ON LINEAR AND EXTENDED LINEAR REALIZATION OF GENERALIZED AUTOMATA EXTENSIONS

Bolestaw Mikotajczak*

TR 77-304

Department of Computer Science
Cornell University
Ithaca, New York 14853

* Author on leave from the Technical University of Poznań, Poland. This research has been supported in part by Ministry of Higher Education, Science and Technics Grant.

ON LINEAR AND EXTENDED LINEAR REALIZATION OF GENERALIZED AUTOMATA EXTENSIONS

Bolestaw Mikotajczak*

Summary

The relation between ordinary automata, their fixed analogs of extensions, fixed analogs of generalized state-input extension with fixed mappings on input alphabet and characteristic semigroups are considered. The necessary and sufficient conditions for a fixed analog of an extension and generalized state-input extension with fixed mappings on input alphabets of the ordinary automaton to be linearly realizable over the field GF(p) are given. The equations describing fixed analogs of an extension and generalized state-input extension with fixed mappings on input alphabets are also stated.

---

* Author on leave from the Technical University of Poznań, Poland. This research has been supported in part by Ministry of Higher Education, Science and Technics Grant.

List of symbols:

$GF(p)$	- Galois field with characteristic p
V	- strictly periodic automaton
V^*	- fixed analog of strictly periodic automaton
T,τ	- periods of strictly periodic automata
S,Σ,Ω	- sets of states, inputs and outputs, respectively
M,N	- transition and output functions of an automaton
x,y	- words, sequences of symbols from Σ
$\|x\|$	- length of word x
I	- free input semigroup of an automaton
$\overline{I}$	- characteristic semigroup of an automaton
$\bar{x}$	- equivalence class of $\overline{I}$ containing x
$g,g^0,g^1,\ldots,g^{q-1}$	- state isomorphisms
A,B,C,D,ψ_0	- matrices of linear realization of an automaton
α_1,α_2	- mappings from S and Σ into the set of n-ple and k-ple of elements from GF(p), respectively
$\exists\forall$	- general and particular quantifiers
$\equiv$	- equivalence relation
π	- partition
$\mathcal{A}^1 \times \mathcal{A}^2$	- direct product of automata
$\mathcal{A}^1 \cup \mathcal{A}^2$	- direct sum of automata
G,H,K,P	- groups and subgroups

$T(\mathcal{A}_\sigma)$ - transition graph of an autonomous automaton $\mathcal{A}_\sigma$

(g_i, h_i), $i=0,1,\ldots,q-1$ - state-input isomorphisms

$h(\mathcal{A})$ - h-transformation of $\mathcal{A}$

1. Introduction

The notion of a periodic automaton as a special time-varying automaton was introduced by Gill [4,5]. We shall go into the study of linear and extended linear realizability over the field GF(p) of the fixed analog of extension and generalized state-input extensions with fixed mappings on input alphabet of a class of periodic automata, namely the class of extensions and generalized state-input extensions with fixed mappings on input alphabet. For each periodic automaton V as well as for the special case of a periodic automaton - an ordinary finite automaton - there can be defined a family of new periodic automata, called extensions and generalized state-input extensions with fixed mappings on input alphabet of the periodic automaton, whose periods are multiples of the period of V. The term "extension of a periodic automaton" first appears in [6]. On the other hand the term "time-varying linear automaton" first appears in [2] as a generalization of an ordinary linear automaton. Here the terms "extension and generalized state-input extensions with fixed mappings on input alphabet of an linear automaton" are introduced and their properties are investigated.

First we quote a few definitions to be used later.

A strictly periodic automaton V is a triple (S',Σ,M'), where S' is a finite sequence of finite, nonempty sets called the state sets $S'_0,S'_1,\ldots,S'_{T-1}$, Σ is finite, nonempty set called the input set, M' is a finite sequence of functions called the transition functions $M'_0,M'_1,\ldots,M'_{T-1}$, where

$$M'_t : S'_t \times \Sigma \to S'_{t+1 \pmod T} \qquad \text{for } t \in \{0,1,\ldots,T-1\}.$$

