Acta Cybernetica **18** (2007) 23–46.

Groups and Semigroups Defined by some Classes of Mealy Automata

Alexander S. Antonenko* and Eugene L. Berkovich*

Abstract

Two classes of finite Mealy automata (automata without branches, slow-moving automata) are considered in this article. We study algebraic properties of transformations defined by automata of these classes. We consider groups and semigroups defined by automata without branches.

Keywords: Finite automata; Groups defined by automata; Semigroups defined by automata; Finite automaton transformations.

Introduction

In this paper we study finite state Mealy automata over two-symbol alphabet and finite state automata transformations defined by them. We shall examine algebraic properties of these transformations, various groups and semigroups of automata transformations and groups defined by noninitial automata of special types.

Groups of automaton transformations have been already investigated in the early sixties of the 20th century (see [1]-[4]). Recent result in the field of semigroups and groups are presented in [6]-[7]. The papers [5] and [8] present reviews of the main results of the theory of automaton transformation groups and semigroups.

Mealy automata turned out to be a convenient tool of defining groups and semigroups. The thing is that small (in number of states and alphabet symbols) Mealy automata generate complex groups.

Those of particular interest are groups with extremal properties, for example, periodic groups of Burnside type, groups of intermediate growth, etc. Mealy automata are used to construct examples of such groups. With their help, Burnside's problem was solved, as well as the problem of intermediate growth groups existence, posed by Milnor in 1968 (the solution of the latter belongs to Grigorchuk).

In the work [10] semigroups and the growth functions of two state automata over two-symbol alphabets are investigated. The question on what groups and semigroups are defined by three state automata over two-symbol alphabets remains unsolved. Therefore, we consider two special classes of automata.

*Odessa I. I. Mechnikov National University. E-mail: {aantonenko,eberk}@mail.ru

The first part of this study sets out the basic definitions and results of Mealy automata theory and gives the definitions of groups and semigroups defined by automata.

The second part is dedicated to Mealy automata over two-symbol alphabets, and a classification of states of such automata is suggested. Two special types of automata are defined on this basis: automata without branches and slow-moving automata.

We obtain results for automata without branches which characterize the groups defined by them for any number of states. Also we study semigroups defined by automata without branches.

The class of slow-moving automata is very wide, and this is why we have limited our investigation to its subclass, namely slow-moving automata of finite type. We have studied the algebraic properties of transformations defined by slow-mowing finite state automata. We have also found family of slow-moving transformations of finite type such that any other one is a composition of members of this family.

1 Preliminaries

Definition 1 ([11, 12])**.** *A finite Mealy automaton is an ordered quintuple $A = (X, Y, Q, \pi, \lambda)$, where X is the input alphabet, Y is the output alphabet, Q is the finite nonempty set of states, $\pi : X \times Q \to Q$ is the transition function and $\lambda : X \times Q \to Y$ is the output function. X and Y are finite nonempty sets.*

We will consider only finite automata whose input and output alphabets coincide ($X = Y$). We denote such automata by the quadruples $A = (X, Q, \pi, \lambda)$. Mainly we will consider automata over the two-symbol alphabet $X = \{0, 1\}$.

Let $T_X = \{f \mid f : X \to X\}$ be the semigroup of all transformations of the set X (the full transformation semigroup), $S_X = \{f \mid f : X \to X, f \text{ is bijective}\}$ the group of all bijective transformations of the set X (the full symmetric group), X^* the set of all finite words over X and X^ω the set of all infinite words (ω-words) over X.

It is convenient to describe finite automata by the Moore diagrams. We will use the following modification of it. The Moore diagram of an automaton A is an edge-labelled and vertex-labelled directed multigraph D_A with the set of vertices Q. Vertices q_i and q_j of the graph D_A are connected by the oriented edge in direction from q_i to q_j marked by the label x, if $\pi(x, q_i) = q_j$. Here $x \in X,\ q_i, q_j \in Q$. Every vertex q is labelled by the transformation $\lambda_q \in T_X$ of the alphabet X that corresponds to the output function at the state q, i.e. $\lambda_q(x) = \lambda(x, q)$, where $x \in X,\ q \in Q$.

The functions π and λ can be extended naturally to mappings of the set $X^* \times Q$ into the sets Q and X^* by the following equalities [12]:

$$\begin{aligned} &\pi(\Lambda, q) = q, \quad \pi(wx, q) = \pi\left(x, \pi(w, q)\right), \\ &\lambda(\Lambda, q) = \Lambda, \quad \lambda(wx, q) = \lambda(w, q)\lambda\left(x, \pi(w, q)\right), \end{aligned}$$

where $\Lambda \in X^*$ is the empty word, $q \in Q,\ w \in X^*$ and $x \in X$. The function λ

can also be extended in a natural way to a mapping $\lambda : X^\omega \times Q \to X^\omega$ (see for example, [12]).

Definition 2 ([12])**.** *The transformation $f_q : X^\omega \to X^\omega$ defined by the equality $f_q(u) = \lambda(u, q)$, where $u \in X^\omega$, is called the automaton transformation defined by the automaton $A = (X, Q, \pi, \lambda)$ at state q.*

The Mealy automaton $A = (X, Q, \pi, \lambda)$, where $Q = \{q_0, q_1, \ldots, q_{n-1}\}$, defines the set $F_A = \left\{f_{q_0}, f_{q_1}, \ldots, f_{q_{n-1}}\right\}$ of automaton transformations over X^ω.

Definition 3. *The Mealy automaton A is called invertible if all transformations from the set F_A are bijections.*

It is easy to show (see for example [5]) that A is invertible if and only if the transformation λ_q is a permutation of X for each state $q \in Q$.

Definition 4 ([12])**.** *The Mealy automata $A_i = (X, Q_i, \pi_i, \lambda_i)$, $i = 1, 2$, are called isomorphic if there exist two permutations $\xi, \psi \in S_X$ and a one-to-one mapping $\theta : Q_1 \to Q_2$ such that*

$$\theta\pi_1(x, q) = \pi_2(\xi x, \theta q), \qquad \psi\lambda_1(x, q) = \lambda_2(\xi x, \theta q)$$

for all $x \in X$ and $q \in Q_1$.

Definition 5 ([12])**.** *The Mealy automata A_i, $i = 1, 2$, are called equivalent if $F_{A_1} = F_{A_2}$.*

Proposition 6 ([12])**.** *Each class of equivalent Mealy automata over the alphabet X contains, up to isomorphism, a unique automaton that is minimal with respect to the number of states (such an automaton is called reduced).*

The minimal automaton can be found using the standard algorithm of minimization.

Definition 7 ([13])**.** *For $i = 1, 2$, let $A_i = (X, Q_i, \pi_i, \lambda_i)$ be arbitrary Mealy automata. The automaton $A = (X, Q_1 \times Q_2, \pi, \lambda)$ whose transition and output functions are defined by*

$$\begin{aligned} \pi\left(x, (q_1, q_2)\right) &= \left(\pi_1\left(\lambda_2\left(x, q_2\right), q_1\right), \pi_2\left(x, q_2\right)\right), \\ \lambda\left(x, (q_1, q_2)\right) &= \lambda_1\left(\lambda_2\left(x, q_2\right), q_1\right), \end{aligned}$$

where $x \in X$ and $(q_1, q_2) \in Q_1 \times Q_2$, is called the product *of the automata A_1 and A_2.*

Proposition 8 ([13])**.** *For any states $q_1 \in Q_1$, $q_2 \in Q_2$ and arbitrary word $u \in X^*$ the following equality holds:*

$$f_{(q_1,q_2),A}(u) = f_{q_1,A_1}\left(f_{q_2,A_2}(u)\right).$$

Definition 9. *The semigroup generated by the set $F_A = \left\{f_{q_0}, f_{q_1}, \ldots, f_{q_{n-1}}\right\}$ of transformations defined by a Mealy automaton A in all of its states is called the semigroup defined by the automaton A. In the case of an invertible automaton A the group generated by F_A is called the group defined by the automaton A.*

2 Two special classes of automata

In this section we consider two special classes of automata. We will use the following classification of automata states.

Definition 10. *Let $A = (X, Q, \pi, \lambda)$ be a finite automaton. Let us call a state $q \in Q$*

1. *a rest state if for each $x \in X$, $\quad \pi(x, q) = q$ (the automaton will stay in this state)*
2. *an unconditional jump state if there exists a $q' \in Q$, such that $q' \neq q$ and for each $x \in X$, $\quad \pi(x, q) = q'$*
3. *a waiting state if there exists an $x \in X$ such that $\pi(x, q) = q'$, $q' \neq q$ and for each symbol $x' \in X$ with $x' \neq x$, $\pi(x', q) = q$. We will also call this state x-waiting state*
4. *a multi-waiting state if there exist $X' \subset X$ and $q' \neq q$ such that $2 \leq |X'| < |X|$ and for each $x' \in X'$, $\pi(x', q) = q'$ and for each $x \notin X'$, $\pi(x, q) = q$*
5. *a conditional jump state or branch state if there exist two distinct symbols $x_1 \neq x_2$ such that $\pi(x_1, q) \neq \pi(x_2, q) \neq q$*

Definition 11. *We say that an automaton A is an automaton without branches if all of its states are rest states or unconditional jump ones.*

In other words, the transition function of an automaton without branches depends only on the current state and is independent of input symbols. So for all $q \in Q$ and $x \in X$, we denote $\pi(x, q)$ by $s(q)$.

