\tilde{I}_A$.*

Proof. (2) Let $s\in S_A$ and $x=x_1\cdots x_n$, where $x_i\in I$ for $i=1, \cdots, n$. Suppose that $M(s, x)\in S_A$, then

$$\xi_x\colon t\to M(t, x), \qquad t\in S_A,$$

is a mapping from S_A onto S_A by Theorem 2.2. If $n=1$, then $x=x_1\in I_A$ and I_A is not empty. If $n\geqq 2$, then

$$M(M(s, x_1\cdots x_{n-1}), x_n)\in S_A$$

and so

$$M(s, x_1\cdots x_{n-1})\in S_A.$$

This shows that $x_n\in I_A$ and I_A is not empty. Similarly, since all $M(s, x_1\cdots x_{n-1})$, $M(s, x_1\cdots x_{n-2})$, $\cdots$, $M(s, x_1)$ are in S_A, we have that $x_1, \cdots, x_n\in I_A$ and $x\in\tilde{I}_A$.

(1) If $|S_A|\neq 1$, then there exist elements $s, t\in S_A$ such that $s\neq t$. Since s is a generator of A, there exists $x\in\tilde{I}$ such that $M(s, x)=t\in S_A$. In this case, the element x is not ε. Therefore, from (2) we have (1) of our lemma. Q.E.D.

Definition 2.7. Let $A=(S, I, M)$ be a cyclic automaton such that $I_A\neq\varnothing$. Then the automaton A^* is defined by $A^*=(S_A, I_A, M_A)$, where M_A is the restriction of M to $S_A\times\tilde{I}_A$.

Note that if A is a strongly connected automaton, then $A=A^*$.

LEMMA 2.2. *Let $A=(S, I, M)$ be a cyclic automaton such that $I_A\neq\varnothing$, then the restriction of $G(A)$ to S_A is a subgroup of $G(A^*)$.*

Proof is straightforward and, therefore, omitted.

THEOREM 2.3 *Let $A=(S, I, M)$ be a quasi-regular automaton such that $|S_A|\neq 1$. Then we have*

(1) *$A^*=(S_A, I_A, M_A)$ is a quasi-perfect automaton.*

(2) $G(A)\cong G(A^*)$.

(3) $I=I_A\cup I_0$ *and* $I_A\cap I_0=\varnothing$, *where*

$$x\in I_A \Leftrightarrow M(s, x)\in S_A \quad \text{for all} \quad s\in S_A,$$
$$x\in I_0 \Leftrightarrow M(s, x)\notin S_A \quad \text{for all} \quad s\in S.$$

Proof. If a quasi-regular automaton A is strongly connected, then A is quasi-perfect and this theorem is obvious.

(3) Assume that $I-I_A\neq\varnothing$ and $x\in I-I_A$. If $M(s, x)\in S_A$ for some $s\in S$, then $s\in S_A$ and from Lemma 2.1 we have $x\in I_A$. This is a contradiction. Hence if $x\in I-I_A$, then $M(s, x)\notin S_A$ for all $s\in S$.

(1) (2) For given $s, t\in S_A$ there exists $x\in\tilde{I}$ such that $M(s, x)=t$. In this case, the element x must be in $\tilde{I}_A$ by Lemma 2.1. Consequently, A^* is strongly connected and so $|G(A^*)|\leqq|S_A|$ by Corollary 2.1. On the other hand, by the quasi-regularity and by Lemma 2.2, we have that $|S_A|=|G(A)|\leqq|G(A^*)|$. Therefore $|S_A|=|G(A)|=|G(A^*)|$. This means that A^* is quasi-perfect and $G(A)$ is isomorphic to $G(A^*)$.

Q.E.D.

PROPOSITION 2.2. *Let* $A=(S, I, M)$ *be a quasi-regular automaton such that* $|S_A|\neq 1$. *If* A *is abelian and* B_i *is a* $G(A)$*-orbit, then* $A_i=(B_i, I_A, M_i)$ *is a perfect automaton, where* M_i *is the restriction of* M *to* $B_i\times\tilde{I}_A$.

