Publ. Math. Debrecen
67/1-2 (2005), 115–130

On permutation groups generated by time-varying Mealy automata

By ADAM WORYNA (Gliwice)

Abstract. This paper is devoted to the groups generated by time-varying Mealy automata with a changing alphabet. It is proved that any finitely generated residually finite group can be realized as a group of some time-varying automaton with a finite set of states. Groups generated by various time-varying automata are considered.

1. Introduction

The theory of Mealy automata and groups generated by such automata have rapidly expanded in recent years. The groups of automata can be described as groups acting on the homogenous rooted tree. An extensive presentation of this theory is included in [3]. The idea of an automaton with a changing alphabet and a changing set of its internal states is a natural generalization. It allows to construct groups acting on level homogenous rooted trees which may be not homogeneous.

Let A be a given time-varying automaton. Any state q from the set Q_0 of its internal states defines a transformation f_q on the set of words over the changing alphabet. The (semi)group $\langle f_q \colon q \in Q_0 \rangle$ is called the (semi)group

Mathematics Subject Classification: 20E08, 68Q68.
Key words and phrases: time-varying automaton, changing alphabet, group generated by time-varying automaton.
The author thanks Professor V. I. Sushchanskii for his thorough advice.

generated by automaton A or the automaton (semi)group defined by A. If the changing alphabet is finite any such (semi)group is residually finite.

The groups of automata are difficult to study for many simple automata. There is no standard to studying such groups. A changing alphabet brings specific difficulties. For instance the word problem is solvable in the class of groups generated by finite state automata with a fixed alphabet (see for example [9]) but there are finitely generated residually finite groups with undecidable word problem (for example [2], [6]). Hence the word problem is undecidable in the class of groups generated by finite state time-varying automata.

Section 2 contains definitions of a time-varying Mealy automaton and functions defined by such automaton as well as the description of groups generated by these functions in terms of wreath product. In Section 3 we show that any finitely generated residually finite group can be realized as a group of some time-varying automaton with a finite set of states. In Section 4 we study the wreath product $\mathbb{Z} \wr \mathbb{Z}_n$ as a group of some 2-state automaton. Section 5 gives an example of a 2-state automaton group in which every finite group can be embedded.

2. Groups defined by time-varying Mealy automata

The paper [10] includes the primary notions about time-varying Mealy automata, different types of such automata as well as a description of functions defined by these automata was given. Recall some useful definitions and facts.

A changing alphabet is an infinite sequence $X = (X_t)_{t\in\mathbb{N}_0}$ of nonempty finite sets X_t (sets of letters). A word over a given changing alphabet X is a finite sequence $x_0x_1 \dots x_l$, where $x_i \in X_i$ for $i = 0, 1, \dots, l$. We denote by X^* the set of all words over X (including the empty word $\emptyset$).

Definition 1. A time-varying Mealy automaton over the changing alphabet X is a quadruple

$$A = (Q, X, \varphi, \psi),$$

where:

(1) $Q = (Q_t)_{t\in\mathbb{N}_0}$ (sequence of sets of internal states),

(2) $\varphi = (\varphi_t)_{t\in\mathbb{N}_0}$, $\varphi_t : Q_t \times X_t \to Q_{t+1}$ (sequence of transition functions),
(3) $\psi = (\psi_t)_{t\in\mathbb{N}_0}$, $\psi_t : Q_t \times X_t \to X_t$ (sequence of output functions).

An automaton A with a fixed initial state $q \in Q_0$ is called the initial automaton and denoted by A_q. If A is a given automaton then for every state $q \in Q_0$ the initial automaton A_q defines a function $f_q : X^* \to X^*$ as follows:

$$f_q(x_0x_1 \dots x_l) = \psi_0(q_0, x_0)\psi_1(q_1, x_1) \dots \psi_l(q_l, x_l), \tag{1}$$

where $q_0 = q$ and $q_i = \varphi_{i-1}(q_{i-1}, x_{i-1})$ for $i = 1, \dots, l$. The function f_q is called the automaton function defined by the initial automaton A_q.

An automaton A is called permutational if the mapping of the set X_t defined as follows

$$x \mapsto \psi_t(q, x)$$

is permutation for any $t \in \mathbb{N}_0$ and $q \in Q_t$. If A is a permutational automaton then the functions f_q are permutations on X^* for all $q \in Q_0$.

Let $A_{q_0} = (Q, X, \varphi^A, \psi^A)$, $B_{r_0} = (R, X, \varphi^B, \psi^B)$ be initial automata over a common alphabet X and f_{q_0}, h_{r_0} be automaton functions defined by the above automata. Then the superposition $h_{r_0} \circ f_{q_0}$ is an automaton function defined by the automaton $C_{s_0} = (S, X, \varphi, \psi)$ for which:

$$S_t = Q_t \times R_t, \ \ s_0 = (q_0, r_0),$$

$$\varphi_t((q, r), x) = \left(\varphi_t^A(q, x), \varphi_t^B\left(r, \psi_t^A(q, x)\right)\right),$$

$$\psi_t((q, r), x) = \psi_t^B\left(r, \psi_t^A(q, x)\right).$$

The automaton C_{s_0} is called the product of the automata A_{q_0}, B_{r_0}. If A_{q_0} is a permutational automaton then f_{q_0} is a permutation. The inverse function $f_{q_0}^{-1}$ is also an automaton permutation defined by the automaton $D_{q_0} = (Q, X, \varphi, \psi)$ for which

$$\varphi_t(q, x) = \varphi_t^A(q, x'), \quad \psi_t(q, x) = x',$$

where the letter x' is defined by the equality $\psi_t^A(s, x') = x$. The automaton D_{q_0} is called the inverse to the automaton A_{q_0}.

