Algebra and Discrete Mathematics RESEARCH ARTICLE
Number 3. **(2008).** pp. 98 – 111

The generalized dihedral groups $Dih(\mathbb{Z}^n)$ as groups generated by time-varying automata

Adam Woryna

Communicated by V. I. Sushchansky

Abstract. Let $\mathbb{Z}^n$ be a cubical lattice in the Euclidean space $\mathbb{R}^n$. The generalized dihedral group $Dih(\mathbb{Z}^n)$ is a topologically discrete group of isometries of $\mathbb{Z}^n$ generated by translations and reflections in all points from $\mathbb{Z}^n$. We study this group as a group generated by a $(2n+2)$-state time-varying automaton over the changing alphabet. The corresponding action on the set of words is described.

Introduction

For any abelian group A the generalized dihedral group $Dih(A)$ is defined as a semidirect product of A and $\mathbb{Z}_2$ with $\mathbb{Z}_2$ acting on A by inverting elements, i.e.

$$Dih(A) = A \rtimes_{\phi} \mathbb{Z}_2,$$

with $\phi(0)$ the identity and $\phi(1)$ inversion. If A is cyclic, then $Dih(A)$ is called a dihedral group. The subgroup of $Dih(A)$ of elements $(a, 0)$ is a normal subgroup of index 2, isomorphic to A, while the elements $(a, 1)$ are all their own inverse. This property in fact characterizes generalized dihedral groups, in the sense that if a group G has a subgroup N of index 2 such that all elements of the complement $G - N$ are of order two, then N is abelian and $G \simeq Dih(N)$.

Let $\mathbb{Z}^n$ be a free abelian group of rank n. We may look on it as a cubical lattice in the Euclidean space $\mathbb{R}^n$. The corresponding generalized

2000 Mathematics Subject Classification: *20E22, 20E08, 20F65.*

Key words and phrases: *generalized dihedral groups, time-varying automaton, group generated by time-varying automaton.*

dihedral group $Dih(\mathbb{Z}^n)$ is a topologically discrete group of isometries of $\mathbb{Z}^n$ generated by translations and reflections in all points from $\mathbb{Z}^n$. In case $n = 1$ this is the isometry group of $\mathbb{Z}$, which is called the infinite dihedral group and is isomorphic to the free product of two cyclic groups of order two. For $n = 2$ it is a type of the so-called wallpaper group - the mathematical concept to classify repetitive designs on two-dimensional surfaces. For $n = 3$ this is the so-called space group of a crystal. Our new look on the group $Dih(\mathbb{Z}^n)$ is via the time-varying automata theory. Namely, we realize this group as a group defined by a $(2n+2)$-state time-varying automaton over the changing alphabet.

1. Time-varying automata and groups generated by them

Let $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ be a set of nonnegative integers. A *changing alphabet* is an infinite sequence

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

where X_t are nonempty, finite sets (sets of letters). A *word* over the changing alphabet X is a finite sequence $x_0x_1\ldots x_l$, where $x_i \in X_i$ for $i = 0, 1, \ldots, l$. We denote by X^* the set of all words (including the empty word $\emptyset$). By $|w|$ we denote the length of the word $w \in X^*$. The set of words of the length t we denote by $X^{(t)}$. For any $t \in \mathbb{N}_0$ we also consider the set $X_{(t)}$ of finite sequences in which the i-th letter ($i = 1, 2, \ldots$) belongs to the set X_{t+i-1}. In particular $X_{(0)} = X^*$.

Definition 1. *A time-varying Mealy automaton is a quintuple*

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

where:

1. $Q = (Q_t)_{t\in\mathbb{N}_0}$ *is a sequence of sets of inside states,*
2. $X = (X_t)_{t\in\mathbb{N}_0}$ *is a changing input alphabet,*
3. $Y = (Y_t)_{t\in\mathbb{N}_0}$ *is a changing output alphabet,*
4. $\varphi = (\varphi_t)_{t\in\mathbb{N}_0}$ *is a sequence of transitions functions of the form*

$$\varphi_t \colon Q_t \times X_t \to Q_{t+1},$$

5. $\psi = (\psi_t)_{t\in\mathbb{N}_0}$ *is a sequence of output functions of the form*

$$\psi_t \colon Q_t \times X_t \to Y_t.$$

We say that an automaton A is *finite* if the set

$$S = \bigcup_{t\in\mathbb{N}_0} Q_t$$

of all its inside states is finite. If $|S| = n$, we say that A is an *n-state automaton.*

It is convenient to present a time-varying Mealy automaton as a labelled, directed, locally finite graph with vertices corresponding to the inside states of the automaton. For every $t \in \mathbb{N}_0$ and every letter $x \in X_t$ an arrow labelled by x starts from every state $q \in Q_t$ to the state $\varphi_t(q, x)$. Each vertex $q \in Q_t$ is labelled by the corresponding *state function*

$$\sigma_{t,q}\colon X_t \to Y_t, \quad \sigma_{t,q}(x) = \psi_t(q, x). \tag{1}$$

To make the graph of the automaton clear, the sets of vertices V_t and $V_{t'}$ corresponding to the sets Q_t and $Q_{t'}$ respectively, are disjoint whenever $t \neq t'$ (in particular, different vertices may correspond to the same inside state). Moreover, we will substitute a large number of arrows connecting two fixed states and having the same direction for a one multi-arrow labelled by suitable letters and if the labelling of such a multi-arrow is obvious we will omit this labelling.