The number T is called the period of V; if T=1, then a periodic automaton reduces to an ordinary finite automaton. The length of word $x = \alpha_0\alpha_1\cdots\alpha_{k-1}$ we denote by $|x| = k$ and understand as a number of literals in this word. The set of all finite sequences of elements from Σ will be denoted by I. The set I, together with the operation of concatenation, is a free semigroup, called the input semigroup. Let R be a relation between elements of I such that xRy if and only if for every $s \in S$ follows $M(s,x) = M(s,y)$. The equivalence class which contains $x \in I$ will be denoted by $\bar{x}$. The set of all such equivalence classes will be denoted by $\bar{I}$. $\bar{I}$ is called a characteristic semigroup of an automaton. Any transition function M'_t can be extended to domain $S'_t \times I$ as follows:

if $M'_t(s,\sigma_0,\sigma_1,\ldots,\sigma_{k-1})$ is defined, then

$M'_t(s,\sigma_0,\sigma_1,\ldots,\sigma_{k-1},\sigma_k) = M'_{t+k(\mathrm{mod}\ T)}(M'_t(s,\sigma_0,\sigma_1,\ldots,\sigma_{k-1}),\sigma_k)$ where

$s \in S'_t$; $\sigma_0,\sigma_1,\ldots,\sigma_k \in \Sigma$ and $t \in \{0,1,\ldots,T-1\}$.

A fixed analog V* of a strictly periodic automaton $V = (S',\Sigma,M')$ is an ordinary automaton (S^*,Σ,M^*), where $S^* = \bigcup_{t=0}^{T-1} S'_t$, and $M^*: S^* \times \Sigma \to S^*$ is a transition function defined for all $s \in S'_t$, $\sigma \in \Sigma$ and $t \in \{0,1,\ldots,T-1\}$ as $M^*(s,\sigma) = M'_t(s,\sigma)$.

Let $V^1 = (S^1,\Sigma,M^1)$ and $V^2 = (S^2,\Sigma,M^2)$ be periodic automata with the same peroid T, and let g be a one-to-one transformation of $S^1 = \bigcup_{t=0}^{T-1} S^1_t$ onto $S^2 = \bigcup_{t=0}^{T-1} S^2_t$ and h a one-to-one transformation of Σ onto Σ such that g transforms S^1_0 onto S^2_0, S^1_1 onto $S^2_1,\ldots,S^1_{T-1}$ onto S^2_{T-1} and for all $s \in S^1_t$ (g,h) satisfies

$$M^2_t(g(s),\sigma) = g(M^1_t(s,h(\sigma)))$$

then (g,h) is called a state-input isomorphism of V^1 onto V^2. If T=1, i.e. if

both V^1 and V^2 reduce to ordinary finite automata, then the definition of the state-input isomorphism reduces to the well known definition [3].

Now we introduce notions and notations associated with generalized periodic sums and generalized extensions of ordinary finite automata.

Let $\mathcal{A}^0 = (S^0,\Sigma,M^0), \mathcal{A}^1 = (S^1,\Sigma,M^1),\ldots,\mathcal{A}^{q-1} = (S^{q-1},\Sigma,M^{q-1})$ be ordinary finite automata and let (ψ^i,ϕ^i), $i = 0,1,\ldots,q-1$ be one-to-one transformation of S^i onto $S^{i+1(\mathrm{mod}\ q)}$ and Σ onto Σ, respectively. A <u>generalized periodic sum of $\mathcal{A}^0,\mathcal{A}^1,\ldots,\mathcal{A}^{q-1}$ associated with transformations (ψ^i,ϕ^i)</u>, $i = 0,1,\ldots,q-1$ is a periodic automaton $V^+ = (S^+,\Sigma,M^+)$ with period equal to $T=q$ where S^+ is a sequence $\bar{S}^0,\bar{S}^1,\ldots,\bar{S}^{q-1}$; M^+ is a sequence $\bar{M}^0,\bar{M}^1,\ldots,\bar{M}^{q-1}$ whereas $\bar{S}^i = S^i$ for $i = 0,1,\ldots,q-1$ $\bar{M}^i(s,\sigma) = \psi^i M^i(s,\phi^i(\sigma))$ for $s \in S^i$ and $\sigma \in \Sigma$. A generalized periodic sum of $\mathcal{A}^0,\mathcal{A}^1,\ldots,\mathcal{A}^{q-1}$ (shortly GPS) will be denoted $V^+ = \mathrm{comp}_{(\psi^i,\phi^i)}(\mathcal{A}^0,\mathcal{A}^1,\ldots,\mathcal{A}^{q-1})$.