We consider the set $\mathrm{SA}(X)$ of all automaton functions defined by time-varying automata over a given changing alphabet X. Since the identity

function id_{X^*} is an automaton transformation and the superposition of automaton functions is also of this type, the set $\mathrm{SA}(X)$ forms a monoid with id_{X^*} as the neutral element. The construction of the product of automata and the inverse automaton allows to specify the following submonoids in $\mathrm{SA}(X)$ (see [10]):

(1) automaton functions defined by automata with a constant sequence of its sets of states,

(2) automaton functions defined by automata with equi-bounded sets of states,

(3) the set $\mathrm{GA}(X)$ of automaton functions defined by permutational automata.

Let $A = (Q, X, \varphi, \psi)$ be a time-varying automaton. If there exist $T > 0$ and $\tau \geq 0$ such that

$$Q_{t+T} = Q_t,\ X_{t+T} = X_t, \quad \varphi_{t+T} = \varphi_t, \quad \psi_{t+T} = \psi_t$$

for every $t \geq \tau$ then A is called a (T, τ)-periodic automaton and the alphabet X – a (T, τ)-periodic alphabet.

Let $v \in X^*$ be a word of the length $n = |v|$ and f be an automaton function defined by some initial automaton over X. Then we can define a function $f_v : X_{(n)} \to X_{(n)}$ by equality (see [10])

$$f(vu) = f(v)f_v(u),$$

where $X_{(n)}$ denotes the set of all finite sequences of letters in which the i-th letter belongs to X_{n+i-1} for any $i = 1, 2, \ldots$. The function f_v is called the v-remainder of f.

Let X be a given changing alphabet. We consider the set $\mathrm{PSA}(X)$ of automaton functions defined by all periodic automata over X as well as the set $\mathrm{FRSA}(X)$ of automaton functions with a finite set of remainders. The above sets are nonempty only if X is periodic (see [10], Theorem 4.3).

Let X be a (T, τ)-periodic alphabet. If $f, h \in \mathrm{PSA}(X)$, where f is defined by some (T_1, τ_1)-periodic automaton and h is defined by some (T_2, τ_2)-periodic automaton then the product of these automata is a (T', τ')-periodic automaton for $T' = \mathrm{lcm}(T_1, T_2)$, $\tau' = \max(\tau_1, \tau_2)$. Of course the identity function $\mathrm{id}_{X^*} \in \mathrm{PSA}(X)$.

For the set $\mathrm{FRSA}(X)$ we have: $\mathrm{id}_{X^*} \in \mathrm{FRSA}(X)$ since all remainders of id_{X^*} are defined by words of length at most $T + \tau$. Moreover, for any v-remainder of $f \circ h$ we have $(f \circ h)_v = f_{h(v)} \circ h_v$. Hence, if R_f and R_h are sets of remainders then $|R_{f \circ h}| \leq |R_f| \cdot |R_h|$.

Thus, if X is a periodic alphabet then $\mathrm{PSA}(X)$ and $\mathrm{FRSA}(X)$ form submonoids of $\mathrm{SA}(X)$. It is worth seeing that $\mathrm{FRSA}(X)$ is a proper submonoid of $\mathrm{PSA}(X)$ (see [10], Example 4.1).

The set $\mathrm{GA}(X)$ is the group of invertible elements of $\mathrm{SA}(X)$. The group $\mathrm{GA}(X)$ may be characterized as a certain wreath product.

Definition 2. The wreath product over an infinite sequence (G_0, M_0), $(G_0, M_0), \ldots$ of permutation groups is the group of all permutations g of the set $M = \prod_{i=0}^{\infty} M_i$, satisfying the following conditions

(i) if $g(x_0, x_1, \ldots) = y_0, y_1, \ldots$ then y_i depends only on $i+1$ first coordinates $x_0, x_1, \ldots, x_i$ for any $i = 0, 1, \ldots,$

(ii) if we fix $x_0^0, \ldots, x_{i-1}^0$ then the transformation

$$g_{x_0^0, \ldots, x_{i-1}^0} : x_i \mapsto y_i$$

induced by g is a permutation from the group G_i.