Definition 12. *We call an automaton A slow-moving if all of its states are rest states or waiting ones.*

In other words, for every state q, there is at most one symbol x such that $\pi\,(x, q) \neq q$.

Definition 13. *We call a transformation $f : X^\omega \to X^\omega$ slow-moving (without branches) if it can be defined by a slow-moving automaton (without branches).*

Example 14. Consider an example of a slow-moving automaton over the two-symbol alphabet $X = \{0,\ 1\}$ shown in Figure 1. We will consider an infinite input word $w \in X^\omega$ as a 2-adic integer. Let f denote the slow-moving transformation defined by this automaton at the state q_1. Then f adds one to any input 2-adic integer. Therefore this automaton is called "adding machine".

Consider the transformation $f^2 = f \circ f$. It is clear that f^2 adds two to an input 2-adic integer.

Therefore f^2 does not change the first input symbol, and then, not depending on what the first symbol was, acts as transformation f again. Thus, the second symbol is changed, in any case. So the initial state of the automaton defining such transformation can be neither the state of waiting nor the one of rest and the transformation f^2 is not slow-moving.

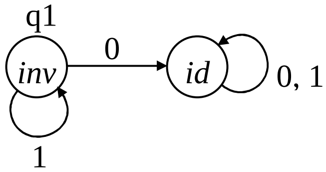

Figure 1: The adding machine

So the product of two slow-moving automata (transformations) is not a slow-moving automaton (transformation) in general.

3 Automata without branches

Definition 15. *We call the word transformation $f : X^\omega \to X^\omega$ symbol-by-symbol one, if*

$$f(x_1 x_2 \ldots x_n \ldots) = g_1(x_1)\, g_2(x_2) \ldots g_n(x_n) \ldots$$

where $g_i : X \to X$.

Lemma 16. *The transformation defined by an automaton without branches is a symbol-by-symbol transformation.*

The proof is clear.

Thus, the transformation f is completely defined by a word $g \in (T_X)^\omega$, $g = g_1 g_2 \ldots$. Let us denote the corresponding transformation by F_g:

$$F_g(x_1 x_2 \ldots x_n \ldots) = g_1(x_1)\, g_2(x_2) \ldots g_n(x_n) \ldots, \quad g \in X^\omega, \quad g = g_1 g_2 \ldots g_n \ldots$$

In case f is defined by an invertible automaton over the two-symbol alphabet, each map g_i is either the identity permutation, or transposition. In the first case, we consider $g_i = 0$, in the second one $g_i = 1$.

Lemma 17. *Let the transformation f be defined by an automaton without branches with n states. Then $f = F_{uw}$, where $|u| = n$, and $w \in (T_X)^\omega$ is a periodic word. Moreover, the length of the period does not exceed n.*

Proof. Let $A = (X, Q, \pi, \lambda)$ be an automaton without branches. Then the transformation corresponding to the state $q_k \in Q$ is F_g, where $g = g_1 g_2 \cdots$, $g_{i+1} = \lambda_{s^i(q_k)}$. Recall that $s(q_i) = \pi(x, q_i)$.

Let us consider the sequence $s^i(q_k)$ where $i = 0, 1, 2, \ldots$. Members of this sequence belong to the set $Q = \{q_0, q_1, \ldots, q_{n-1}\}$, which consists of n elements. Hence there are two equal elements $s^p(q_k) = s^{p+l}(q_k)$ among the first $n+1$ ones, where $p < n+1$, $l > 0$, $l \le n$.

Let $r = n - p \ge 0$. Fix an arbitrary $i > 0$. Applying $s^p(q_k) = s^{p+l}(q_k)$, we obtain $s^{r+i}(s^p(q_k)) = s^{r+i}\left(s^{p+l}(q_k)\right)$. Hence $s^{n+i}(q_k) = s^{n+i+l}(q_k)$.

So the sequence $s^i\left(q_k\right)$ is periodic beginning from the member $s^n\left(q_k\right)$. It follows that the sequence $g_{i+1} = \lambda_{s^i(q_k)}$ is periodic beginning from the member g_{n+1}. The length l of the period does not exceed n. $\square$

3.1 Groups defined by invertible automata without branches over a two-symbol alphabet

Let us remark that the output function of an invertible automaton over a two-symbol alphabet corresponding to a state q_i is either the identical permutation or the transposition. In the first case we write $\lambda_{q_i} = 0 \in Z_2$. In the second case we write $\lambda_{q_i} = 1 \in Z_2$. Since the transition function π of an automaton without branches is independent of any input symbols, we use the notation $s(q_i) = \pi(x, q_i)$. Let us consider $\left(Z_2\right)^0$ as the trivial group. The following theorem is applicable:

Theorem 18. *Let U be an invertible automaton without branches over a two-symbol alphabet and let n be the number of its states. Then the group defined by it is isomorphic to the group $\left(Z_2\right)^r$, where $r = \operatorname{rank} A$,*

$$A = \begin{pmatrix} \lambda_{q_0} & \lambda_{s(q_0)} & \cdots & \lambda_{s^{n-1}(q_0)} \\ \lambda_{q_1} & \lambda_{s(q_1)} & \cdots & \lambda_{s^{n-1}(q_1)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{q_{n-1}} & \lambda_{s(q_{n-1})} & \cdots & \lambda_{s^{n-1}(q_{n-1})} \end{pmatrix},$$

$$A \in M_n(Z_2), \quad s(q_i) = \pi(x, q_i), \quad x \in X.$$

We first prove some auxiliary lemmas. Let $v^* = vvv\ldots$, where $v \in \left(Z_2\right)^n, v^* \in \left(Z_2\right)^\omega$. We can associate each word uv having the length $n+m$ ($|u| = n$, $|v| = m$) with the map $P_{uv} = F_{uv^*}$.

Lemma 19. *The composition of invertible maps P_{uv} and P_{sw} is the map P_{uv+sw}, where $u, s \in \left(Z_2\right)^n$, $v, w \in \left(Z_2\right)^m$, addition is taken modulo 2 like in the group $\left(Z_2\right)^{n+m}$.*

Proof. The proof is straightforward. $\square$

Lemma 20. *Let U be an invertible automaton without branches over a two-symbol alphabet, n the quantity of its states and m the least common multiple of all lengths of the periods of sequences $\left\{s^i\left(q_k\right)\right\}_{i=n}^{\infty}$, $k = 0, \ldots, n-1$, $l = n+m$.*

Then the group defined by U is isomorphic to the group $\left(Z_2\right)^r$, where $r = \operatorname{rank} A'$,

$$A' = \begin{pmatrix} \lambda_{q_0} & \lambda_{s(q_0)} & \cdots & \lambda_{s^{l-1}(q_0)} \\ \lambda_{q_1} & \lambda_{s(q_1)} & \cdots & \lambda_{s^{l-1}(q_1)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{q_{n-1}} & \lambda_{s(q_{n-1})} & \cdots & \lambda_{s^{l-1}(q_{n-1})} \end{pmatrix},$$

$$A' \in M_{nl}(Z_2), \quad s(q_i) = \pi(x, q_i), \quad x \in X.$$

Proof. Let us denote by G the group defined by U. Note that all the transformations commute with each other and their orders are equal to 2. So every element of G is a composition of certain transformations f_i. Transformation $f_k = P_u$, where u is the k-th row of the matrix A' (m is a period for any sequence $s^i\,(q_k)$ beginning from n-th member). The composition of these transformations f_i is the transformation P_w, where w is the sum of the corresponding rows.

Thus, every element of G is a map P_w, where w is a linear combination of rows of A' in the linear space $(Z_2)^{n+m}$ over the field Z_2 . There are r linearly independent rows among rows of the matrix A'. The vector w is uniquely representable in the form of linear combination of r linearly independent rows of the matrix A'.

Set one-to-one correspondence between the elements $g \in G$, $g = P_w$, and r-vectors of coefficients of linear combination of linear independent rows of the matrix A' representing the vector w. Composition operation corresponds to the operation of addition of the coefficient vectors from $(Z_2)^r$.

Thus, G is isomorphic to $(Z_2)^r$. □

Proof of Theorem 18. To prove the theorem we need to show that $\operatorname{rank} A = \operatorname{rank} A'$. For this, let k be the minimal number such that the first k-1 columns of the matrix A' are linearly independent, but the first k ones are linearly dependent.