For instance Figure 1 presents a 2-state time-varying automaton in which $Q_t = \{0, 1\}$, $X_t = Y_t = \{0, 1, \ldots, t + 1\}$ and the state functions $\sigma_{t,0} = \sigma_t$ and $\sigma_{t,1} = 1$ are respectively a cyclical permutation $(0, 1, \ldots, t+1)$ and the identity permutation of the set X_t.

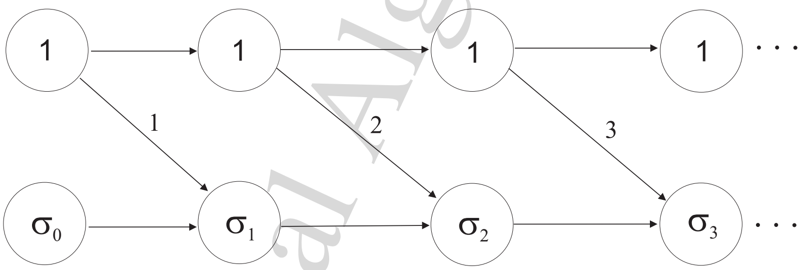

Figure 1: an example of a 2-state time-varying automaton

A time-varying automaton may be interpreted as a machine, which being at a moment $t \in \mathbb{N}_0$ in a state $q \in Q_t$ and reading on the input tape a letter $x \in X_t$, goes to the state $\varphi_t(q, x)$, types on the output tape the letter $\psi_t(q, x)$, moves both tapes to the next position and then proceeds further to the next moment $t + 1$.

The automaton A with a fixed *initial state* $q \in Q_0$ is called the *initial automaton* and is denoted by A_q. The above interpretation defines a natural action of A_q on the words. Namely, the initial automaton A_q defines a function $f_q^A\colon X^* \to Y^*$ as follows:

$$f_q^A(x_0x_1...x_l) = \psi_0(q_0, x_0)\psi_1(q_1, x_1)...\psi_l(q_l, x_l),$$

where the sequence $q_0, q_1, \ldots, q_l$ of inside states is defined recursively:

$$q_0 = q, \qquad q_i = \varphi_{i-1}(q_{i-1}, x_{i-1}) \quad \text{for} \quad i = 1, 2, \ldots, l. \tag{2}$$

This action may be extended in a natural way on the set X^ω of infinite words over X.

The function f_q^A is called the *automaton function* defined by A_q. The image of a word $w = x_0x_1 \ldots x_l$ under a map f_q^A can be easily found using the graph of the automaton. One must find a directed path starting in a vertex $q \in Q_0$ and with consecutive labels $x_0, x_1, \ldots, x_l$. Such a path will be unique. If $\sigma_0, \sigma_1, \ldots, \sigma_l$ are the labels of consecutive vertices in this path, then the word $f_q^A(w)$ is equal to $\sigma_0(x_0)\sigma_1(x_1) \ldots \sigma_l(x_l)$.

In the set of words over a changing alphabet we consider for any $k \in \mathbb{N}_0$ the equivalence relation $\sim_k$ as follows:

$w \sim_k v$ if and only if w and v have a common prefix of the length k.

Let X and Y be changing alphabets and let f be a function of the form $f\colon X^* \to Y^*$. If f preserves the relation $\sim_k$ for any k, then we say that f *preserves beginnings of the words.* If $|f(w)| = |w|$ for any $w \in X^*$, then we say that f *preserves lengths of the words.*

Theorem 1. *[7] The function $f\colon X^* \to Y^*$ is an automaton function (defined by some initial automaton A_q) if and only if it preserves beginnings and lengths of the words.*

Definition 2. *Let $f\colon X^* \to Y^*$ be an automaton function and let $w \in X^*$ be a word of the length $|w| = n$. The function $f_w\colon X_{(n)} \to Y_{(n)}$ defined by the equality*

$$f(wv) = f(w)f_w(v)$$

is called a remainder of f on the word w or simply a w-remainder of f.

Definition 3. *Let $A = (Q, X, Y, \varphi, \psi)$ be a time-varying Mealy automaton. For any $t_0 \in \mathbb{N}_0$ the automaton $A|^{t_0} = (Q', X', Y', \varphi', \psi')$ defined as follows*

$$Q'_t = Q_{t_0+t}, \;\; X'_t = X_{t_0+t}, \;\; Y'_t = Y_{t_0+t}, \;\; \varphi'_t = \varphi_{t_0+t}, \;\; \psi'_t = \psi_{t_0+t},$$

is called a t_0-remainder of A.