This wreath product we denote by

$$\wr_{i=0}^{\infty}(G_i, M_i) = \wr_{i=0}^{\infty} G_i.$$

Proposition 1. *The set* $\mathrm{GA}(X)$ *of all automaton permutations defined by permutational time-varying automata over the changing alphabet* X *forms (under superposition) a group isomorphic to the wreath product over the infinite sequence of symmetric groups on sets* $X_0, X_1, X_2, \ldots$

$$\mathrm{GA}(X) \cong \wr_{i=0}^{\infty} S(X_i).$$

Proof. For any $g \in \wr_{i=0}^{\infty} S(X_i)$ we consider a function $f_g : X^* \to X^*$ defined as:

$$f_g(x_0 x_1 \ldots x_l) = g_{\emptyset}(x_0) g_{x_0}(x_1) g_{x_0, x_1}(x_2) \ldots g_{x_0, x_1, \ldots, x_{l-1}}(x_l)$$

for an arbitrary word $x_0 x_1 \ldots x_l$, where $g_{x_0, \ldots, x_{i-1}} \in S(X_i)$ are transformations induced by g according to the above definition of the wreath product. The map $g \mapsto f_g$ defines the required isomorphism. □

3. Representation of groups by means of time-varying automata

For every permutational automaton A we construct the group

$$G(A) = \langle f_q \colon q \in Q_0 \rangle.$$

The group $G(A)$ is called the group generated by automaton A. It is a residually finite group for every automaton A. It turns out that groups of this form include the class of finitely generated residually finite groups.

Theorem 1. *For any n-generated residually finite group G there is a time-varying automaton A with an n-element set of states and such that*

$$G \cong G(A).$$

Proof. Since G is countable, its elements can be put in sequence

$$g_{-1} = 1, g_0, g_1, \dots .$$

For the element g_i $(i \geq 0)$ there is a normal subgroup $N_i \lhd G$ of finite index such that $g_i \notin N_i$. The map

$$g \mapsto (gN_i)_{i \in \mathbb{N}_0}$$

defines the embedding of G into the cartesian product $\prod_{i=0}^{\infty} G/N_i$. For any $i = 0, 1, \dots$ since $|G/N_i| < \infty$, there is a finite set X_i such that G/N_i can be embedded into the symmetric group $S(X_i)$. Hence, the group $\prod_{i=0}^{\infty} G/N_i$ and consequently the group G can be embedded into the cartesian product $\prod_{i=0}^{\infty} S(X_i)$ of symmetric groups. Let

$$K = \langle \kappa_0, \kappa_1, \dots, \kappa_{n-1} \rangle$$

be the subgroup of $\prod_{i=0}^{\infty} S(X_i)$ isomorphic to G. We construct an automaton $A = (Q, X, \varphi, \psi)$ in the following way:

(1) $X = (X_t)_{t \in \mathbb{N}_0}$,

(2) $Q_t = \{\kappa_0, \kappa_1, \dots, \kappa_{n-1}\}$,

(3) $\varphi_t(\kappa_i, x) = \kappa_i$, $i = 0, 1, \dots, n-1$,

(4) $\psi_t(\kappa_i, x) = \kappa_i^{(t)}(x)$, $i = 0, 1, \dots, n-1$,

where $\kappa_i^{(t)}$ is the permutation at the $(t+1)$-th position in κ_i. The automaton A is permutational by definition.

Let f_{κ_i} be the generator of $G(A)$ defined by the initial automaton A_{κ_i}. Then for any word $x_0x_1\dots x_l \in X^*$ we have according to (1):

$$\begin{aligned} f_{\kappa_i}(x_0x_1\dots x_l) &= \psi_0(\kappa_i, x_0)\psi_1(\kappa_i, x_1)\dots\psi_l(\kappa_i, x_l) \\ &= \kappa_i^{(0)}(x_0)\kappa_i^{(1)}(x_1)\dots\kappa_i^{(l)}(x_l). \end{aligned}$$

For every $\kappa \in K$ we define a function $f_\kappa : X^* \to X^*$ as follows

$$f_\kappa(x_0x_1\dots x_l) = \kappa^{(0)}(x_0)\kappa^{(1)}(x_1)\dots\kappa^{(l)}(x_l).$$

Then for any $\kappa, \kappa' \in K$ the equality $f_{\kappa\circ\kappa'} = f_\kappa \circ f_{\kappa'}$ holds and $f_\kappa \in G(A)$ according to definition of K. Furthermore if $\kappa, \kappa' \in K$ are different then $\kappa^{(t)}(x) \neq \kappa'^{(t)}(x)$ for some $t \in \mathbb{N}_0$, $x \in X_t$ and $f_\kappa \neq f_{\kappa'}$. Hence the map $\kappa \mapsto f_\kappa$ defines the required isomorphism. □

We denote by $+_k$ and $-_k$ the respective arithmetical operations (mod k). Let $n > 1$ be a given integer and $X = (X_t)_{t\in\mathbb{N}_0}$ be a changing alphabet of the form $X_t = \{0, 1, \dots, t+n-1\}$. If $u = z_0z_1\dots z_l$ is any sequence of letters such that $z_i \in X_{i+\tau}$ for some $\tau \in \mathbb{N}_0$, $i = 0, 1, \dots, l$ then for every integer m we denote by $u \oplus m$ the following sequence of letters

$$(z_0 +_{\tau+n} m)(z_1 +_{\tau+n+1} m)\dots(z_l +_{\tau+n+l} m).$$

Example. Let $A = (Q, X, \psi, \varphi)$ be an automaton for which:

(1) $X_t = \{0, 1, \dots, t+1\}$,

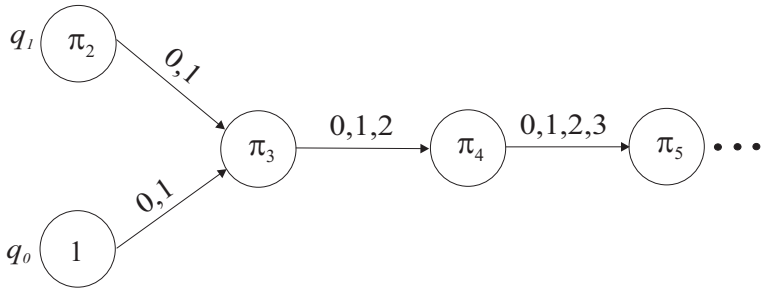
(2) $Q_0 = \{q_0, q_1\}$, $Q_t = \{q_1\}$ for $t \in \mathbb{N}$,

(3) $\varphi_t(q, x) = q_1$ for $t \in \mathbb{N}_0$, $q \in Q_t$,

(4) $\psi_0(q_0, x) = x$ for $x \in X_0$,

$\psi_t(q_1, x) = x +_{t+2} 1$.

The above automaton is presented in the picture (1 and π_i constitute the neutral element and the cycle $(0, 1, \dots, i+1)$ of the symmetric group S_{i+2} for any $i = 0, 1, \dots$).



We denote the generators f_{q_0} and f_{q_1} of $G(A)$ by a and b respectively. The generators transform a word $\epsilon u \in X^*$ with $\epsilon \in \{0,1\}$ in the following way $a(\epsilon u) = \epsilon(u \oplus 1)$, $b(\epsilon u) = (\epsilon \oplus 1)(u \oplus 1)$ and both a and b have infinite order. Furthermore, $ab(\epsilon u) = (\epsilon \oplus 1)(u \oplus 2) = ba(\epsilon u)$. Let $c = a^{-1}b$. We easily check that c^2 is the identity function. Hence every element of $G(A)$ is of the form $c^r a^s$, $r \in \{0,1\}$, $s \in \mathbb{Z}$. We have $c^r a^s(\epsilon u) = (\epsilon \oplus r)(u \oplus s)$ and the mapping $c^r a^s \mapsto (r,s)$ defines an isomorphism $G(A) \cong \mathbb{Z}_2 \times \mathbb{Z}$.

4. The wreath product $\mathbb{Z} \wr \mathbb{Z}_n$ as a 2-state automaton group

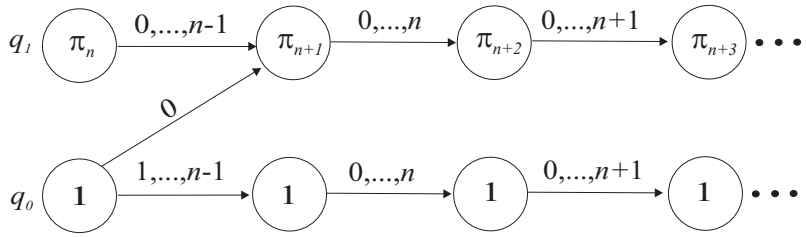
Let $n > 1$ be a given number and $A = (Q, X, \psi, \varphi)$ be an automaton in which:

(1) $X_t = \{0, 1, \ldots, n + t - 1\}$,

(2) $Q_t = \{q_0, q_1\}$,

(3) $\varphi_0(q_0, 0) = q_1$, $\varphi_t(q_0, x) = q_0$ for $x \neq 0$,
$\varphi_t(q_1, x) = q_1$,

(4) $\psi_t(q_0, x) = x$,
$\psi_t(q_1, x) = x +_{t+n} 1$.



We denote the generators f_{q_0}, f_{q_1} of $G(A)$ by α and β respectively. For a word $\epsilon u \in X^*$ with $\epsilon \in \{0, 1, \ldots, n-1\}$ we have:

$$\alpha(0u) = 0(u \oplus 1), \ \alpha(\epsilon u) = \epsilon u \quad \text{for } \epsilon = 1, \ldots, n-1,$$

$$\beta(\epsilon u) = (\epsilon \oplus 1)(u \oplus 1).$$

In particular both α and β have infinite order.

Lemma 1. *If an element γ of $G(A)$ is represented by a word in α, β of the form*

$$\alpha^{r_1}\beta^{s_1}\alpha^{r_2}\beta^{s_2}\ldots\alpha^{r_k}\beta^{s_k}, \tag{2}$$

then we have

$$\gamma(\epsilon u) = (\epsilon \oplus s)(u \oplus (s + r(\epsilon))), \tag{3}$$

where $s = \sum_{i=1}^{k} s_i$, $r(\epsilon) = \sum_i r_i$, where we sum over all i for which $n \mid s_i + \cdots + s_k + \epsilon$ (if there are no suitable indexes, we assume $r(\epsilon) = 0$).