Then the k-th column is a linear combination of previous columns:

$$A^k = b_1 A^1 + b_2 A^2 + ... + b_{k-1} A^{k-1}, \tag{1}$$

where A^i is a i-th column of the matrix A'. We can write (1) in a more detailed form:

$$\begin{aligned}
\lambda_{s^{k-1}(q_1)} &= b_1 \lambda_{q_1} + b_2 \lambda_{s(q_1)} + \cdots + b_{k-1} \lambda_{s^{k-2}(q_1)} \\
\lambda_{s^{k-1}(q_2)} &= b_1 \lambda_{q_2} + b_2 \lambda_{s(q_2)} + \cdots + b_{k-1} \lambda_{s^{k-2}(q_2)} \\
&\dots \\
\lambda_{s^{k-1}(q_n)} &= b_1 \lambda_{q_n} + b_2 \lambda_{s(q_n)} + \cdots + b_{k-1} \lambda_{s^{k-2}(q_n)}
\end{aligned}$$

Let us prove that

$$A^{p+k} = b_1 A^{p+1} + b_2 A^{p+2} + ... + b_{k-1} A^{p+k-1}, \tag{2}$$

for all p from 0 to $l - k$.

Really, fix an arbitrary i between 1 and n. Let $s^p(q_i) = q_r$. Then

$$\begin{aligned}
b_1 \lambda_{s^p(q_i)} + b_2 \lambda_{s^{p+1}(q_i)} + ... + b_{k-1} \lambda_{s^{p+k-2}(q_i)} &= b_1 \lambda_{q_r} + b_2 \lambda_{s(q_r)} + ... + b_{k-1} \lambda_{s^{k-2}(q_r)} \\
&= \lambda_{s^{k-1}(q_r)} = \lambda_{s^{p+k-1}(q_i)}
\end{aligned}$$

Thus (2) has been shown. From (2) we can conclude, by induction, that the column A^{p+k} for any $p = 0, \dots, l-k$ is a linear combination of the columns A^1, A^2, …, A^{k-1}. Since $k \le n+1$, we conclude that $\operatorname{rank} A = \operatorname{rank} A'$. □

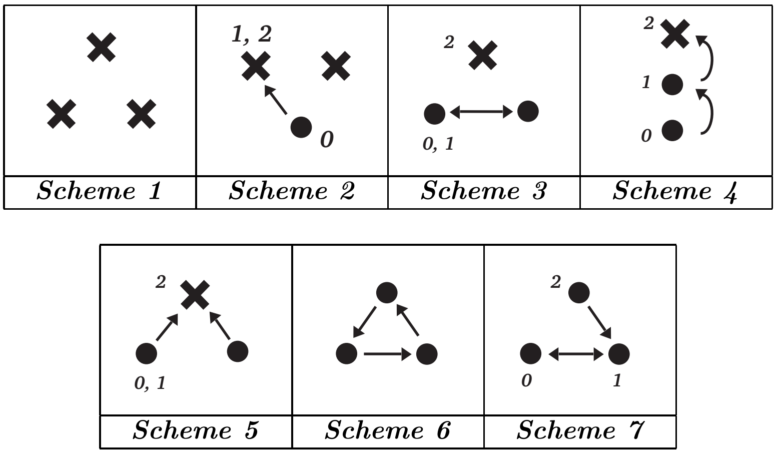

Figure 2: Schemes of transition functions of invertible automata without branches with three states

Theorem 18 allowed us to describe the groups defined by invertible automata without branches with three states.

Definition 21. *We call two transition functions $\pi_1, \pi_2 : X \times Q \to Q$ equivalent, if there exists a permutation $\theta \in S_Q$ such that*

$$\pi_1(x, q) = \theta^{-1}\pi_2(x, \theta(q)) \quad \forall x \in X, q \in Q$$

For automata without branches this equation is $s(q_i) = \theta^{-1}s(\theta(q_i))$.

There are 7 equivalence classes of transition functions of invertible automata without branches with three states. They can be described with the help of schemes (see Figure 2). The cross signs denotes rest states; the dot signs denotes unconditional jump states. The arrows indicate action of transition function. Consider for example automata with transition function corresponding to Scheme 7.

Scheme 7. *Let $t_i = \lambda_{q_i} \in Z_2$.*

$$A = \begin{pmatrix} t_0 & t_1 & t_0 \\ t_1 & t_0 & t_1 \\ t_2 & t_1 & t_0 \end{pmatrix}$$

If $t_0 = 0$, $t_1 = 0$, $t_2 = 1$, then the rank equals 1.
If $t_0 = 0$, $t_1 = 1$, $t_2 = 0$, then the rank equals 2.
If $t_0 = 0$, $t_1 = 1$, $t_2 = 1$, then the rank equals 3.
If $t_0 = 1$, $t_1 = 0$, $t_2 = 0$, then the rank equals 2.
If $t_0 = 1$, $t_1 = 0$, $t_2 = 1$, then the rank equals 2.
If $t_0 = 1$, $t_1 = 1$, $t_2 = 0$, then the rank equals 2.
If $t_0 = 1$, $t_1 = 1$, $t_2 = 1$, then the rank equals 1.

3.2 Semigroups defined by automata without branches

Let $v^* = vvv\ldots$, where $v \in (T_X)^n$, $v^* \in (T_X)^\omega$. We can associate each word uv having the length $n+m$ ($|u| = n$, $|v| = m$) with the map $P_{uv} = F_{uv^*}$.

Lemma 22. *The composition of the invertible maps P_{uv} and P_{sw} is the map $P_{uv \circ sw}$, where $u, s \in (T_X)^n$, $v, w \in (T_X)^m$, and by $\circ$ we denote element by element composition of vectors.*

Proof. The proof is straightforward. □

For semigroups defined by automata we can formulate a theorem being a rough analogue to Lemma 20.

Theorem 23. *Let U be an automaton without branches and let n be the number of its states. Let m be the least common multiple of all lengths of periods of sequences $\left\{s^i(q_k)\right\}_{i=n}^{\infty}$, $k = 0, \ldots, n-1$, and let $l = n+m$.*

Then each transformation defined by U is representable in the form P_w, where $w = \left(\lambda_q, \lambda_{s(q)}, \ldots, \lambda_{s^{l-1}(q)}\right) \in (T_X)^l$. Therefore, the semigroup defined by U is isomorphic to the semigroup

$$sg\left(\left(\lambda_{q_0}, \lambda_{s(q_0)}, \ldots, \lambda_{s^{l-1}(q_0)}\right), \ldots, \left(\lambda_{q_n}, \lambda_{s(q_n)}, \ldots, \lambda_{s^{l-1}(q_n)}\right)\right)$$

where $sg(g_0, \ldots, g_n)$ is the semigroup generated by $g_0, \ldots, g_n$.

Proof. The semigroup defined by U is generated by the transformations f_i, which, by Lemma 17, are representable in the form F_{uw} where $|u| = n$, $w \in X^\omega$ is a periodic word, $uw = \left(\lambda_{q_i}, \lambda_{s(q_i)}, \ldots, \lambda_{s^{l-1}(q_i)}, \ldots\right)$. By the definition of m, f_i are representable in the form P_{uv}, where $|u| = n$, $|v| = m$. Finally, the isomorphism follows from Lemma 22. □

3.3 Semigroups defined by automata without branches over two-symbol alphabets

Automaton transformations over the two-symbol alphabet $X = \{0, 1\}$ are uniquely determined by vectors u of length l the components of which belong to

$$T_X = T_2 = \left\{\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \beta = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, id = \varepsilon = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, inv = \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}$$

By Lemma 22, the composition of transformations corresponds to the element-by-element composition of vectors. So we reduce study of semigroups defined by automata without branches to study of semigroups of vectors the elements of which belong to T_2.

Let f, g be transformations defined by an arbitrary automaton without branches over two-symbol alphabet. The relationships $fff = f$, $fgff = fg$ are true.

We established by numerical experiments that the semigroups of automaton transformations defined by automata without branches with 3 states over the two-symbol alphabet have the following 19 orders (numbers of elements): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 18, 20, 22, 25, 31. Note that the groups defined by such invertible automata have only one of the following orders: 1, 2, 4, 8.

4 Slow-moving automata

The class of slow-moving automata is very wide and it is a rather complicated thing to investigate algebraic properties of transformations defined by slow-moving automata in a general form. That is why we shall consider one more class of automata, namely *automata of finite type* and investigate the transformations defined by slow-moving automata of that class.

4.1 Automata of finite type

Definition 24. *We call a finite automaton A a finite type automaton if the sequence of automaton states for any infinite input word and for any initial state will stabilize.*

Definition 25. *A transformation of infinite words $f : X^\omega \to X^\omega$ we call a finite automaton transformation of finite type if there is a finite type automaton defining the transformation f in some initial state.*

It is rather easy to determine whether the given automaton is a finite type one by its Moore diagram.