If $f = f_q^A$ is defined by the initial automaton A_q and $w = x_0 x_1 \dots x_l$, then the w-remainder f_w is an automaton function generated by the initial automaton B_{q_l}, where $B = A|^l$ is an l-remainder of A and the initial state q_l is defined by (2).

Definition 4. *An automaton A in which input and output alphabets coincide and every its state function $\sigma_{t,q}\colon X_t \to X_t$ is a permutation of X_t is called a permutational automaton.*

If A is a permutational automaton, then for every $q \in Q_0$ the transformation $f_q^A\colon X^* \to X^*$ is a permutation of X^*.

The set $SA(X)$ of automaton functions defined by all initial automata over a common input and output alphabet X forms a monoid with the identity function as the neutral element. The subset $GA(X)$ of functions generated by permutational automata is a group of invertible elements in $SA(X)$. The group $GA(X)$ is an example of residually finite group (see [8]).

Definition 5. *Let $A = (Q, X, X, \varphi, \psi)$ be a time-varying permutational automaton. The group of the form*

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

is called the group generated by automaton A.

For any permutational automaton A the group $G(A)$ is residually finite, as a subgroup of $GA(X)$. It turns out that groups of this form include the class of finitely generated residually finite groups.

Theorem 2. *[8] For any n-generated residually finite group G there is an n-state time-varying automaton A such that $G \cong G(A)$.*

2. The embedding into the permutational wreath product

In this section we describe a close realtion between time-varying automata groups and permutational wreath products. Let K and H be finitely generated groups such that H is a permutation group of a finite set L. We define the permutational wreath product $K \wr_L H$ as a semidirect product

$$(\underbrace{K \times K \times \ldots \times K}_{|L|}) \rtimes H,$$

where H acts on the direct product by permuting the factors.

Let G be any subgroup of $GA(X)$. For any $i \in \mathbb{N}_0$ we define the group

$$G_i = \left\langle f_w \colon\ f \in G,\ w \in X^{(i)} \right\rangle,$$

which is a group generated by remainders f_w of functions $f \in G$ on all words $w \in X^*$ of the length $|w| = i$. In particular $G_0 = G$.

Proposition 1. *For any $f, g \in SA(X)$ and any word $w \in X^*$ we have*

$$(fg)_w = f_w g_{f(w)}. \tag{3}$$

If $g \in GA(X)$, then

$$\left(g^{-1}\right)_w = \left(g_{g^{-1}(w)}\right)^{-1}. \tag{4}$$

Proof. For any $u \in X_{(|w|)}$ we have

$$(fg)(wu) = (fg)(w)(fg)_w(u).$$

On the other hand

$$\begin{aligned}(fg)(wu) &= g(f(wu)) = g(f(w)f_w(u)) = \\ &= g(f(w))g_{f(w)}(f_w(u)) = (fg)(w)(f_w g_{f(w)})(u),\end{aligned}$$

what gives (3) from the previous equality. The formula (4) follows by substitution of f for g^{-1} in (3). □

Proposition 2. *Let us put the letters of the set X_i into the sequence*

$$x_0, x_1, \ldots, x_{m-1}.$$

Then the mapping

$$\Psi(g) = (g_{x_0}, g_{x_1}, \ldots, g_{x_{m-1}})\sigma_g \tag{5}$$

defines the embedding of the group G_i into the permutational wreath product $G_{i+1} \wr_{X_i} S(X_i)$, where the permutation $\sigma_g \in S(X_i)$ is defined by $\sigma_g(x) = g(x)$.

Proof. The equalities

$$g(xu) = \sigma_g(x)g_x(u), \quad x \in X_i,\ u \in X_{(i+1)}$$

imply that Ψ is one-to-one. Next, by Proposition 1 we have:

$$\begin{aligned}\Psi(fg) &= ((fg)_{x_0}, \ldots, (fg)_{x_{m-1}})\sigma_{fg} = \\ &= \left(f_{x_0}g_{\sigma_f(x_0)}, \ldots, f_{x_{m-1}}g_{\sigma_f(x_{m-1})}\right)\sigma_f\sigma_g = \\ &= (f_{x_0}, f_{x_1}, \ldots, f_{x_{m-1}})\sigma_f\ (g_{x_0}, g_{x_1}, \ldots, g_{x_{m-1}})\sigma_g = \Psi(f)\Psi(g).\end{aligned}$$

Hence Ψ is a homomorphism. □

We will rewrite (5) in the form

$$g = [g_{x_0}, g_{x_1}, \ldots, g_{x_{m-1}}]\sigma_g$$

and call this the *decomposition* of g. In case $\sigma_g = 1$ (the identity permutation) we will write $g = [g_{x_0}, g_{x_1}, \ldots, g_{x_{m-1}}]$.