Proof. By induction on the length of (2). □

Thus the word (2) defines a unique $(n+1)$-tuple of integers

$$(s, r(0), r(1), \ldots, r(n-1)). \tag{4}$$

Using Lemma 1 we obtain the following algorithms solving the word and the conjugacy problem in $G(A)$:

Let w, w' be words in α, β. We calculate the $(n+1)$-tuples

$$(s, r(0), r(1), \ldots, r(n-1)),$$

$$(s', r'(0), r'(1), \ldots, r'(n-1))$$

defined by w and w' respectively. Then

$$w = w' \Leftrightarrow n \mid s - s' \quad \text{and} \quad s' + r'(i) = s + r(i) \tag{5}$$

for $i = 0, 1, \ldots, n-1$. For the conjugacy problem we have w, w' are conjugate $\Leftrightarrow n \mid s - s'$ and there is $\xi \in \{0, 1, \ldots, n-1\}$ such that

$$\sum_{i=0}^{\eta-1} \left(s' + r'(is +_n j)\right) = \sum_{i=0}^{\eta-1} (s + r(is +_n j +_n \xi))$$

for $j = 0, 1, \ldots, \gcd(n, s) - 1$, where $\eta = \frac{n}{\gcd(n,s)}$.

The wreath product $\mathbb{Z} \wr \mathbb{Z}_n$ is a semi-direct product $\prod_{\mathbb{Z}_n} \mathbb{Z} \rtimes \mathbb{Z}_n$ with the action of $\mathbb{Z}_n$ on $\mathbb{Z}^n$ by a cyclic shift. In a sense this group is dual to the wreath product $\mathbb{Z}_n \wr \mathbb{Z}$ which is known as the lamplighter group (see [4]). We mention some properties of the group $\mathbb{Z} \wr \mathbb{Z}_n$. The center of $\mathbb{Z} \wr \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}$ and its quotient group is isomorphic to the semi-direct product $\mathbb{Z}^{n-1} \rtimes \mathbb{Z}_n$, where $\mathbb{Z}_n$ acts on $\mathbb{Z}^{n-1}$ by linear transformations as follows

$$z \longmapsto \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -1 \\ 1 & 0 & \ldots & 0 & 0 & -1 \\ 0 & 1 & \ldots & 0 & 0 & -1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & -1 \\ 0 & 0 & \ldots & 0 & 1 & -1 \end{pmatrix}^i \cdot z, \quad z \in \mathbb{Z}^{n-1},$$

for every $i \in \mathbb{Z}_n$. The wreath product $\mathbb{Z} \wr \mathbb{Z}_n$ is a metabelian, nonnilpotent group. The commutator subgroup $(\mathbb{Z} \wr \mathbb{Z}_n)'$ is isomorphic to the cartesian product $\mathbb{Z}^{n-1}$. The abelianization of $\mathbb{Z} \wr \mathbb{Z}_n$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_n$.

Theorem 2. *Let $G = G(A)$ be the group generated by the automaton A. Then*

(i) $G \cong \mathbb{Z} \wr \mathbb{Z}_n$,

(ii) *the stabilizer $St_G(k) \cong \mathbb{Z}^n$ for any $k \geq 1$,*

(iii) *the quotient group $G/St_G(1)$ is a cyclic group of order n generated by $\beta St_G(1)$. For $k > 1$ the quotient group $G/St_G(k)$ is isomorphic to the wreath product $\mathbb{Z}_\tau \wr \mathbb{Z}_n$, where $\tau = \operatorname{lcm}(n+1, \ldots, n+k-1)$,*

(iv) *for any $v \in X^*$ the vertex stabilizer $St_G(v) \cong \mathbb{Z}^n$. For the orbit $\operatorname{Orb}_G(v) = \{\gamma(v) : \gamma \in G\}$ we have*

$$|\operatorname{Orb}_G(v)| = \begin{cases} n & \text{if } |v| = 1 \\ n \cdot \operatorname{lcm}(n+1, \ldots, n+|v|-1) & \text{if } |v| > 1 \end{cases}$$

The group G acts transitively on the set $X^{(l)}$ of words of length l if and only if $l \leq 3$ in case n is odd and $l \leq 4$ in case n is even. Two words $\epsilon u, \epsilon' u' \in X^*$ belong to the same orbit if and only if $u' = u \oplus r$ for some integer r.