Proposition 26. *A finite automaton is an automaton of finite type if and only if its Moore diagram is an oriented graph containing no oriented cycles besides the loops.*

Proof. Necessity. Let us suppose that the Moore diagram of a finite automaton contains an oriented cycle:

$$q_{i_1}, q_{i_2}, \ldots, q_{i_k}, q_{i_1}$$

Let the automaton start work from the state q_{i_1}. Then there is a sequence of input symbols such that the automaton will subsequently be in the states

$$q_{i_1}, q_{i_2}, \ldots, q_{i_k}, q_{i_1}, q_{i_2}, \ldots, q_{i_k}, q_{i_1}, \ldots$$

Therefore, the sequence of states is not stabilized.

Sufficiency. Let us take an initial state and a sequence of input symbols. Denote the respective sequence of automaton states by $\{q_{i_k}\}_{k=1}^{\infty}$. If the automaton was in some state q and then went to some other state then it will not be able to return to the state q (since its Moore diagram does not contain oriented cycles besides the loops). Consequently, for each state q there is at most one number n such that $q = q_{i_n} \neq q_{i_{n+1}}$, which means that there are only finitely many numbers n for which $q_{i_n} \neq q_{i_{n+1}}$, that is the sequence $\{q_{i_k}\}_{k=1}^{\infty}$ is stabilized. □

Note that the product of two slow-moving automata (transformations) is not necessarily a slow-moving automaton (transformation), see Example 14. In contrast to the class of slow-moving automata the class of automata of finite type is closed with respect to the product.

Proposition 27.

1. *The product of two automata of finite type is an automaton of finite type again.*
2. *The automaton inverse to an invertible automaton of finite type will be of finite type*

Proof. Statement 1 follows from the definition of the automata product: if the sequence of the first automaton states is stabilized at the state q_1 at the n-th step, and that of the second one is stabilized at the state q_2 at the m-th step, then the sequence of the states of the product is stabilized at the state (q_1, q_2) at the step with number $\max(m, n)$.

Statement 2 Let A be an invertible automaton of finite type. By Proposition 26 its Moore diagram contains no oriented cycles besides the loops. Then the Moore diagram of the inverse automaton of A contains no oriented cycles besides the loops, so it is also an automaton of finite type. □

Corollary 28. *The set of all finite automaton transformations of finite type is a subsemigroup of the semigroup of all finite automaton transformations.*

Corollary 29. *The set of all invertible finite automaton transformations of finite type is a subgroup of the group of all invertible finite automaton transformations.*

4.2 Transformations Defined by Invertible Slow-moving Automata of Finite Type over Two-symbol Alphabets

In this section we shall consider only invertible slow-moving automata of finite type over the two-symbol alphabet $X = \{0, 1\}$. We have studied the algebraic properties of transformations defined by such automata. We have also found a family of slow-moving transformations of finite type such that any other one is a composition of members of this family.

To describe the transformations defined by such automata we shall need special operators acting on the set of all transformations of infinite words $T_{X^\omega} = \{f | f : X^\omega \to X^\omega\}$. Let p be some substitution from the set $S_X = \{id, inv\}$ (here id is an identical substitution, inv is a transposition). For convenience of notation extend the action of p substitution to the sets X^*, X^ω symbol by symbol:

$$p(x_1 x_2 \dots x_n) = p(x_1)\, p(x_2) \dots p(x_n)\,,\ p(x_1 x_2 \dots x_n \dots) = p(x_1)\, p(x_2) \dots p(x_n) \dots$$

Let $f \in T_{X^\omega}$. We will denote by $p0]f$ the mapping which acts on an input word as a p substitution up to the first occurrence of zero (including it), and then as an f transformation. We can consider $p0]$ as the operator of the form

$$p0] : T_{X^\omega} \to T_{X^\omega}$$

Definition 30. *Let $f \in T_{X^\omega}$. Then $p0]f = g$ is the transformation which acts by the rule*

$$g\,(1^n 0w) = p\,(1^n 0)\, f\,(w)\,,\ \forall w \in X^\omega, n \geq 0, \quad g\,(1^*) = 1^*$$

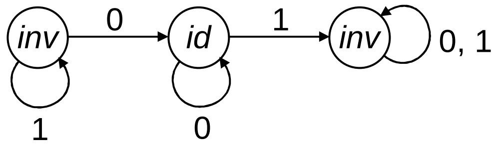

Figure 3: A slow-moving finite state automaton defining the transformation $inv0]id1]inv$.

Here 1^* is the infinite word composed of the symbol 1. In other words g acts up to the first zero (including it) by p substitution, and then by f transformation.

The operators

$$p1] : T_{X^\omega} \to T_{X^\omega}$$

are defined similarly.

Definition 31. *Let $f \in T_{X^\omega}$. Then $p1]f = g$ is the transformation which acts by the rule*

$$g\left(0^n 1 w\right) = p\left(0^n 1\right) f\left(w\right), \forall w \in X^\omega, n \geq 0, \quad g\left(0^*\right) = 0^*$$

Let us denote the set of all such operators by $W_G = \{p0], p1] | p \in S_X\}$.

Example 32. A slow-moving transformation $s = inv0]id1]inv$ transforms the words from X^ω as follows. All the symbols up to the first zero (inclusive) are inverted, then until the first one (after the first zero), inclusively, all symbols will remain unchanged, and the rest of the symbols will be inverted again.

This transformation is defined by the automaton shown in Figure 3.

Any transformations defined by *invertible* slow-moving finite state automata can be represented with the help of the above-mentioned operators.

Proposition 33. *Let A be a slow-moving invertible finite state automaton. Then any transformation f defined by it can be represented in the form*

$$f = h_1 h_2 \dots h_k p, \text{ where } h_i \in W_G,\ p \in S_X,\ k \geq 0. \tag{3}$$

The converse is also true: if the transformation f can be represented in the form (3), then it can be defined by a slow-moving invertible automaton of finite type.

Proof. Let A be an invertible slow-moving automaton of finite type. Remove from its Moore diagram all the loops. Then there will be no more than one arc going from each vertex (since all the states are waiting states or rest states).

In addition the obtained graph will not contain any oriented cycles (since A is an automaton of finite type).

Let us fix some initial state q_1 of the automaton. Let us move along the graph beginning from its vertex q_0 until we reach the vertex without edges coming from it (sooner or later it will happen since the number of vertices is finite and we cannot be twice in one and the same vertex). While doing it we shall visit vertices corresponding to the waiting states $q_1, q_2, \ldots, q_k$ and to the rest state q_{k+1}, where $k \geq 0$. Let q_i be the x_i-waiting state and let the corresponding output function be given by the permutation p_i, where $1 \leq i \leq k$. Let p be the output function corresponding to the rest state q_{k+1}. Then the transformation f defined by the automaton A in its initial state q_1 can be represented in the form $f = h_1 h_2 \ldots h_k p$, where $h_i = p_i x_i]$.

Let us prove the converse statement. Let the transformation f be represented in the form $f = h_1 h_2 \ldots h_k p$, where $h_i = p_i x_i]$. Then the automaton with the x_i-waiting states q_i $(1 \leq i \leq k)$ and output functions p_i together with the rest state q_{k+1} and the output function p will define the transformation f. $\square$

To formulate the properties of the introduced operators we shall need one more denotation for them. Let $p \in S_X$, $x \in X$. Set

$$px] = \begin{pmatrix} p\,(x) \\ x \end{pmatrix}.$$

Let us agree that $p^0 = id$, and $p^1 = p$, $p \in S_X$.

Example 34. A slow-moving transformation

$$s = inv0]id1]id0]inv1]id1]inv \tag{4}$$

may also be represented in the form

$$s = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} inv. \tag{5}$$

From notation (4) it is clear how exactly the transformation acts, and what automaton defines it. However, notation in the form (5) turns out to be more convenient in many cases, for example, when one has to find a composition of two transformations or turn to the inverted transformation.

Proposition 35. *The operators from the set W_G have the following properties:*

1. *Bijective transformation under the action of the operator in the form $p0]$ or $p1]$ turn into a bijective one, and a finite automaton transformation into a finite automaton one.*
2. $px_1]px_2]\ldots px_k]p = p$, $\forall p \in S_X, x_i \in X, i = \overline{1,k}$.
3. $\begin{pmatrix} a \\ b \end{pmatrix} f \circ \begin{pmatrix} b \\ c \end{pmatrix} g = \begin{pmatrix} a \\ c \end{pmatrix} (f \circ g)$, $\forall f, g \in T_{X^\omega}, a, b, c \in X$.
4. $\begin{pmatrix} a \\ a \end{pmatrix} (f \circ g) = \begin{pmatrix} a \\ a \end{pmatrix} f \circ \begin{pmatrix} a \\ a \end{pmatrix} g$, $\forall f, g \in T_{X^\omega}, a \in X$.
5. $\left[\begin{pmatrix} a \\ b \end{pmatrix} f\right]^{-1} = \begin{pmatrix} b \\ a \end{pmatrix} f^{-1}$, $\forall f \in T_{X^\omega}$, *$f$ is bijective.*

6. $inv^x \circ \begin{pmatrix} a \\ b \end{pmatrix} f \circ inv^y = \begin{pmatrix} a+x \\ b+y \end{pmatrix} (inv^x \circ f \circ inv^y)$, $\forall f \in T_{X^\omega}, a, b, x, y \in X$, *addition here and further on is taken modulo 2.*

Proof. Property 2 follows directly from the definition of the operator $px]$.