3. $Dih(\mathbb{Z}^n)$ as a time-varying automaton group

Let $m_0 = 2, m_1, m_2, \ldots$ be an infinite sequence of positive even numbers and let $a_1, a_2, \ldots, a_k$ be a sequence of positive odd numbers such that

$$\sup_i \left\{ \frac{m_i}{a_1^i + a_2^i + \ldots + a_k^i} \right\} = \infty. \tag{6}$$

Lemma 1. *Let $r_1, r_2, \ldots, r_k$ be integers such that the congruence*

$$a_1^i r_1 + a_2^i r_2 + \ldots + a_k^i r_k \equiv 0 \pmod{m_i}$$

holds for any $i \in \mathbb{N}_0$. Then $r_1 = r_2 = \ldots = r_k = 0$.

Proof. There are integers q_i, such that $a_1^i r_1 + \ldots + a_k^i r_k = q_i m_i$ for $i \in \mathbb{N}_0$. Let us denote $c = \max\{|r_1|, \ldots, |r_k|\}$. For any $i \in \mathbb{N}_0$ we have

$$|q_i m_i| = |a_1^i r_1 + \ldots + a_k^i r_k| \leq c(a_1^i + \ldots + a_k^i).$$

We show that $q_i = 0$ for infinitely many $i \in \mathbb{N}_0$. Otherwise, there is $i_0 \in \mathbb{N}_0$ such that $q_i \neq 0$ for all $i \geq i_0$. Then

$$c \geq \frac{|q_i m_i|}{a_1^i + \ldots + a_k^i} \geq \frac{m_i}{a_1^i + \ldots + a_k^i}$$

for all $i \geq i_0$, what is contrary to the assumption (6). Let $i_1 < i_2 < \ldots$ be an infinite sequence for which $q_{i_j} = 0$, $j \in \mathbb{N}_0$. Thus $(r_1, \ldots, r_k)$ is a solution of the homogeneous system of linear equations

$$a_1^{i_j} x_1 + \ldots + a_k^{i_j} x_k = 0, \quad j = 1, \ldots, k.$$

The matrix of this system is a generalized Vandermonde $k \times k$ matrix. It is known that its determinant is always positive. Hence all r_i are equal to zero. □

We define a $2k$-state time-varying, permutational automaton A in which (in point 4 below $x \pm_m y$ denotes an arithmetical operation modulo m):

1. $Q_t = \{a_1, -a_1, a_2, -a_2, \ldots, a_k, -a_k\}$,
2. $X_t = \{0, 1, \ldots, m_t - 1\}$,
3. $\varphi_t(\pm a_i, x) = a_i \cdot (-1)^x$,
4. $\psi_t(\pm a_i, x) = x \pm_{m_t} a_i^t$.

We are going to show that the group $G(A)$ generated by the automaton A is isomorphic to the generalized dihedral group $Dih(\mathbb{Z}^{k-1})$.

The graph of A is a disjoint sum of k graphs of the form depicted in the Figure 2, each one defining a 2-state time-varying automaton with the set $\{-a_i, a_i\}$ of its inside states (the labelling σ_t constitutes a cyclical permutation $(0, 1, \ldots, m_t - 1)$ of the set X_t). Directly from the above

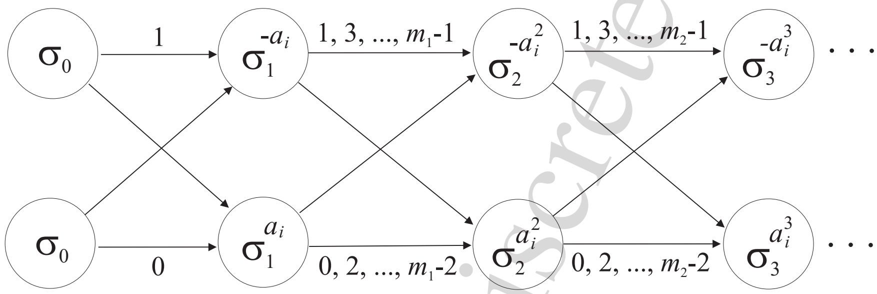

Figure 2: the fragment of A corresponding to the states $\pm a_i \in Q_0$

graph we see that $f^A_{a_i} = f^A_{-a_i}$ for $i = 1, 2 \ldots, k$, and hence

$$G(A) = \langle f^A_{a_1}, f^A_{a_2}, \ldots, f^A_{a_k}\rangle.$$

To simplify, we denote

$$f_i = f^A_{a_i}$$

for $i = 1, 2, \ldots, k$. For any $i \in \{1, 2, \ldots, k\}$ and any $j \in \mathbb{N}_0$ we also denote by $f_{i,j}$ the remainder of f_i on a zero-word $00\ldots0$ of the length j. In particular $f_i = f_{i,0}$.

Proposition 3. *The decomposition of $f^\varepsilon_{i,j}$, $\varepsilon \in \{-1, 1\}$ is as follows*

$$f^\varepsilon_{i,j} = [f_{i,j+1}, f^{-1}_{i,j+1}, f_{i,j+1}, f^{-1}_{i,j+1}, \ldots, f_{i,j+1}, f^{-1}_{i,j+1}]\sigma_j^{\varepsilon a_i^j}.$$

In particular $f_i^2 = 1$ for $i = 1, 2, \ldots, k$.