Proof. We prove first that $A_i=(B_i, I_A, M_i)$ is well-defined as an automaton. Let $x\in I_A$ and $s\in B_i$, then there exist $u\in S_A$ and $y\in\tilde{I}$ such that $M(u, y)=s$. From the fact that S_A itself is a $G(A)$-orbit and from Theorem 2.2, we have that $M(v, y)\in B_i$ for all $v\in S_A$. Since $M(u, x)\in S_A$ and

$$M(s, x)=M(M(u, y), x)=M(u, yx)$$
$$=M(u, xy)=M(M(u, x), y),$$

we have $M(s, x)\in B_i$. Therefore, if $x\in I_A$, then $M(s, x)\in B_i$ for all $s\in B_i$ and we can define the automaton $A_i=(S_i, I_A, M_i)$.

Let $s, t\in B_i$, then there exist $u\in S_A$ and $y\in\tilde{I}$ such that $M(u, y)=s$. Since ξ_y: $w\to M(w, y)$, $w\in S_A$, is an onto mapping by Theorem 2.2, we can find some $v\in S_A$ such that $M(v, y)=t$. Using Lemma 2.1, we have $M(u, x)=v$ for some $x\in\tilde{I}_A$, and

$$M(s, x)=M(M(u, y), x)=M(M(u, x), y)=M(v, y)=t.$$

Thus $A_i=(B_i, I_A, M_i)$ is strongly connected. Since A_i is abelian and the restriction of $G(A)$ to B_i is transitive, i.e., $G(A_i)$ is transitive on B_i, the automaton A_i is perfect.

Q.E.D.

In the case that a quasi-regular automaton A is not abelian, $A_i=(B_i, I_A, M_i)$ is not necessarily well-defined as an automaton.

Let $A=(S, I, M)$ be an automaton. If for any given $(s, t)\in S\times S$ there exists some $x\in\tilde{I}$ such that $M(s, x)=t$ or $M(t, x)=s$, then A is called unilaterally connected. Note that a unilaterally connected automaton is a cyclic automaton (Theorem 16.1 of [6]).

Let $A=(S, I, M)$ be a quasi-regular automaton and B_i be a $G(A)$-orbit such that $|B_i|\geqq 2$. If A is unilaterally connected and $s, t\in B_i$ $(s\neq t)$, then there exists some $x\in\tilde{I}$

such that $M(s, x)=t$ or $M(t, x)=s$. Suppose that $M(s, x)=t$. Since $s\in B_i$ and $M(s, x)\in B_i$, ξ_x: $u\to M(u, x)$, $u\in B_i$, is a mapping from B_i onto B_i by Theorem 2.2. Therefore, the set

$$I_i=\{x\in\tilde{I}\mid M(s, x)\in B_i \quad \text{for all} \quad s\in B_i\}$$

contains an element $x\in\tilde{I}$ such that $x\neq\varepsilon$, and hence I_i is an infinite set. We can define the automaton

$$\tilde{A}_i=(B_i, I_i, \tilde{M}_i)\,,$$

where $\tilde{M}_i$ is the restriction of M to $B_i\times I_i$. We note again that if $M(s, x)\in B_i$ for some $s\in B_i$, then $M(t, x)\in B_i$ for all $t\in B_i$. In Barnes [1], $\tilde{A}_i$ is called a full subautomaton. Define the equivalence relation on I_i by $x\rho y$ if and only if $\tilde{M}_i(s, x)=\tilde{M}_i(s, y)$ for all $s\in B_i$, and denote by $[x]$ the set of all $y\in I_i$ such that $x\rho y$ and by $[I_i]$ the set of all such classes. We define the automaton

$$A_{(i)}=(B_i, [I_i], M_i)$$

by

$$M_i(s, [x])=\tilde{M}_i(s, x)\ (=M(s, x))\,.$$

Then we have the following result.