Let us prove *Property 3.* Let $\begin{pmatrix} a \\ b \end{pmatrix} = p_1 b]$, that is $a = p_1(b)$, and $\begin{pmatrix} b \\ c \end{pmatrix} = p_2 c]$, that is $b = p_2(c)$. Let us consider the action of the transformation $\begin{pmatrix} a \\ b \end{pmatrix} f \circ \begin{pmatrix} b \\ c \end{pmatrix} g$ on the word $w \in X^\omega$ in the next two cases

$$1)\ w = \bar{c}^n c w_1 \quad \text{and} \quad 2)\ w = \bar{c}^*,$$

Here and further on $\bar{c}$ is the symbol which is not equal to c, i. e. $1-c$, $\bar{c}^*$ is an infinite word consisting only of the symbol $\bar{c}$, $c \in X$, $w_1 \in X^\omega$

$$1)\quad \left[\begin{pmatrix} a \\ b \end{pmatrix} f \circ \begin{pmatrix} b \\ c \end{pmatrix} g\right] (\bar{c}^n c w_1) = (p_1 b] f \circ p_2 c] g) (\bar{c}^n c w_1) =$$
$$= (p_1 b] f) (p_2 (\bar{c}^n c)\, g(w_1)) = (p_1 b] f) \left(p_2 (\bar{c})^n\, p_2 (c)\, g(w_1)\right) = (*)$$

Note that $p_2(c) = b$, therefore $p_2(\bar{c}) = \bar{b}$ (since p_2 is injective). Then $(*) = (p_1 b] f) \left(\bar{b}^n b g(w_1)\right) = p_1 \left(\bar{b}\right)^n p_1(b)\, f(g(w_1)) = p_1 (p_2(\bar{c}))^n\, p_1(p_2(c))\, f(g(w_1)) = [(p_1 \circ p_2)\, c]\, (f \circ g)] (\bar{c}^n c w_1) = \left[\begin{pmatrix} p_1(p_2(c)) \\ c \end{pmatrix} (f \circ g)\right] (\bar{c}^n c w_1) = \left[\begin{pmatrix} a \\ c \end{pmatrix} (f \circ g)\right] (\bar{c}^n c w_1)$

$$2)\quad \left[\begin{pmatrix} a \\ b \end{pmatrix} f \circ \begin{pmatrix} b \\ c \end{pmatrix} g\right] (\bar{c}^*) = (p_1 b] f \circ p_2 c] g) (\bar{c}^*) = (p_1 b] f) \left(p_2 (\bar{c})^*\right) =$$
$$(p_1 b] f) \left(\bar{b}^*\right) = p_1 \left(\bar{b}\right)^* = p_1 (p_2 (\bar{c}))^* = ((p_1 \circ p_2)\, c]\, (f \circ g)) (\bar{c}^*) =$$
$$\left(\begin{pmatrix} p_1(p_2(c)) \\ c \end{pmatrix} (f \circ g)\right) (\bar{c}^*) = \left(\begin{pmatrix} a \\ c \end{pmatrix} (f \circ g)\right) (\bar{c}^*)$$

Properties 4 and 5 follow directly from *Property 3.*

To prove *Property 6* we shall use the relationships (6), which follow from *Property 1*:

$$inv^x = \begin{pmatrix} a+x \\ a \end{pmatrix} inv^x; \quad inv^y = \begin{pmatrix} b \\ b+y \end{pmatrix} inv^y \tag{6}$$

From (6), applying *Property 3*, we obtain the required relationship.

The first statement of *Property 1* follows from the already proved *Property 5.*

Let us prove that a finite automaton transformation f under the action of the operator $px] \in W_G$ turns into a finite automaton one. Let f be defined by some finite initial automaton A_q (with initial state q).

Let us add to the set of states of this automaton a new state q_0. At the same time let us extend the transition function at this state by $\pi(\bar{x}, q_0) = q_0$; $\pi(x, q_0) = q$ and the output function by $\lambda(\bar{x}, q_0) = \lambda(x, q_0) = p(x)$. It is evident that q_0 will be an x-waiting state. Let us choose this state the initial one. Then the obtained initial automaton A'_{q_0} will determine the transformation f. ☐

It follows from Property 2 of Proposition 35 that the representation (3) for slow-moving transformation of finite type is not single-valued but it could be always brought to the form:

$$p_1x_1]p_2x_2]\dots p_kx_k]p, \text{ where } p\neq p_k \quad p,p_i\in S_X, \quad x_i\in X, \quad i=\overline{1,k} \tag{7}$$

Let us call the representation (7) *canonical*.

Proposition 36. *Every slow-moving transformation of finite type has exactly one canonical representation.*

Proof. Assume that the transformation f have two different canonical representations:

$$f=p_1x_1]p_2x_2]\dots p_kx_k]p=p'_1x'_1]p'_2x'_2]\dots p'_{k'}x'_{k'}]p'$$

Let us suppose that there exists a number l such that $\forall i<l:\ p_i=p'_i,\ x_i=x'_i$, and $p_l\neq p'_l$ or $x_l\neq x'_l$. Otherwise we have $k\neq k'$ (without loss of generality we may assume $k<k'$) and $\forall i=\overline{1,k}:\quad p_i=p'_i,\ x_i=x'_i$. This case will be considered later.

Note that the situation $k=k',\quad \forall i=\overline{1,k}:\quad p_i=p'_i,\ x_i=x'_i$ and $p\neq p'$ is impossible since one of the representations will not be canonical.

If $p_l\neq p'_l$, it is easily seen that

$$\begin{aligned}f\left(x_1x_2\dots x_{l-1}aw\right)&=\left(p_1x_1]p_2x_2]\dots p_kx_k]p\right)\left(x_1x_2\dots x_{l-1}aw\right)=\\&=p_1(x_1)p_2(x_2)\dots p_{l-1}(x_{l-1})p_l(a)u\\f\left(x_1x_2\dots x_{l-1}aw\right)&=\left(p'_1x'_1]p'_2x'_2]\dots p'_kx'_k]p'\right)\left(x_1x_2\dots x_{l-1}aw\right)=\\&=p'_1(x_1)p'_2(x_2)\dots p'_{l-1}(x_{l-1})p'_l(a)u'\end{aligned}$$

where $a\in X$, $w,u,u'\in X^\omega$. This is impossible since $p_l\left(a\right)\neq p'_l\left(a\right)$. If $p_l=p'_l=p_0$, then we shall find a maximal number m such that $p_0=p_l=p_{l+1}=\ldots=p_m,\quad m\leq k$ (if $m<k$, then $p_m\neq p_{m+1}$).

Similarly, m' is a maximal number such that $p'_l=p'_{l+1}=\ldots=p'_{m'}$. Let us assume that $m-l\leq m'-l$, the case $m-l\geq m'-l$ can be treated in a similar way. Then it is not difficult to see that

$$\begin{aligned}f\left(x_1x_2\dots x_{l-1}x_l\dots x_maw\right)&=\left(p_1x_1]p_2x_2]\dots p_kx_k]p\right)\left(x_1x_2\dots x_{l-1}x_l\dots x_maw\right)=\\&=p_1(x_1)p_2(x_2)\dots p_{l-1}(x_{l-1})p_0\left(x_l\dots x_m\right)r(a)u,\end{aligned}$$

where $r=p_{m+1}$ if $m<k$, and $r=p$ if $m=k$ ($a\in X$, $w,u,u'\in X^\omega$). On the other hand

$$\begin{aligned}f\left(x_1x_2\dots x_{l-1}x_l\dots x_maw\right)&=\left(p'_1x'_1]p'_2x'_2]\dots p'_{k'}x'_{k'}]p'\right)\left(x_1x_2\dots x_{l-1}x_l\dots x_maw\right)=\\&=p'_1(x_1)p'_2(x_2)\dots p'_{l-1}(x_{l-1})p_0\left(x_l\dots x_m\right)p_0(a)u'\end{aligned} \tag{8}$$

which is impossible since $p_0\left(a\right)\neq r\left(a\right)$.