Proof. Let us denote by $f^-_{i,j}$ the remainder of f_i on the word $11\ldots1$ of the length j. Directly from the graph of A we have

$$\begin{aligned} f_{i,j} &= [f_{i,j+1}, f^-_{i,j+1}, f_{i,j+1}, f^-_{i,j+1}, \ldots, f_{i,j+1}, f^-_{i,j+1}]\sigma_j^{a_i^j}, \\ f^-_{i,j} &= [f_{i,j+1}, f^-_{i,j+1}, f_{i,j+1}, f^-_{i,j+1}, \ldots, f_{i,j+1}, f^-_{i,j+1}]\sigma_j^{-a_i^j}. \end{aligned}$$

As a_i is an odd number, we obtain:

$$f_{i,j}f^-_{i,j} = f^-_{i,j}f_{i,j} = [f_{i,j+1}f^-_{i,j+1}, f^-_{i,j+1}f_{i,j+1}, f_{i,j+1}f^-_{i,j+1}, \ldots, f^-_{i,j+1}f_{i,j+1}].$$

Hence $f_{i,j}^{-}f_{i,j} = f_{i,j}f_{i,j}^{-} = 1$ and in consequence $f_{i,j}^{-} = f_{i,j}^{-1}$. In particular

$$f_i^2 = f_{i,0}^2 = [f_{i,1}, f_{i,1}^{-1}]\sigma_0[f_{i,1}, f_{i,1}^{-1}]\sigma_0 = [f_{i,1}f_{i,1}^{-1}, f_{i,1}^{-1}f_{i,1}] = 1.$$

□

Since all the generators f_i are of order two, every element $g \in G(A)$ is of the form $g = f_{\nu_1}f_{\nu_2}\dots f_{\nu_r}$ for some $\nu_1, \nu_2, \dots, \nu_r \in \{1, 2, \dots, k\}$ and $\nu_{j+1} \neq \nu_j$ for $j = 1, \dots, r-1$.

Proposition 4. *Let g_w be a remainder of g on the word $w \in X^{(i)}$. Then*

$$g_w = \begin{cases} f_{\nu_1,i}f_{\nu_2,i}^{-1}\dots f_{\nu_r,i}^{(-1)^{r-1}}, & \text{if } x \text{ even,} \\ f_{\nu_1,i}^{-1}f_{\nu_2,i}\dots f_{\nu_r,i}^{(-1)^r}, & \text{if } x \text{ odd,} \end{cases}$$

where x is the last letter of w.

Proof. By Proposition 1 we may write

$$g_w = (f_{\nu_1}f_{\nu_2}\dots f_{\nu_r})_w = (f_{\nu_1})_{w_1}(f_{\nu_2})_{w_2}\dots(f_{\nu_r})_{w_r},$$

where $(f_{\nu_j})_{w_j}$ $(j = 1, \dots, r)$ is a remainder of f_{ν_j} on the word

$$w_j = f_{\nu_1}f_{\nu_2}\dots f_{\nu_{j-1}}(w) \in X^{(i)}.$$

From the graph of A and by Proposition 3, the remainder of any generator $f_t = f_{a_t}^A$ on an arbitrary word $v \in X^{(i)}$ is equal to $f_{t,i}^{\varepsilon}$ for some $\varepsilon \in \{-1, 1\}$. In consequence

$$g_w = f_{\nu_1,i}^{\varepsilon_1}f_{\nu_2,i}^{\varepsilon_2}\dots f_{\nu_r,i}^{\varepsilon_r}$$

for some $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r \in \{-1, 1\}$. Let $w' \in X^*$ be a prefix of w of the length $|w| - 1 = i - 1$. Then

$$g_{w'} = f_{\nu_1,i-1}^{\varepsilon_1'}f_{\nu_2,i-1}^{\varepsilon_2'}\dots f_{\nu_r,i-1}^{\varepsilon_r'}$$

for some $\varepsilon_1', \varepsilon_2', \dots, \varepsilon_r' \in \{-1, 1\}$. By Proposition 1 the element $f_{\nu_j,i}^{\varepsilon_j}$ is equal to $(f_{\nu_j,i-1}^{\varepsilon_j'})_{x'}$ - the remainder of $f_{\nu_j,i-1}^{\varepsilon_j'}$ on a one-letter word x', where

$$x' = f_{\nu_1,i-1}^{\varepsilon_1'}f_{\nu_2,i-1}^{\varepsilon_2'}\dots f_{\nu_{j-1},i-1}^{\varepsilon_{j-1}'}(x) = x +_{m_{i-1}} (\varepsilon_1'a_{\nu_1}^{i-1} + \dots + \varepsilon_{j-1}'a_{\nu_{j-1}}^{i-1}).$$