PROPOSITION 2.3. *Under the hypothesis and with the notation mentioned above, $A_{(i)}$ is a quasi-perfect automaton.*

Proof. If $g\in G(A)$ and $s\in B_i$, then $(s)g\in B_i$ and for any $x\in I_i$ we have

$$\begin{aligned}(M_i(s, [x]))g&=(M(s, x))g\\&=M((s)g, x)=M_i((s)g, [x])\,.\end{aligned}$$

Hence the restriction of g to B_i is an element in $G(A_{(i)})$. Since B_i is an orbit of $G(A)$, $G(A_{(i)})$ is transitive on B_i. By the unilateral connectedness of A, for any given s, $t\in B_i$ $(s\neq t)$ there exists some $x\in I_i$ such that $M(s, x)=t$ or $M(t, x)=s$. Without loss of generality we may assume that $M(s, x)=t$. Since B_i is a $G(A)$-orbit, there exists some $h\in G(A)$ such that $(s)h=t$. Note that $M(s, x)=t=(s)h$. By induction on n, we have

$$M(s, x^n)=(s)h^n\,.$$

If m is the order of h, then

$$\begin{aligned}M(t, x^{m-1})&=M(M(s, x), x^{m-1})\\&=M(s, x^m)=(s)h^m=s\,.\end{aligned}$$

Therefore, for given s, $t\in B_i$ there exist some elements x, $y\in I_i$ such that $M(s, x)=t$ and $M(t, y)=s$. This means that $A_{(i)}$ is strongly connected. Thus $A_{(i)}$ is a quasi-perfect automaton. Q.E.D.

Remark 2.2. Let $A=(S, I, M)$ be an automaton and $s\in S$. The relation ρ_s on $\tilde{I}$ is defined by $x\rho_s y$ if and only if $M(s, x)=M(s, y)$. It is obvious that ρ_s is a right

congruence relation on the free semigroup $\tilde{I}$. In Masunaga *et al.* [10], the quasi-state-independent automaton is defined as follows:

An automaton $A=(S, I, M)$ is called quasi-state-independent with respect to a state s if it satisfies the condition

$$\rho_s \subseteqq \rho_t \qquad \text{for all} \quad t \in S .$$

If B is a $G(A)$-orbit and $s, t \in B$, then $\rho_s=\rho_t$. Thus, if an automaton is quasi-perfect, then it is quasi-state-independent with respect to any state of it. A quasi-perfect automaton is also quasi-regular. In general there are quasi-regular automata which are not quasi-state-independent.

Example 2.1. Let $A=(S, I, M)$ be a cyclic automaton such that

$$S=\{1, 2, 3, 4, 5, 6\}, \qquad I=\{x, y\}$$

and

M	1	2	3	4	5	6
x	2	1	3	4	4	3
y	3	4	5	6	5	6

,

where $M(i, x)$ and $M(i, y)$ are obtained from the above table. For example, $M(1, x)=2$. Then A is quasi-regular, but A is not quasi-state-independent.

PROPOSITION 2.4. *Let G be a finite group. Then there exists a quasi-regular automaton $A=(S, I, M)$ such that $I-I_A \neq \varnothing$ and $G(A)$ is isomorphic to G.*

Proof. Let ∞ and ξ be symbols. Define the automaton

$$A=(G \cup \{\infty\}, G \cup \{\xi\}, M)$$

by

$$M(s, g)=\begin{cases} s \circ g & \text{if } s \in G \text{ and } g \in G , \\ \infty & \text{if } s=\infty , \\ \infty & \text{if } g=\xi , \end{cases}$$

where $\circ$ is the group operation. Then $G(A)$ is isomorphic to the left regular representation of G and so $G(A)$ is transitive on $S_A(=G)$. Therefore A is quasi-regular. Q.E.D.

Note that the quasi-regular automaton which is mentioned in the above proof is quasi-state-independent.

Now we give an example of a construction of a quasi-regular automaton by using $\bar{\Delta}G_1$-matrices.