We need only consider the case when $k<k'$ and $\forall i=\overline{1,k}:p_i=p'_i,\ x_i=x'_i$. There are two subcases:

1. $\exists s > k : p'_s \neq p$ and
2. $(\forall s > k : p'_s = p) \,\&\, (p' \neq p)$

In the first subcase let s be the minimal number such that $p'_s \neq p$. In the word $f\,(x'_1 x'_2 \dots x'_s aw)$ the symbol with number $s{+}1$ will be $p'_s\,(a)$ on one side and $p\,(a)$ on the other side. In the second subcase in the word $f\,(x'_1 x'_2 \dots x'_k aw)$ the symbol with number $k{+}1$ will be $p'\,(a)$ on one side and $p\,(a)$ on the other side. Therefore, in any cases we obtain a contradiction. $\square$

Let us consider a family of slow-moving transformations of finite type:

$$\alpha_0 = inv, \quad \alpha_1 = id0]inv, \quad \alpha_2 = id0]id0]inv, \quad \dots, \quad \alpha_n = id0]^n inv, \quad \dots$$

All the α_i are the involutions, that is $\alpha_i^2 = id$. We will show that all the slow-moving transformations of finite type can be represented in the form of compositions of α_i.

Theorem 37. *The following equality holds*

$$\begin{gathered}\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_{n-1}}{b_{n-1}} inv^{a_n} = \\ = \alpha_0^{a_0}\alpha_1^{a_0+a_1}\alpha_2^{a_1+a_2}\dots\alpha_{n-1}^{a_{n-2}+a_{n-1}}\alpha_n^{a_{n-1}+a_n+b_{n-1}}\alpha_{n-1}^{b_{n-1}+b_{n-2}}\dots\alpha_2^{b_2+b_1}\alpha_1^{b_1+b_0}\alpha_0^{b_0} \\ n \geq 1 \end{gathered} \tag{9}$$

Proof. The proof will be made by induction on n.
Base of induction: $n = 1$.

Applying Property 6 of Proposition 35, we obtain

$$\begin{aligned}\binom{a_0}{b_0} inv^{a_1} &= inv^{a_0}\circ inv^{a_0}\circ\binom{a_0}{b_0} inv^{a_1}\circ inv^{b_0}\circ inv^{b_0} = \\ &= inv^{a_0}\circ\binom{a_0+a_0}{b_0+b_0}\left(inv^{a_0}\circ inv^{a_1}\circ inv^{b_0}\right)\circ inv^{b_0} = \\ &= \alpha_0^{a_0}\circ\binom{0}{0}\left(inv^{a_0+a_1+b_0}\right)\circ\alpha_0^{b_0} = \alpha_0^{a_0}\circ\alpha_1^{a_0+a_1+b_0}\circ\alpha_0^{b_0}\end{aligned}$$

If $a_0{+}a_1{+}b_0 = 0$, then $\binom{0}{0}\left(inv^{a_0+a_1+b_0}\right) = id$, otherwise $\binom{0}{0}\left(inv^{a_0+a_1+b_0}\right) = \alpha_1$.
Transition of induction: Suppose that the statement of the theorem is valid for $n = k-1$. Let us prove it for $n = k$:

$$\begin{aligned}&\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_{k-1}}{b_{k-1}} inv^{a_k} = \\ &\qquad = inv^{a_0}\circ inv^{a_0}\circ\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_{k-1}}{b_{k-1}} inv^{a_k}\circ inv^{b_0}\circ inv^{b_0} =\end{aligned}$$

Applying Property 6 of Proposition 35, we obtain

$$= inv^{a_0} \circ \binom{a_0 + a_0}{b_0 + b_0} \left[inv^{a_0} \circ \binom{a_1}{b_1} \cdots \binom{a_{k-1}}{b_{k-1}} inv^{a_k} \circ inv^{b_0} \right] \circ inv^{b_0} =$$

Applying the assumption of induction:

$$= inv^{a_0} \circ \binom{0}{0} \left[inv^{a_0} \circ \alpha_0^{a_1} \alpha_1^{a_1+a_2} \alpha_2^{a_2+a_3} \dots \alpha_{k-2}^{a_{k-2}+a_{k-1}} \alpha_{k-1}^{a_{k-1}+a_k+b_{k-1}} \circ \right.$$

$$\left. \circ\, \alpha_{k-2}^{b_{k-1}+b_{k-2}} \dots \alpha_2^{b_3+b_2} \alpha_1^{b_2+b_1} \alpha_0^{b_1} \circ inv^{b_0} \right] \circ inv^{b_0} =$$

$$= \alpha_0^{a_0} \circ \binom{0}{0} \left[\alpha_0^{a_0+a_1} \alpha_1^{a_1+a_2} \alpha_2^{a_2+a_3} \dots \alpha_{k-2}^{a_{k-2}+a_{k-1}} \alpha_{k-1}^{a_{k-1}+a_k+b_{k-1}} \circ \right.$$

$$\left. \circ\, \alpha_{k-2}^{b_{k-1}+b_{k-2}} \dots \alpha_2^{b_3+b_2} \alpha_1^{b_2+b_1} \alpha_0^{b_1+b_0} \right] \circ \alpha_0^{b_0} =$$

Applying Property 4 of Proposition 35 and the relationship $\binom{0}{0} \alpha_i = \alpha_{i+1}$, we obtain

$$= \alpha_0^{a_0} \alpha_1^{a_0+a_1} \alpha_2^{a_1+a_2} \dots \alpha_{k-1}^{a_{k-2}+a_{k-1}} \alpha_k^{a_{k-1}+a_k+b_{k-1}} \alpha_{k-1}^{b_{k-1}+b_{k-2}} \dots \alpha_2^{b_2+b_1} \alpha_1^{b_1+b_0} \alpha_0^{b_0}.$$

□

Thus, a slow-moving transformation of finite type can be represented as follows:

$$s = \alpha_{i_1} \alpha_{i_2} ... \alpha_{i_k}, \tag{10}$$

where

(10.1) $i_r \neq i_{r+1}$ for all $r = \overline{1,k}$ and

(10.2) there exists an m, so that $i_p < i_q$, if $p < q \leq m$, and $i_p > i_q$, if $m \leq p < q$.

On the contrary, if $\{i_r\}_{r=1}^k$ is the sequence of nonnegative integers satisfying conditions (10.1) and (10.2), then it follows from Theorem 37 that the transformation $s = \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}$ is slow-moving of finite type (it is not difficult to select the corresponding a_i, $b_i \in Z_2$).

4.3 Noninvertible slow-moving automata of finite type

Let us consider the slow-moving automata of finite type over the two-symbol alphabet $X = \{0, 1\}$ being a generalization of the corresponding invertible automata studied in Section 4.2. To describe the transformations defined by such automata, we need to extend the set of the operators considered in Section 4.2.

Let p be some transformation from the set $T_X = T_2 = \{id = \varepsilon, inv = \sigma, \alpha, \beta\}$. Extend the action of the transformation p to the sets X^* and X^ω symbol by symbol as in Section 4.2.

The operators $p0]$ and $p1]$ are introduced similarly as in Section 4.2:

$$p0] : T_{X^\omega} \to T_{X^\omega}, \quad p0]f = g,$$

where g acts according to the rule

$$g\left(1^n 0w\right) = p\left(1^n 0\right) f\left(w\right), \forall w \in X^\omega, n \geq 0, \quad g\left(1^*\right) = p\left(1^*\right)$$

and

$$p1] : T_{X^\omega} \to T_{X^\omega}, \quad p1]f = g,$$

where g acts according to the rule

$$g\left(0^n 1w\right) = p\left(0^n 1\right) f\left(w\right), \forall w \in X^\omega, n \geq 0, \quad g\left(0^*\right) = p\left(0^*\right).$$

Set $W_S = \{px]|p \in T_2, x \in X\} = \{p0], p1]|p \in T_2\}$. It is evident that $W_G \subset W_S$.

Proposition 38. *Let A be a slow-moving automaton of finite type. Then any transformation f defined by it can be represented in the form*

$$f = h_1 h_2 \dots h_k p, \text{ where } h_i \in W_S, p \in T_2, k \geq 0 \tag{11}$$

The inverse statement is also true: if the transformation f can be represented in the form (11), then it can be defined by a slow-moving automaton of finite type.

Proof. The proof is similar to that of Proposition 33. □

Let us introduce one more notation for the operators from W_S:

$$px] = \begin{pmatrix} a \\ p\left(x\right) \\ x \end{pmatrix}, a = \begin{cases} 1, & p \in \{\alpha, \beta\} \\ 0, & p \in \{id, inv\} \end{cases}$$

The notation of the form $\begin{pmatrix} 0 \\ a \\ b \end{pmatrix}$ corresponds to the notation $px] = \begin{pmatrix} a \\ b \end{pmatrix} \in W_G$ of Section 4.2. Set $p^0 = id$, and $p^1 = p$, $p \in T_2$. Let $\overline{x} = 1 - x$, $x \in X = \{0, 1\}$.