Since m_{i-1} is even and $a_{\nu_1}, \dots, a_{\nu_{j-1}}$ are all odd, the parity of the letter x' depends only on j and x in the following way: for x even the letter x' is even only for j odd, and for x odd the letter x' is even only for j even. Now, it suffices to see that by Proposition 3 the remainder $(f_{\nu_j,i-1}^{\varepsilon_j'})_{x'}$ is equal to $f_{\nu_j,i}$ for x' even, or to $f_{\nu_j,i}^{-1}$ for x' odd. □

Let $g \in G(A)$ be represented by a group-word

$$f_{\nu_1} f_{\nu_2} \dots f_{\nu_r} \tag{7}$$

(now, we do not assume that $\nu_{j+1} \neq \nu_j$). With the group-word (7) we associate the sequence of integers $r_1, r_2, \dots, r_k$ in which

$$r_i = r_i^- - r_i^+$$

and r_i^+ (r_i^-) denotes the number of occurrences of the generator f_i in even (odd) positions in (7).

Remark 1. Removing in (7) any subword of the form $f_j f_j$ does not change the value of any r_i.

Proposition 5. *Any word $w = x_0 x_1 \dots x_t \in X^*$ is mapped by g on the word $g(w) = y_0 y_1 \dots y_t \in X^*$, where*

$$y_i = x_i +_{m_i} (-1)^{x_{i-1}} \left(a_1^i r_1 + a_2^i r_2 + \dots + a_k^i r_k\right)$$

for $i = 0, 1, \dots, t$ (we assume $x_{-1} = 0$).

Proof. By Remark 1 we may assume that $\nu_{j+1} \neq \nu_j$ for $j = 1, \dots, r-1$. Now, the thesis follows by the equality $y_i = g_{x_0 x_1 \dots x_{i-1}}(x_i)$ and by Proposition 4. □

Let r be the length of the group-word (7). In case r even the number of all the symbols in even positions in (7) is equal to the number of all the symbols in odd positions, and in case r odd these numbers differ by one. Hence the sum

$$\varepsilon = r_1 + r_2 + \dots + r_k$$

is equal to $(r)_2$ - the remainder of r modulo 2.

Theorem 3. *The mapping*

$$\Psi(g) = (r_1, r_2, \dots, r_{k-1})\, \varepsilon$$

defines the isomorphism between the groups $G(A)$ and $Dih(\mathbb{Z}^{k-1})$.

Proof. First we show that Ψ is a well-defined, one-to-one mapping from $G(A)$ to $Dih(\mathbb{Z}^{k-1})$. Let $g = f_{\nu_1} \dots f_{\nu_r}$ and $g' = f_{\mu_1} \dots f_{\mu_s}$ be any elements of $G(A)$. Let

$$r_1, \dots, r_k,\ \ \varepsilon = r_1 + \dots + r_k,$$
$$r'_1, \dots, r'_k,\ \ \varepsilon' = r'_1 + \dots + r'_k$$

be sequences corresponding to the group-words $f_{\nu_1}\ldots f_{\nu_r}$ and $f_{\mu_1}\ldots f_{\mu_s}$ respectively. By Proposition 5 we have: $g=g'$ if and only if

$$x_i+_{m_i}(-1)^{x_{i-1}}(a_1^i r_1+\ldots+a_k^i r_k)=x_i+_{m_i}(-1)^{x_{i-1}}(a_1^i r_1'+\ldots+a_k^i r_k')$$

for any $x_{i-1}\in X_{i-1}, x_i\in X_i$ and any $i\in\mathbb{N}_0$. This condition is equivalent to the congruences:

$$a_1^i(r_1-r_1')+\ldots+a_k^i(r_k-r_k')\equiv 0 \pmod{m_i}$$

for any $i\in\mathbb{N}_0$. By Lemma 1 this is equivalent to the equalities: $r_i=r_i'$ for $i=1,2,\ldots,k$. In particular $\varepsilon=\varepsilon'$. As a result we have: $g=g'$ if and only if $\Psi(g)=\Psi(g')$. To show Ψ is a homomorphism, let us denote $\Psi(gg')=(R_1,\ldots,R_{k-1})\varepsilon''$. Since $gg'=f_{\nu_1}\ldots f_{\nu_r}f_{\mu_1}\ldots f_{\mu_s}$, we have:

$$\varepsilon''=(r+s)_2=(r)_2+_2(s)_2=\varepsilon+_2\varepsilon'.$$

If $\varepsilon=0$, then r is even. Thus for any $i\in\{1,2,\ldots,k-1\}$ the position of any symbol f_i in the group-word $f_{\mu_1}\ldots f_{\mu_s}$ has the same parity as in the group-word $f_{\nu_1}\ldots f_{\nu_r}f_{\mu_1}\ldots f_{\mu_s}$. In consequence $R_i^+=r_i^++r_i'^+$ and $R_i^-=r_i^-+r_i'^-$. Thus for $i=1,2,\ldots,k-1$ we have in this case