Example 2.2. Let $\mathfrak{S}_{14}$ be the symmetric group of degree 14 and let

$$x=(1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8\ 9)\ (10)\ (11)\ (12)\ (13)\ (14) \in \mathfrak{S}_{14}$$

$$y=(1\ 4)\ (2\ 6)\ (3\ 5)\ (7)\ (8\ 9)\ (10\ 11)\ (12\ 13)\ (14) \in \mathfrak{S}_{14} .$$

Put $G=\langle x, y\rangle$, then G is a quasi-regular permutation group. Let

$$x_1=(1\ 2\ 3)\ (4\ 5\ 6) \qquad x_2=(7\ 8\ 9)$$
$$y_1=(1\ 4)\ (2\ 6)\ (3\ 5) \qquad y_2=(7)\ (8\ 9)$$
$$y_3=(10\ 11) \qquad y_4=(12\ 13) \quad \text{and} \quad y_5=(14)=e_5\ ,$$

where e_5 and e_i $(i=1, \cdots, 4)$ in what follows are identity permutations. Let

$$G_1=\langle x_1, y_1\rangle \qquad B_1=\{1, 2, 3, 4, 5, 6\}$$
$$G_2=\langle x_2, y_2\rangle \qquad B_2=\{7, 8, 9\} \qquad G_3=\langle y_3\rangle \qquad B_3=\{10, 11\}$$
$$G_4=\langle y_4\rangle \qquad B_4=\{12, 13\} \qquad G_5=\langle y_5\rangle \qquad B_5=\{14\}\ ,$$

then

$$\Delta=\{(G_1, B_1), (G_2, B_2), (G_3, B_3), (G_4, B_4), (G_5, B_5)\}$$

is the set of all constituents of G. We consider reducers of these permutation groups. Let

$$^*x_1=(1\ 2\ 3)\ (4\ 6\ 5) \quad \text{and} \quad ^*y_1=(1\ 4)\ (2\ 5)\ (3\ 6)\ ,$$

then $^*G_1=\langle ^*x_1, ^*y_1\rangle$ is the centralizer of G_1. Let

$$\alpha_1=\begin{pmatrix} e_1 & x_1 & x_1^2 & y_1 & y_1x_1 & y_1x_1^2 \\ e_2 & x_2 & x_2^2 & y_2 & y_2x_2 & y_2x_2^2 \end{pmatrix}$$

and

$$\xi_1=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 7 & 8 & 9 \end{pmatrix},$$

then, since $P(x_1)P(\xi_1)=P(\xi_1)P(x_2)$ and $P(y_1)P(\xi_1)=P(\xi_1)P(y_2)$, (α_1, ξ_1) is a reducer of G_1 onto G_2. Let

$$\alpha_2=\begin{pmatrix} e_1 & x_1 & x_1^2 & y_1 & y_1x_1 & y_1x_1^2 \\ e_3 & e_3 & e_3 & y_3 & y_3 & y_3 \end{pmatrix}$$

and

$$\xi_2=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 10 & 10 & 10 & 11 & 11 & 11 \end{pmatrix},$$

then, (α_2, ξ_2) is a reducer of G_1 onto G_3. Let

$$\xi_3=\begin{pmatrix} 7 & 8 & 9 \\ 14 & 14 & 14 \end{pmatrix} \quad \text{and} \quad \alpha_3=\begin{pmatrix} e_2 & x_2 & x_2^2 \\ e_5 & e_5 & e_5 \end{pmatrix},$$

then (α_3, ξ_3) is a reducer of G_2 onto G_5. Let

$$\xi_4=\begin{pmatrix} 10 & 11 \\ 12 & 13 \end{pmatrix} \quad \text{and} \quad \alpha_4=\begin{pmatrix} e_3 & y_3 \\ e_4 & y_4 \end{pmatrix}$$

and let

$$\xi_5=\begin{pmatrix}12 & 13\\ 10 & 11\end{pmatrix} \quad \text{and} \quad \alpha_5=\begin{pmatrix}e_4 & y_4\\ e_3 & y_3\end{pmatrix}.$$