Proposition 39. *The following properties hold for the operators from W_S:*

1. *Finite automaton transformations turn into finite automaton transformations under the action of operators of the form $p0]$ or $p1]$.*
2. $px_1]px_2] \dots px_k]p = p$, *for all* $p \in T_2, x_i \in X, i = \overline{1, k}$.
3. *for all* $g \in T_{X^\omega}$, $a, b \in X$, $x \in X^\omega$, $n \geq 0$

$$\left(\begin{pmatrix} 0 \\ a \\ b \end{pmatrix} g\right)\left(\overline{b}^n bx\right) = \overline{a}^n ag\left(x\right), \quad \left(\begin{pmatrix} 0 \\ a \\ b \end{pmatrix} g\right)\left(\overline{b}^*\right) = \overline{a}^*,$$

4. for all $g \in T_{X^\omega}$, $a, b \in X$, $x \in X^\omega$, $n \geq 0$

$$\left(\begin{pmatrix}1\\a\\b\end{pmatrix} g\right)\left(\overline{b}^n bx\right) = a^{n+1} g(x), \quad \left(\begin{pmatrix}1\\a\\b\end{pmatrix} g\right)\left(\overline{b}^*\right) = a^*$$

5. $\begin{pmatrix}d\\a\\b\end{pmatrix} f \circ \begin{pmatrix}0\\b\\c\end{pmatrix} g = \begin{pmatrix}d\\a\\c\end{pmatrix} (f \circ g), \quad \forall f, g \in T_{X^\omega}, a, b, c \in X.$

6. $inv^x \circ \begin{pmatrix}d\\a\\b\end{pmatrix} f \circ inv^y = \begin{pmatrix}d\\a+x\\b+y\end{pmatrix} (inv^x \circ f \circ inv^y), \quad \forall f \in T_{X^\omega}, a, b, x, y \in X,$
the addition here and further on is taken modulo 2.

Proof.

1. The proof is similar to that of Property 1 for the operators from W_G.
2. The proof follows from the definition of $px]$.
3. Let $p \in \{id, inv\}$, $p(b) = a$, $p\left(\overline{b}\right) = \overline{a}$. Then $pb] = \begin{pmatrix}0\\a\\b\end{pmatrix}$, hence from the definition of $pb]$ the property follows.
4. Let $p \in \{\alpha, \beta\}$,$p(b) = p\left(\overline{b}\right) = a$. Then $pb] = \begin{pmatrix}1\\a\\b\end{pmatrix}$, hence from the definition of $pb]$ the property follows.
5. Let us consider the action of the left and right sides of equality on words of the form $\overline{c}^n cx$, where $n \geq 0$, $x \in X^\omega$ and $c^* = cc\ldots$

   Using properties 3 and 4 we obtain:

$$\left[\begin{pmatrix}d\\a\\b\end{pmatrix} f \circ \begin{pmatrix}0\\b\\c\end{pmatrix} g\right](\overline{c}^n cx) = \begin{pmatrix}d\\a\\b\end{pmatrix} f\left[\begin{pmatrix}0\\b\\c\end{pmatrix} g(\overline{c}^n cx)\right] = \begin{pmatrix}d\\a\\b\end{pmatrix} f\left(\overline{b}^n bg(x)\right) =$$

$$= \begin{cases}\overline{a}^n af(g(x)), & d = 0\\ a^{n+1} f(g(x)), & d = 1\end{cases} = \begin{cases}\overline{a}^n a(f \circ g)(x), & d = 0\\ a^{n+1}(f \circ g)(x), & d = 1\end{cases} = \begin{pmatrix}d\\a\\c\end{pmatrix} (f \circ g)(\overline{c}^n cx)$$

$$\left[\begin{pmatrix}d\\a\\b\end{pmatrix} f \circ \begin{pmatrix}0\\b\\c\end{pmatrix} g\right](\overline{c}^*) = \begin{pmatrix}d\\a\\b\end{pmatrix} f\left[\begin{pmatrix}0\\b\\c\end{pmatrix} g(\overline{c}^*)\right] = \begin{pmatrix}d\\a\\b\end{pmatrix} f\left(\overline{b}^*\right) =$$

$$= \begin{cases}\overline{a}^*, & d = 0\\ a^*, & d = 1\end{cases} = \begin{pmatrix}d\\a\\c\end{pmatrix} (f \circ g)(\overline{c}^*)$$

6. By Property 2, $\begin{pmatrix} 0 \\ a+x \\ a \end{pmatrix} inv^x = inv^x a]inv^x = inv^x$; $\begin{pmatrix} 0 \\ b \\ b+y \end{pmatrix} inv^y = inv^y b]iny^y = inv^y$. We have $\begin{pmatrix} d \\ a \\ b \end{pmatrix} f \circ inv^y = \begin{pmatrix} d \\ a \\ b \end{pmatrix} f \circ \begin{pmatrix} 0 \\ b \\ b+y \end{pmatrix} inv^y = \begin{pmatrix} d \\ a \\ b+y \end{pmatrix} (f \circ inv^y)$. If $x = 0$, then Property 6 turns into the last equality. Otherwise, if $d = 0$ then Property 5 gives

$$inv^x \circ \begin{pmatrix} 0 \\ a \\ b \end{pmatrix} f \circ inv^y = \begin{pmatrix} 0 \\ a+x \\ a \end{pmatrix} inv^x \circ \begin{pmatrix} 0 \\ a \\ b+y \end{pmatrix} (f \circ inv^y) =$$
$$= \begin{pmatrix} 0 \\ a+x \\ b+y \end{pmatrix} (inv^x \circ f \circ inv^y)$$

If $d = 1, x = 1$, then $inv \circ \begin{pmatrix} 1 \\ a \\ b \end{pmatrix} f \circ inv^y = inv \circ \begin{pmatrix} 1 \\ a \\ b+y \end{pmatrix} (f \circ inv^y)$. By the definitions of the operators $\begin{pmatrix} 1 \\ a \\ b+y \end{pmatrix}$ and $\begin{pmatrix} 1 \\ a+1 \\ b+y \end{pmatrix}$ we obtain $inv \circ \begin{pmatrix} 1 \\ a \\ b+y \end{pmatrix} (f \circ inv^y) = \begin{pmatrix} 1 \\ a+1 \\ b+y \end{pmatrix} (inv \circ f \circ inv^y)$, which proves Property 6.

□

Similarly as in Section 4.2, we can introduce the notion of the canonical representation of an arbitrary (not necessarily invertible) slow-moving finite automaton transformation of finite type which is unique.

Let

$$\alpha_0 = inv, \quad \alpha_1 = id0]inv, \quad \alpha_2 = id0]id0]inv, \quad \ldots, \quad \alpha_n = id0]^n inv, \quad \ldots$$
$$\beta_1 = \alpha 0]id, \beta_2 = id0]\alpha 0]id, \beta_3 = id0]id0]\alpha 0]id, \ldots, \beta_n = id0]^{n-1}\alpha 0]id, \ldots$$
$$\gamma_1 = \alpha 0]inv, \gamma_2 = id0]\alpha 0]inv, \gamma_3 = id0]id0]\alpha 0]inv, \ldots, \gamma_n = id0]^{n-1}\alpha 0]inv, \ldots$$
$$\delta_0 = \alpha, \quad \delta_1 = id0]\alpha, \quad \delta_2 = id0]id0]\alpha, \quad \ldots, \quad \delta_n = id0]^n\alpha, \quad \ldots$$
$$\lambda_{1,i} = \alpha_i, \lambda_{2,i} = \beta_{i+1}, \lambda_{3,i} = \gamma_{i+1}, \lambda_{4,i} = \delta_i, i \geq 0$$

It is evident that we have $\lambda_{j,i+1} = id0]\lambda_{j,i} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \lambda_{j,i}, i \geq 0, 1 \leq j \leq 4$.

All α_i are involutions, $\alpha_i^2 = id$, all β_i, δ_i are idempotents, that is $\beta_i^2 = \beta_i, \delta_i^2 = \delta_i$. It is clear that $\alpha_0^2 = id$, $\delta_0^2 = \delta_0$. Let us prove the idempotency of β_1. We have $\beta_1(1^n 0x) = 0^{n+1}x$, $\beta_1^2(1^n 0x) = \beta_1(0^{n+1}x) = \beta_1(00^n x) = 00^n x = \beta_1(1^n 0x)$, $\beta_1(1^*) = 0^* = 00^*, \beta_1^2(1^*) = \beta_1(00^*) = 00^* = \beta_1(1^*)$. Then, $\alpha_i^2 = id0]^i(\alpha_0^2) = id0]^i id = id$, $\beta_i^2 = id0]^{i-1}(\beta_1^2) = id0]^{i-1}\beta_1 = \beta_i$, $\delta_i^2 = id0]^i(\delta_0^2) = id0]^i\delta_0 = \delta_i$. It is evident that γ_i are not idempotents.

Theorem 37 can be generalized to the following: all the slow-moving transformations of finite type can be represented in the form of compositions of $\alpha_i, \beta_i, \gamma_i, \delta_i$ (or which is the same $\lambda_{j,i}, i \geq 0, 1 \leq j \leq 4$).