$$R_i=R_i^--R_i^+=(r_i^--r_i^+)+(r_i'^--r_i'^+)=r_i+r_i'.$$

If $\varepsilon=1$, then r is odd and the positions of any f_i in group-words $f_{\mu_1}\ldots f_{\mu_s}$ and $f_{\nu_1}\ldots f_{\nu_r}f_{\mu_1}\ldots f_{\mu_s}$ are of different parity. In consequence $R_i^+=r_i^++r_i'^-$ and $R_i^-=r_i^-+r_i'^+$. Thus for $i=1,2,\ldots,k-1$ we have in this case

$$R_i=R_i^--R_i^+=(r_i^--r_i^+)-(r_i'^--r_i'^+)=r_i-r_i'.$$

Hence $\Psi(gg')=\Psi(g)\Psi(g')$. Tho show Ψ is onto we take any sequence of integers $r_1,r_2,\ldots,r_k$ with the sum $\varepsilon=r_1+r_2+\ldots+r_k\in\{0,1\}$. Then there is a group-word $f_{\nu_1}f_{\nu_2}\ldots f_{\nu_r}$ in the symbols $f_1,f_2,\ldots,f_k$ for which:

(i) $r=|r_1|+|r_2|+\ldots+|r_k|$,

(ii) the symbol f_i $(i=1,2,\ldots,k)$ occurs $|r_i|$ times in this word,

(iii) if $r_i>0$ $(r_i<0)$, then each f_i occurs in the odd (even) position.

Then $\Psi(g)=(r_1,r_2,\ldots,r_{k-1})\,\varepsilon$ for the element $g=f_{\nu_1}f_{\nu_2}\ldots f_{\nu_r}$. □

Corollary 1. *Let $||g||$ be the length of the shortest presentation of any $g \in G(A)$ as a product of generators $f_1, \dots, f_k$. If*

$$\Psi(g) = (r_1, r_2, \dots, r_{k-1})\varepsilon,$$

then

$$||g|| = |r_1| + |r_2| + \dots + |r_{k-1}| + |r_1 + r_2 \dots + r_{k-1} - \varepsilon|.$$

Proof. Any group-word $f_{\nu_1} f_{\nu_2} \dots f_{\nu_r}$ satisfying the conditions (i)-(iii) in the proof of Theorem 3 constitutes the shortest representative of g. □

Using Theorem 3 one may derive the following algorithms solving the word problem (WP) and the conjugacy problem (CP) in $G(A)$.

ALGORITHMS: Let $f_{\nu_1} \dots f_{\nu_r}$ and $f_{\mu_1} \dots f_{\mu_s}$ be any group-words in $f_1, \dots, f_k$. Calculate their sequences: $r_1, \dots, r_k, \varepsilon$ and $r'_1, \dots, r'_k, \varepsilon'$. Then

(WP) the group-words define the same element if and only if $r_i = r'_i$ for $i = 1, \dots, k$,

(CP) the group-words define the conjugate elements if and only if $\varepsilon = 0$ and $r_i = -r'_i$ for $i = 1, \dots, k$, or if $\varepsilon = 1$ and $r_i \equiv r'_i \pmod 2$ for $i = 1, \dots, k$.

4. The action on the set of words

With the group $G = G(A)$ we associate the following subgroups:

1. $St_G(w) = \{g \in G \colon g(w) = w\}$ - the stabilizer of the word $w \in X^*$,
2. $St_G(n) = \bigcap_{w \in X^{(n)}} St_G(w)$- the stabilizer of the n-th level, which is the intersection of the stabilizers of the words of the length n,
3. P_u - the stabilizer of an infinite word $u \in X^\omega$ (the so called parabolic subgroup).

Theorem 4. *Let $n \in \mathbb{N}$, $w \in X^{(n)}$ and $u \in X^\omega$. Then*

$$St_G(w) = St_G(n) \simeq \mathbb{Z}^{k-1}$$

and the parabolic subgroup P_u is a trivial group.

Proof. Let $\Psi(g) = (r_1, \dots, r_{k-1})\varepsilon$. By proposition 5 we have $g \in St_G(w)$ if and only if $g \in St_G(n)$ if and only if $\varepsilon = 0$ and

$$(a_1^i - a_k^i)r_1 + (a_2^i - a_k^i)r_2 + \ldots + (a_{k-1}^i - a_k^i)r_{k-1} \equiv 0 \pmod{m_i}$$

for $0 < i < n$. Thus in case $n = 1$ we have: $g \in St_G(w)$ if and only if $g \in St_G(n)$ if and only if $\varepsilon = 0$. Hence $St_G(w) = St_G(1) \simeq \mathbb{Z}^{k-1}$ in this case. Thus for $n \geq 1$ the stabilizer $St_G(w) = St_G(n) < St_G(1)$ is isomorphic with a free abelian group of rank $l \leq k-1$. On the other hand, if each r_i is divisible by the product $m_1m_2 \dots m_{n-1}$, then the element g with $\Psi(g) = (r_1, \dots, r_{k-1})0$ is an element of the stabilizer $St_G(n)$. In consequence $St_G(n)$ contains $\mathbb{Z}^{k-1}$ as a subgroup. Thus $St_G(n)$ must be isomorphic with $\mathbb{Z}^{k-1}$. The triviality of any parabolic subgroup is a direct consequence of Lemma 1. □