Then (α_4, ξ_4) and (α_5, ξ_5) are reducers of G_3 and G_4, respectively. Next, we construct the following $\bar{\Delta}G_1$-matrices;

$$U=\begin{bmatrix} P(*x_1) & & & & \\ & P(e_2) & & & \\ & & P(e_3) & & \\ & & & P(e_4) & \\ & & & & P(e_5) \end{bmatrix}$$

$$V=\begin{bmatrix} P(*y_1) & & & & \\ & P(e_2) & & & \\ & & P(y_3) & & \\ & & & P(y_4) & \\ & & & & P(e_5) \end{bmatrix}$$

$$W=\begin{bmatrix} 0 & P(\xi_1) & & & \\ & P(e_2) & & & \\ & & P(e_3) & & \\ & & & P(e_4) & \\ & & & & P(e_5) \end{bmatrix}$$

$$Z=\begin{bmatrix} 0 & 0 & P(\xi_2) & 0 & 0 \\ & 0 & 0 & 0 & P(\xi_3) \\ & & 0 & P(\xi_4) & 0 \\ & & P(\xi_5) & 0 & 0 \\ & & & & P(e_5) \end{bmatrix}$$

Then, it is easy to see that U, V, W and Z commute with $P(x)$ and $P(y)$. Consider the preimages u, v, w and z of U, V, W and Z, respectively, and define the automaton $A=(S, I, M)$ such that

$$S=\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\},$$

$$I=\{u, v, w, z\},$$

and

M	1	2	3	4	5	6	7	8	9	10	11	12	13	14
u	2	3	1	6	4	5	7	8	9	10	11	12	13	14
v	4	5	6	1	2	3	7	8	9	11	10	13	12	14
w	7	8	9	7	8	9	7	8	9	10	11	12	13	14
z	10	10	10	11	11	11	14	14	14	12	13	10	11	14

Then, since $G \subseteq G(A)$ and $|G| = |S_A|$, we have $G(A) = G$.

Definition 2.8. Let $A = (S, I, M)$ be an automaton and $G(A)$ be its automorphism group. Then for a subgroup H of $G(A)$, the factor automaton, A/H, is $A/H = (\bar{S}, I, \bar{M})_H$, where $\bar{S}$ is the set of all H-orbits on S and for $\bar{s} \in \bar{S}$ and $x \in \tilde{I}$, $\bar{M}(\bar{s}, x) = \overline{M(s, x)}$. (The symbol $\bar{s}$ denotes the H-orbit which contains an element s of S.)

If $A = (S, I, M)$ is cyclic automaton and H is a subgroup of $G(A)$. Then A/H is a cyclic automaton, and an H-orbit B is a generator of A/H if and only if $B \subseteq S_A$.

PROPOSITION 2.5. *Let $A = (S, I, M)$ be a quasi-regular automaton and H be a subgroup of $G(A)$, then $I_A = I_{A/H}$.*

Proof. If $|S_A| = 1$, then $|G(A)| = |S_A| = 1$. Therefore $G(A) = H = \{1_G\}$ (the identity group) and A/H is isomorphic to A. Thus we have that $I_A = I_{A/H}$.

Suppose that $|S_A| \neq 1$, then $I_A \neq \varnothing$ by Lemma 2.1. By $\bar{S}_A$ we denote the set of all generators of A/H. Let $x \in I_A$ and $B_1 \in \bar{S}_A$. If $\bar{M}(B_1, x) = B_2$, then there exists $s \in B_1$ and $t \in B_2$ such that $M(s, x) = t$. Note that $s \in B_1 \subseteq S_A$ and $x \in I_A$, then in views of Theorem 2.3 we have that $t \in S_A$ and $B_2 \subseteq S_A$. Therefore $B_2 \in \bar{S}_A$ and so $I_A \subseteq I_{A/H}$.

Let $y \in I_{A/H}$ and $B \in \bar{S}_A$, then $B \subseteq S_A$ and $\bar{M}(B, y) \in \bar{S}_A$. This means that $M(s, y) \in S_A$ for $s \in B (\subseteq S_A)$. By Theorem 2.3 we have that $y \in I_A$, so that $I_{A/H} \subseteq I_A$.
Q.E.D.