Theorem 40. *Any slow-moving transformation of finite type $f = h_1 h_2 \dots h_k p$, where $h_i \in W_S$, $p \in T_2$, $k \geq 0$, can be represented in the form*

$$f = f_1 \circ f_2 \circ \dots \circ f_r,\ r > 0,\ f_j \in \{\lambda_{s,i} | i \geq 0, 1 \leq s \leq 4\},\ j = \overline{1,r} \tag{12}$$

More exactly, if $h_i = \begin{pmatrix} c_{i-1} \\ b_{i-1} \\ a_{i-1} \end{pmatrix}$, $a_{i-1}, b_{i-1}, c_{i-1} \in X$, $i = \overline{1,k}$ *then*

$$f = L_0(c_0, a_0, b_0) \circ L_1(c_1, a_1, b_1) \circ \dots \circ L_{k-1}(c_{k-1}, a_{k-1}, b_{k-1}) \circ C_k(p) \circ \\ \circ R_{k-1}(b_{k-1}) \circ \dots \circ R_1(b_1) \circ R_0(b_0) \tag{13}$$

where

$$L_i(c, a, b) = \begin{cases} \alpha_i^a \circ \alpha_{i+1}^a, & \text{if } c = 0 \\ \alpha_i^a \circ \beta_{i+1} \circ \alpha_{i+1}^b, & \text{if } c = 1, a + b = 0 \\ \alpha_i^a \circ \gamma_{i+1} \circ \alpha_{i+1}^b, & \text{if } c = 1, a + b = 1 \end{cases}$$

$$R_i(b) = \alpha_{i+1}^b \circ \alpha_i^b$$

$$C_i(p) = \begin{cases} id, & \text{if } p = id \\ \alpha_i, & \text{if } p = inv \\ \delta_i, & \text{if } p = \alpha \\ \alpha_i \circ \delta_i, & \text{if } p = \beta \end{cases}$$

The form of the function (13) turns into the form of the function (12) by throwing id from the composition (13), except for the case $f = id$.

Proof. We will prove the theorem by induction on the number k.

The base of induction. Let $k = 0$. Then $f = p \in \{id, inv, \alpha, \beta\}$, and

$$id = C_0(id) = \alpha_0 \circ \alpha_0, \quad inv = \alpha_0 = C_0(inv), \quad \alpha = \delta_0 = C_0(\alpha), \\ \beta = inv \circ \alpha = \alpha_0 \circ \delta_0 = C_0(\beta)$$

that is f can be represented in forms (12) and (13).

Suppose that the statement of the theorem holds for $k = l$ and prove it for $k = l + 1$. Let $g = h_2 h_3 \dots h_k p$. Then $f = h_1 g$ and by the induction hypothesis g can be represented as $g = L_0(c_1, a_1, b_1) \circ L_1(c_2, a_2, b_2) \circ \cdots \circ L_{k-2}(c_{k-1}, a_{k-1}, b_{k-1}) \circ C_{k-1}(p) \circ R_{k-2}(b_{k-1}) \circ \cdots \circ R_0(b_1)$. Note that $id0]L_i(c, a, b) = L_{i+1}(c, a, b)$, $id0]R_i(b) = R_{i+1}(b)$, $id0]C_i(p) = C_{i+1}(p)$, therefore

$$id0]g = L_1(c_1, a_1, b_1) \circ L_2(c_2, a_2, b_2) \circ \cdots \circ L_{k-1}(c_{k-1}, a_{k-1}, b_{k-1}) \circ C_k(p) \circ \\ \circ R_{k-1}(b_{k-1}) \circ \cdots \circ R_1(b_1)$$

There are two cases to consider:

Let $h_1 = \begin{pmatrix} 0 \\ a \\ b \end{pmatrix}$. Then

$$\begin{pmatrix} 0 \\ a \\ b \end{pmatrix} g = inv^a \circ \left(inv^a \circ \begin{pmatrix} 0 \\ a \\ b \end{pmatrix} g \circ inv^b \right) \circ inv^b =$$
$$= inv^a \circ \left(\begin{pmatrix} 0 \\ a+a \\ b+b \end{pmatrix} \left(inv^a \circ g \circ inv^b \right) \right) \circ inv^b = \alpha_0^a \circ \left(id0] \left(\alpha_0^a \circ g \circ \alpha_0^b \right) \right) \circ inv^b =$$
$$= \alpha_0^a \circ \alpha_1^a \circ id0]g \circ \alpha_1^b \circ \alpha_0^b = L_0(0, a, b) \circ id0]g \circ R_0(b)$$

from which (13) follows.

Let $h_1 = \begin{pmatrix} 1 \\ a \\ b \end{pmatrix}$. Then

$$\begin{pmatrix} 1 \\ a \\ b \end{pmatrix} g = \begin{pmatrix} 1 \\ a \\ b \end{pmatrix} id \circ \begin{pmatrix} 0 \\ b \\ b \end{pmatrix} g =$$
$$= inv^a \circ \left(inv^a \circ \begin{pmatrix} 1 \\ a \\ b \end{pmatrix} id \circ inv^b \right) \circ inv^b \circ inv^b \circ \left(inv^b \circ \begin{pmatrix} 0 \\ b \\ b \end{pmatrix} g \circ inv^b \right) \circ inv^b =$$
$$= inv^a \circ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \left(inv^a \circ id \circ inv^b \right) \circ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \left(inv^b \circ g \circ inv^b \right) \circ inv^b =$$
$$= \alpha_0^a \circ \alpha 0]inv^{a+b} \circ \alpha_1^b \circ id0]g \circ \alpha_1^b \circ \alpha_0^b = L_0(1, a, b) \circ id0]g \circ R_0(b)$$

from which (13) follows. □

The form (13) is not necessarily minimal. To reduce the number of its elements we can remove from it fragments of the form $\alpha_i \circ \alpha_i$ being equal to id.

Conclusions

In this article we describe groups defined by automata without branches over two-symbol alphabets. Study of semigroups defined by automata without branches is reduced to that of vectors over finite full transformation semigroups. We also study algebraic properties of the transformations defined by slow-moving automata of finite type. We prove that such invertible transformations can be expressed as compositions of members of the family $\{\alpha_i\}$. In the general case, any slow-moving transformation of finite type can be expressed as a composition of α_i, β_i, γ_i, δ_i. Further we need to investigate properties of these transformation families and find all relations between these transformations.

References

[1] B. Csákány, F. Gécseg, *On the groups of automaton permutations*, Kibernetika (Kiev), 1965, No 5, pp. 14–17. (in Russian)

[2] F. Gécseg, *On the groups of one-to-one mappings defined by finite automata*, Kibernetika, Kiev, 1965, No 1, pp. 37–39. (in Russian)

[3] J. Hořejš, *Transformations defined by finite automata*, Probl. kibernetiki, **9** (1963), 23–26. (in Russian)

[4] V. P. Zarovnyi, *Automatonic permutations and group interlacings*, Kibernetika, Kiev, 1965, No. 1, pp. 29–36. (in Russian)

[5] Rostislav I. Grigorchuk, Volodimir V. Nekrashevich, and Vitaliy I. Sushchansky, *Automata, dynamical systems, and groups*, Proceedings of the Steklov Institute of Mathematics, **231** (2000), 128-203.

[6] S.V. Aleshin, *Free semigroup of automata*, Vest. Mosk. Univer. Ser. 1. matem., meh, 1983, 4, pp. 12–14. (in Russian)

[7] A.S. Oliynyk, *On free semigroups of automaton transformations*, Matem. zam, 1998, 63, 2, pp. 248–259. (in Russian)

[8] A.S. Oliynyk, I.I. Reznykov, V.I. Sushchansky, *Transformation semigroups defined by Mealy automata over finite alphabet*, Algerbraic structures and their application: Works of Ukrainian mathematical congress, 2001, pp. 80–99. (in Russian)

[9] I.I. Reznykov, *Mealy automata with two states over two-symbol alphabet, which define finite transformation semigroups*, Visn. Kiyv. Univer. Ser. fiz.-mat. nauk, 2001, 4, pp. 78–86. (in Ukrainian)

[10] I.I. Reznykov, V.I. Sushchansky, *Growth functions of automata with two states over two-symbol alphabet*, Dop. NAN Ukraine, 2002, 2, pp. 76–81. (in Russian)

[11] George H. Mealy, *A method for synthesizing sequential circuits*, Bell System Tech. J. **34**, (1955), 1045–1079

[12] V. M. Glushkov, *The abstract theory of automata*, Russ. Math. Surv., 1961, 16 (5), 1-53.

[13] Ferenc Gécseg, Products of automata, EATCS Monographs on Theoretical Computer Science, 7, Springer-Verlag, Berlin, 1986, viii+107 p.

[14] A.S. Antonenko, E.L. Berkovich, On some algebraic properties of Mealy automata in: Kalmar Workshop on Logic and Computer Science, Szeged, 2003, pp. 59–68.