Let $w = x_0x_1 \dots x_t \in X^*$ be any word over the changing alphabet X, and let

$$Orb(w) = \{g(w) \colon g \in G\}$$

be its orbit. From Proposition 5 and Theorem 3 we see that the word $v = y_0y_1 \dots y_t \in X^*$ belongs to $Orb(w)$ if and only if there are integers $r_1, r_2, \dots, r_{k-1}, \varepsilon$ with $\varepsilon \in \{0, 1\}$ such that

$$y_i = x_i +_{m_i} (-1)^{x_{i-1}}\varepsilon a_k^i +_{m_i} (-1)^{x_{i-1}} \sum_{j=1}^{k-1} (a_j^i - a_k^i) r_j \qquad (8)$$

for $i = 0, 1, \dots, t$. Since, all m_i are even and all a_i are odd, this implies: $y_i - y_0 \equiv x_i - x_0 \pmod 2$ for $i = 0, 1, \dots t$. In particular the action of the group $G(A)$ on the set X^* is not spherically transitive. By adding some additional assumption on m_i, we may obtain a nice description of this action.

Theorem 5. *Let $p_1 < p_2 < p_3 < \dots$ be a sequence of odd primes such that $p_i > i(a_1^i + \ldots + a_k^i)$ and let $m_i = 2p_i$ for $i = 1, 2 \dots$. Then the words $w = x_0x_1 \dots x_t$ and $v = y_0y_1 \dots y_t$ belong to the same orbit if and only if*

$$y_i - y_0 \equiv x_i - x_0 \pmod 2 \qquad (9)$$

for $i = 0, 1, \dots, t$. In particular

$$[G : St_G(t + 1)] = m_0m_1 \dots m_t/2^t$$

for $t = 0, 1, 2, \dots$.

Proof. The equalities $p_i > i(a_1^i + \ldots + a_k^i)$ assure that the condition (6) holds. Thus, it suffices to prove, that if w and v satisfy (9), then there is a sequence $r_1, r_2, \ldots, r_{k-1}, \varepsilon$ with $\varepsilon \in \{0, 1\}$ which satisfies (8). Let us denote: $\varepsilon = (y_0 - x_0)_2$ and $z_i = (y_i - x_i) \cdot (-1)^{x_{i-1}} - \varepsilon a_k^i$, $b_i = (a_1^i - a_k^i)/2$ for $i = 0, 1, \ldots, t$. Then all z_i are even, and for $i = 1, 2, \ldots, t$ the numbers b_i and p_i are coprime. Using the Chinese Remainder Theorem we can find an integer r such that

$$z_i/2 \equiv rb_i \pmod{p_i}$$

for $i = 1, 2, \ldots, t$. Then the sequence $r_1, r_2, \ldots, r_{k-1}, \varepsilon$ in which $r_1 = r$ and $r_2 = \ldots = r_{k-1} = 0$ satisfies (8). As a consequence we obtain

$$[G : St_G(t+1)] = [G : St_G(w)] = |Orb(w)| = m_0 m_1 \ldots m_t / 2^t.$$

□

References

[1] L. Bartholdi, R. I. Grigorchuk, V. Nekrashevych. *From fractal groups to fractal sets*. Fractal in Graz 2001. Analysis-Dynamics-Geometry-Stochastics (P. Grabner and W. Woess, eds.), Trends in Mathematics, vol. 19, Birkhäuser, 2003, pp. 25–118.

[2] R. I. Grigorchuk, V. V. Nekrashevich, V. I. Sushchanskii. *Automata, Dynamical Systems and Groups*. Proseedings of Steklov Institute of Mathematics, 231:128-203, 2000.

[3] R. I. Grigorchuk, A. Ïuk. *Advanced Course on Automata Groups*. Notes of the Course, Centre de Recerca Matematica Bellaterra (Spain), July 2004.

[4] D. E. Joyce: *http://www.clarku.edu/ djoyce/wallpaper*

[5] V. I. Sushchansky. *Group of Automatic Permutations*. Dopovidi NAN Ukrainy, N6:47-51, 1998 (in *Ukrainian*).

[6] V. I. Sushchansky. *Group of Finite Automatic Permutations*. Dopovidi NAN Ukrainy, N2:48-52, 1999 (in *Ukrainian*).

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

[8] A. Woryna. *On permutation groups generated by time-varying Mealy automata*. Publ. Math. Debrecen, vol. 67/1-2 (2005), 115-130.

Contact information

Adam Woryna Institute of Mathematics, Silesian University of Technology, 44-100 Gliwice
E-Mail: Adam.Woryna@polsl.pl

Received by the editors: 23.09.2006
and in final form 14.10.2008.