PROPOSITION 2.6. *Let $A = (S, I, M)$ be a cyclic automaton and H be a normal subgroup of $G(A)$. Then $G(A)/H$ is isomorphic to a subgroup of $G(A)/H$.*

Proof. Let $Hg \in G(A)/H$. Then Hg acts on $\bar{S}$ by $(\bar{s})Hg = \overline{(s)g}$ for all $\bar{s} \in \bar{S}$. By this action Hg is an automorphism of A/H. The action of $G(A)/H$ on $\bar{S}$ is faithful because $G(A)$ is semiregular on S_A by Theorem 2.1. Q.E.D.

THEOREM 2.4. *Let $A = (S, I, M)$ be a quasi-regular automaton and H be a normal subgroup of $G(A)$. Then A/H is a quasi-regular automaton and $G(A)/H$ is isomorphic to $G(A/H)$.*

Proof. Since A is quasi-regular, H is semiregular on S_A. All orbits of a semiregular permutation group have the same length. Thus the restriction of H on S_A has $|S_A|/|H|$ orbits. Hence A/H has $|S_A|/|H|$ generators. Since A is quasi-regular, $|G(A)| = |S_A|$ and so the factor automaton A/H has $|G(A)|/|H|$ generators. Therefore the order of $G(A)/H$ is equal to the number of generators of A/H. By Proposition 2.6 and Theorem 2.1 we conclude that $G(A)/H$ is isomorphic to $G(A/H)$. Q.E.D.

In Theorem 2.4, we see that the result of Fleck [5] is extended naturally to quasi-regular automata. Ito [8] presented the following result:

Let $A = (S, I, M)$ be a strongly connected automaton such that $|S| = p|G(A)|$, where p is a prime number, and H be a normal subgroup of $G(A)$. Then if A is not a permutation automaton, $G(A)/H$ is isomorphic to $G(A/H)$.

In the rest of this section, we extend this result to cyclic automata.

THEOREM 2.5. *Let $A = (S, I, M)$ be a cyclic automaton such that $I_A \neq \varnothing$ and H*

be a normal subgroup of $G(A)$, and let $\bar{S}_A$ be the set of all generators of A/H. If $G(A/H)$ is transitive on $\bar{S}_A$, then A^* is a permutation automaton.

Proof. Let $\{B_i | i=1, \cdots, n\}$ be the set of all H-orbits. Suppose that $M(s, x)=M(t, x)$ for some $x\in\tilde{I}_A$ and some $s, t\in B_i$, where $B_i\subseteqq S_A$. Then there exists $h\in H$ such that $(s)h=t$. Since

$$(M(s, x))h=M((s)h, x)=M(t, x)=M(s, x),$$

$M(s, x)$ is fixed by h. By Theorem 2.1, H is semiregular on S_A and so we have $h=1_G$ (the identity of $G(A)$) and $s=t$. Thus, if $B_i\subseteqq S_A$ and $s, t\in B_i$ $(s\neq t)$, then $M(s, x)\neq M(t, x)$ for all $x\in\tilde{I}_A$. To each $x\in\tilde{I}_A$ we assign a transformation $\hat{x}$ on $\bar{S}$, where

$$\hat{x}: B_j\to \bar{M}(B_j, x), \qquad B_j\in\bar{S}.$$

Let $g\in G(A/H)$, $B_j\in\bar{S}_A$ and $x\in\tilde{I}_A$. Then $\bar{S}_A$ is fixed by g and $\hat{x}$ as a set and we have that $\bar{M}(B_j, x)g=\bar{M}((B_j)g, x)$, so that $(B_j)\hat{x}g=(B_j)g\hat{x}$. This means that the restriction of $\hat{x}$ to $\bar{S}_A$ commutes with all $g\in G(A/H)$ on $\bar{S}_A$. Since $G(A/H)$ is transitive on $\bar{S}_A$, the restriction of $\hat{x}$ to $\bar{S}_A$ is a permutation on $\bar{S}_A$ by Proposition 1.5. Therefore, if $B_i, B_j\in\bar{S}_A$ and $B_i\neq B_j$, then $(B_i)\hat{x}\neq(B_j)\hat{x}$. Thus we have that ξ_x: $s\to M(s, x)$, $s\in S_A$, is a permutation on S_A. Q.E.D.