PROOF. (i) For an arbitrary $(n+1)$-tuple (4) there is a word in α, β which defines it. Indeed, an example of the required word is

$$w_{r_0,r_1,\ldots,r_{n-1},s} = \alpha^{r_0-s}\beta\alpha^{r_1-s}\beta\ldots\alpha^{r_{n-2}-s}\beta\alpha^{r_{n-1}-s}\beta^{s-n+1}, \tag{6}$$

where $r_i = s + r(i -_n s)$. Hence any element of G is represented by some word of the form (6). Furthermore, from the solution (5) any element of G is represented by a unique such word with $r_i \in \mathbb{Z}$ $(i = 0, 1, \ldots, n-1)$ and $s \in \{0, 1, \ldots, n-1\}$. From Lemma 1 the multiplication formula for words (6) is described by the rules

$$w_{r_0,r_1,\ldots,r_{n-1},s} \cdot w_{r'_0,\, r'_1,\ldots,r'_{n-1},s'} = w_{r''_0,r''_1,\ldots,r''_{n-1},s''},$$

where $s'' = s +_n s'$, $r''_i = r_i + r'_{i-s}$ for $i = 0, 1, \ldots, n-1$. Hence the map

$$w_{r_0,r_1,\ldots,r_{n-1},s} \mapsto ((r_0, r_1, \ldots, r_{n-1}), s) \tag{7}$$

is an isomorphism of G and $\mathbb{Z} \wr \mathbb{Z}_n$.

(ii) If γ is an element of G defined by the word (6) then from Lemma 1 $\gamma \in St_G(1) \Leftrightarrow s = 0$. Similarly, for $k > 1$

$$\gamma \in St_G(k) \Leftrightarrow s = 0 \text{ and } \tau \mid r(i) \quad \text{for } i = 0, 1, \ldots, n-1.$$

Now, the map $\phi\colon St_G(k) \to \mathbb{Z}^n$ defined by the rule

$$\phi(w_{r_0,r_1,\ldots,r_{n-1},0}) = \left(r_0/\tau', r_1/\tau', \ldots, r_{n-1}/\tau'\right)$$

is the required isomorphism, where $\tau' = \begin{cases} 1 & \text{if } k = 1 \\ \tau & \text{if } k > 1. \end{cases}$

(iii) The map $\phi_1\colon G \to \mathbb{Z}_n$ defined by

$$\phi_1(w_{r_0,r_1,\ldots,r_{n-1},s}) = s$$

is an epimorphism with $\ker\phi_1 = St_G(1)$. Similarly for $k > 1$, the map $\phi_k\colon G \to \mathbb{Z}_\tau \wr \mathbb{Z}_n$ defined by

$$\phi_k(w_{r_0,r_1,\ldots,r_{n-1},s}) = ((\overline{r}_0, \overline{r}_1, \ldots, \overline{r}_{n-1}), s)$$

is an epimorphism with $\ker\phi_k = St_G(k)$, where $\overline{r}_i$ is the remainder of the division of r_i by τ.

(iv) It results from Lemma 1 and (iii). □

Corollary. *The growth function $\zeta_G(m)$ of G is of order m^n.*

Remark. A slight change of the alphabet X in the above automaton gives a construction of the wreath product $\mathbb{Z} \wr \mathbb{Z}_n$ as a group acting spherically transitively.

5. The universal embedding by a 2-state automaton group

Let $A = (Q, X, \varphi, \psi)$ be an automaton in which:

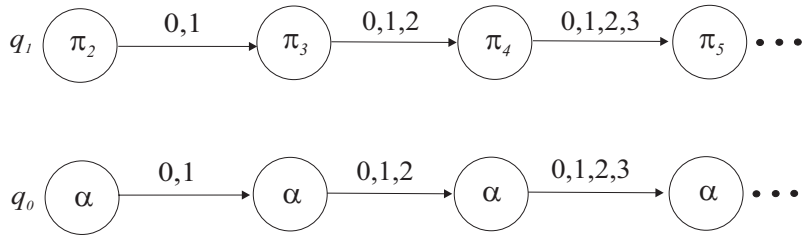
(1) $X_t = \{0, 1, \dots, t+1\}$,

(2) $Q_t = \{q_0, q_1\}$,

(3) $\varphi_t(q_0, x) = q_0$,
$\varphi_t(q_1, x) = q_1$,

(4) $\psi_t(q_0, 0) = 1$, $\psi_t(q_0, 1) = 0$, $\psi_t(q_0, x) = x$ for $x \neq 0, 1$,
$\psi_t(q_1, x) = x +_{t+2} 1$.

The above automaton is presented in the picture (α is the cycle $(0, 1)$ of the symmetric group S_{i+2} for any $i = 0, 1, \dots$).



Let $\alpha_n = (1, 2)$, $\beta_n = (1, 2, \dots, n+1)$ be cycles in the symmetric group S_{n+1} for $n = 1, 2, \dots$ and let $K = \langle \alpha, \beta \rangle$ be the group generated by two sequences of permutations

$$\alpha = (\alpha_1, \alpha_2, \dots), \quad \beta = (\beta_1, \beta_2, \dots)$$

of the infinite Cartesian product $\prod_{i=2}^{\infty} S_i$.