COROLLARY 2.4 *Let $A=(S, I, M)$ be a strongly connected automaton and H be a normal subgroup of $G(A)$. If A is not a permutation automaton, then $G(A/H)$ is not a transitive permutation group.*

Proof. Since A is strongly connected, A satisfies the hypothesis of Theorem 2.5. We take a contraposition of Theorem 2.5. Q.E.D.

PROPOSITION 2.7. *Let $A=(S, I, M)$ be a cyclic automaton such that $|S_A|=p|G(A)|$ and $I_A\neq\varnothing$, where p is a prime number. If A^* is not a permutation automaton, then for any normal subgroup H of $G(A)$, $G(A)/H$ is isomorphic to $G(A/H)$.*

Proof. Let $\bar{S}_A$ be the set of all generators of A/H. By Theorem 2.1,

$$|\bar{S}_A|=|S_A|/|H|=p|G(A)|/|H|=p|G(A)/H|.$$

On the other hand, $|G(A/H)|$ divides $|\bar{S}_A|$ and $|G(A/H)|\geqq|G(A)/H|$ by Proposition 2.6. Hence $|G(A/H)|=|G(A)/H|$ or $p|G(A)/H|$. In the latter case, $G(A/H)$ is transitive on $\bar{S}_A$. This means that A^* is a permutation automaton by Theorem 2.5. Q.E.D.

The final proposition is a generalization of the above-mentioned result of Ito to cyclic automata.

Acknowledgments

The author would like to express his sincere thanks to Prof. K. Honda of St. Paul's University for his careful reading of the manuscript and for his many suggestions. The author is also particularly indebted to Prof. M. Ito of Kyoto Sangyo University and Dr. Y. Masunaga of Tohoku University for their valuable suggestions.

References

[1] BARNES, B.; On the group of automorphisms of strongly connected automata, *Math. System Theory*, **4** (1970), 289–294.

[2] BAVEL, Z.; Structure and transition-preserving functions of finite automata, *J. ACM*, **15** (1968), 135–158.

[3] DÖRFLER, W.; Halbgrouppen und Automaten, *Rend. Sem. Mat. Univ. Padova*, **50** (1973), 1–18.

[4] FLECK, A. C.; Isomorphism group of automata, *J. ACM*, **9** (1962) 469–476.

[5] FLECK, A. C.; On the automorphism group of an automaton, *J. ACM*, **12** (1965), 566–569.

[6] HARARY, F.; *Graph Theory*, Addison-Wesley, Reading, Mass., 1969.

[7] HUPPERT, B.; *Endliche Gruppen I*, Springer, Berlin–Heidelberg, 1967.

[8] ITO, M.; Strongly connected group-matrix type automata whose order are prime, *Trans. IECE Japan*, **59-E** (1976), 6–10.

[9] ITO, M.; A representation of strongly connected automata and its applications, *J. Comput. System Sci.*, **17** (1978), 65–80.

[10] MASUNAGA, Y., NOGUCHI, S. and OIZUMI, J.; A characterization of automata and a direct product decomposition, *J. Comput. System Sci.*, **13** (1976), 74–89.

[11] OEHMKE, R. H.; On the structures of an automaton and its input semigroup, *J. ACM*, **10** (1963), 521–525.

[12] PICKETT, H. E.; Note concerning the algebraic theory of automata, *J. ACM*, **14** (1967), 382–388.

[13] THIERRIN, G.; Permutation automata, *Math. System Theory*, **2** (1968) 83–90.

[14] TRAUTH, C. A., Jr.; Group-type automata, *J. ACM*, **13** (1966), 170–175.

[15] WEEG, G. P.; The structure of an automaton and its operation-preserving transformation group, *J. ACM*, **9** (1962), 345–349.

[16] WIELANDT, H.; *Finite Permutation Groups*, Academic Press, New York, 1964.

Department of Mathematics
Rikkyo University
Ikebukuro, Tokyo
Japan