Theorem 3. *Let $G = G(A)$ be the group generated by the automaton A. Then*

(i) $G \cong K$,

(ii) *every finite group can be embedded into* G,

(iii) *the action of* G *on* X^* *is spherically transitive,*

(iv) *the group* G *contains no free subgroups of rank* > 1. *The semigroup generated by* f_{q_0}, f_{q_1} *is free,*

(v) *the commutator subgroup* G' *is a locally finite group and the abelianization* G/G' *is isomorphic to* $\mathbb{Z}_2 \times \mathbb{Z}$.

PROOF. (i) For any word $x_0x_1 \dots x_l \in X^*$ if

$$f_{q_0}(x_0x_1 \dots x_l) = y_0y_1 \dots y_l,$$

$$f_{q_1}(x_0x_1 \dots x_l) = z_0z_1 \dots z_l$$

then

$$y_i = \alpha_{i+1}(x_i + 1) - 1, \quad z_i = \beta_{i+1}(x_i + 1) - 1 \tag{8}$$

for $i = 0, 1, \dots, l$. Hence, the image of x_i depends on x_i only. As in the proof of Theorem 1 the map $\alpha \mapsto f_{q_0}$, $\beta \mapsto f_{q_1}$ induces the required isomorphism.

(ii) It is enough to prove that the direct product $\coprod_{i=2}^{\infty} A_i$ of alternating groups is a subgroup of K. To this end we show that $N_i \lhd K$ for $i = 0, 1, \dots$, where

$$N_i = \underbrace{\{1\} \times \{1\} \times \dots \{1\}}_{i} \times A_{i+2} \times \{1\} \times \{1\} \times \dots .$$

The case $i = 0$ is obvious. Next, $N_1 = \langle\gamma\rangle \lhd K$, where

$$\gamma = \left(\alpha\beta^2\alpha\beta^{-2}\right)^2 = (1, (1, 2, 3), 1, 1, \dots) \in K.$$

For a given $n > 1$ suppose that $N_i \lhd K$ for all $i < n$. For the element

$$\delta = \left(\alpha\beta^{n+1}\alpha\beta^{-n-1}\right)^2$$

we have $\delta = (\delta_1, \delta_2, \dots, \delta_n, (1, 2, n + 2), 1, 1, \dots)$, where all δ_i are even. It follows from the above assumption that elements $\kappa_i = (\underbrace{1, \dots, 1}_{i-1}, \delta_i^{-1}, 1, 1, \dots)$

for $i = 1, \dots, n$ and consequently the product

$$\kappa = \delta \cdot \kappa_1 \cdot \dots \cdot \kappa_n = (\underbrace{1, \dots, 1}_{n}, (1, 2, n+2), 1, 1, \dots)$$

belong to K. Hence $N_n = \langle \kappa^K \rangle \lhd K$.

(iii) Since the isomorphism $K \cong G$ is induced by the mapping $\alpha \mapsto f_{q_0}$, $\beta \mapsto f_{q_1}$, the spherical transitiveness results from (8) as well as from the inclusion $\coprod_{i=2}^{\infty} A_i < K$.

(iv) It is enough to show that K does not contain a free group F_2. Since α has order 2, any element of K is defined by some word in α, β of the form

$$\alpha^{\epsilon} \beta^{s_1} \alpha \beta^{s_2} \dots \alpha \beta^{s_k}, \quad \epsilon \in \{0, 1\}. \tag{9}$$

Let $s = \sum_{i=1}^{k} s_i$ be the sum of all exponents of β. First we prove the following

Lemma 2. *The element γ from K represented by* (9) *has finite order if and only if $s = 0$.*

Proof of Lemma. Let $m = \sum_{i=1}^{k} |s_i|$. For any n, if $s = 0$ and

$$m + 2 < i < n - m - 2,$$

the permutation of γ at the n-th position maps i into $\beta_n^s(i) = i$. Hence γ has order less or equal to $\exp(S_{2m+4})$. From the other hand for any j, if

$$jm + 2 < i < n - jm - 2,$$

then the j-th power of permutation at the n-th position in γ maps i in $\beta_n^{js}(i)$. If $s \neq 0$ and $n > 2jm + 5$ then $\beta_n^{js}(i) \neq i$. Thus the j-th power of γ is not the neutral element. □

Now, let $\gamma, \gamma' \in K$ and s, s' be sums of exponents of β in some words in α, β representing γ and γ' respectively. From Lemma 2, if $s = 0$ or $s' = 0$ then γ or γ' has finite order. Similarly, if $s, s' \neq 0$, the element $\gamma^{s'} \gamma'^{-s}$ has finite order. Hence, the group generated by γ, γ' is not isomorphic to F_2.

Let γ and γ' be represented by two different words in α, β with non-negative exponents and with the above defined sums s, s'. We may assume that the word representing γ ends with α, while the word representing γ'

ends with β. If $s \neq s'$ then $\gamma \neq \gamma'$, since $\gamma\gamma'^{-1}$ has infinite order by Lemma 2. If $s' = s$ then for a suitably large n, the permutations of γ and γ' at the n-th position map the number 2 to l and $s+2$ respectively, where $l \leq s+1$. Thus $\gamma \neq \gamma'$.

(v) Let $K_\alpha = \langle \alpha^K \rangle$ and $K_\beta = \langle \beta^K \rangle$ be groups generated by conjugacy classes of generators of K. The group K_α consists of all words (9) with $s = 0$ well, torsion elements of K. Indeed, any such word can be expressed as

$$\alpha^\epsilon \beta^{s_1} \alpha \beta^{-s_1} \cdot \beta^{s_1+s_2} \alpha \beta^{-s_1-s_2} \cdot \ldots \cdot \beta^{s_1+\cdots+s_{k-1}} \alpha \beta^{-s_1-\cdots-s_{k-1}}.$$

Since $\alpha\beta K_\alpha = \beta K_\alpha$, the quotient group K/K_α is represented by β^i, $i \in \mathbb{Z}$. Thus the isomorphism $K/K_\alpha \cong \mathbb{Z}$ holds.

If $\gamma \in K_\beta$ then there is a word in α, β representing γ in which α occurs an even number of times. We show as above that any such word represents an element from K_β. All permutations of γ at even positions are even. Consequently $\alpha \notin K_\beta$ and K_β consist exactly of those words in which α occurs an even number of times. Hence $K/K_\beta \cong \mathbb{Z}_2$.

From the isomorphisms $K/K_\alpha \cong \mathbb{Z}$, $K/K_\beta \cong \mathbb{Z}_2$ we obtain the inclusion $K' \subseteq K_\alpha \cap K_\beta$. On the other hand, if $\gamma \in K_\alpha \cap K_\beta$ then $\gamma K' = K'$. Thus $K' = K_\alpha \cap K_\beta$. In other words, K' consists of all torsion elements of K such that permutations at all its positions are even. In particular $\coprod_{i=2}^{\infty} A_i \lhd K'$. From above, K/K' is represented by $\alpha^\epsilon \beta^i$, $\epsilon \in \{0,1\}$, $i \in \mathbb{Z}$ and $G/G' \cong K/K' \cong \mathbb{Z}_2 \times \mathbb{Z}$.

The group K_α is locally finite. Indeed, let $F = \langle \gamma_1, \ldots, \gamma_n \rangle$ be a finitely generated subgroup of K_α. The element

$$\gamma_i = \left(\gamma_1^{(i)}, \gamma_2^{(i)}, \ldots \right)$$

is a Cartesian product of a finite number r_i of infinite sequences of transpositions. Any permutation $\gamma_j^{(i)}$ of the above sequence changes at most $2r_i$ elements. Thus, if $r = 2\sum_{i=1}^{n} r_i$ then there are sets $Z_1, Z_2, \ldots$ with at most r elements each and such that for any γ from F, the permutation at the i-th position changes only elements from Z_i. Hence, F is isomorphic to some subgroup of the infinite Cartesian product of the symmetric groups S_r. Since the last group is locally finite, the group F must be finite.

Now, using the sequence

$$\coprod_{i=2}^{\infty} A_i \lhd K' \lhd K_\alpha$$

we obtain locally finiteness of $K' \cong G'$. □

References

[1] J. D. Dixon and B. Mortimer, Permutation Groups, *Springer*, *New York*, 1996, 346.

[2] V. H. Dyson, A family of groups with nice word problems, *J. Australian Math. Soc.* **17** (1974), 414–425.

[3] R. I. Grigorchuk, V. V. Nekrashevich and V. I. Sushchanskii, Automata, Dynamical Systems and Groups, *Proseedings of Steklov Institute of Mathematics* **231** (2000), 128–203.

[4] R. Grigorchuk and A. Zuk, The Lamplighter Group as a Group Generated by a 2-state Automaton and its spectrum, *Geometriae Dedicata* **87** (2001), 209–244.

[5] P. de la Harpe, Topics in Geometric Group Theory, *The University of Chicago Press*, *Chicago and London*, 2000, 310.

[6] S. Meskin, A finitely generated residually finite groups with an usolvable word problem, *Proc. Amer. Math. Soc.* **43** (1974), 8–10.

[7] B. Mikolajczak, Algebraic and structural automata theory, Translated from the Polish Annals of Discrete Mathematics, 44, *North-Holland Publishing Co.*, *Amsterdam*, 1991, 402.

[8] V. I. Sushchanskii, Group of Automatic Permutations, *Dopovidi NAN Ukrainy*, 1998 N 6, 47–51 (in *Ukrainian*).

[9] V. I. Sushchanskii, Group of Finite Automatic Permutations, *Dopovidi NAN Ukrainy*, 1999 N 2, 48–52 (in *Ukrainian*).

[10] A. Woryna, On transformations given by time-varying Mealy automata, *Zesz. Nauk. Pol. Sl., Seria: Automatyka* **138**, Nr. 1581 (2003), 201–215 (in *Polish*).

ADAM WORYNA
INSTITUTE OF MATHEMATICS
SILESIAN TECHNICAL UNIVERSITY
UL. KASZUBSKA 23, 44-101 GLIWICE
POLAND

E-mail: Adam.Woryna@polsl.pl

(Received October 27, 2003; revised March 9, 2004)