If $\phi^i \equiv \phi$ for every $i = 0,1,\ldots,q-1$ then GPS is called <u>generalized periodic sum with fixed mappings on Σ</u> (shortly GPS_ϕ).

If $\phi^i \equiv \phi \equiv \mathrm{id}$ for every $i = 0,1,\ldots,q-1$ then GPS is called <u>ordinary periodic sum</u> or simply <u>periodic sum</u> (shortly PS) (compare [5]).

A <u>shifted generalized periodic sum of $\mathcal{A}^0,\mathcal{A}^1,\ldots,\mathcal{A}^{q-1}$ associated with transformations (ψ^i,ϕ^i)</u>, $i = 0,1,\ldots,q-1$ is a periodic automaton $V^+ = (S^+,\Sigma,M^+)$ with period equal to $T=q$, where S^+ is a sequence $\bar{S}^0,\bar{S}^1,\ldots,\bar{S}^{q-1}$; M^+ is a sequence $\bar{M}^0,\bar{M}^1,\ldots,\bar{M}^{q-1}$ whereas $\bar{S}^i = S^i$ for $i = 0,1,\ldots,q-1$ $\bar{M}^i(s,\sigma) = M^{i+1(\mathrm{mod}\ q)}(\psi^i(s),\phi^i(\sigma))$ for $s \in S^i$ and $\sigma \in \Sigma$. A shifted generalized periodic sum of $\mathcal{A}^0,\mathcal{A}^1,\ldots,\mathcal{A}^{q-1}$ (shortly SGPS) will be denoted $V^+ = \mathrm{comp}^t_{(\psi^i,\phi^i)}(\mathcal{A}^0,\mathcal{A}^1,\ldots,\mathcal{A}^{q-1})$.

If $\phi^i \equiv \phi$ for every $i = 0,1,\ldots,q-1$ then SGPS is called <u>shifted generalized periodic sum with fixed mappings on Σ</u> (shortly SGPA). If $\phi^i \equiv \phi \equiv \mathrm{id}$ for every $i = 0,1,\ldots,q-1$ then SGPS is called <u>shifted periodic sum</u> (shortly SPS).

Let $\mathcal{A}^0 = (S^0,\Sigma,M^0)$ be finite ordinary automaton. A <u>generalized state-input extension of $\mathcal{A}^0$ associated with state-input isomorphisms (g^i,h^i)</u>, $i = 0,1,\ldots,q-1$ is a periodic automaton $V^+ = (S^+,\Sigma,M^+)$ with period equal to $T=q$, where S^+ is a sequence $(S_0^+,S_1^+,\ldots,S_{q-1}^+)$; M^+ is a sequence $(M_0^+,M_1^+,\ldots,M_{q-1}^+)$, whereas

$$S_i^+ = S^i \qquad \text{for } i = 0,1,\ldots,q-1$$

$$M_i^+(s,\sigma) = g^{i+1 \pmod q}(M^0((g^i)^{-1}(s),\ h^i(\sigma))) \text{ for } s \in S_i^+ \text{ and } \sigma \in \Sigma$$

For the sake of convenience V^+ will be denoted $V^+_{,\mathcal{A}^0} = \operatorname{ext}_{(g^i,h^i)} \mathcal{A}^0$ or GSJE.

If $h^i \equiv h$ for every $i = 0,1,\ldots,q-1$ then GSJE is called <u>generalized state-input extension of $\mathcal{A}^0$ with fixed mappings on Σ</u> (shortly GPJE_h).

If $h^i \equiv h \equiv id$ for every $i = 0,1,\ldots,q-1$ then GSJE is called <u>ordinary extension</u> or simply <u>extension</u> (shortly SE or $\operatorname{ext}_{g^i} \mathcal{A}^0$) [10].

<u>A shifted generalized state-input extension of $\mathcal{A}^0$ associated with state-input isomorphisms (g^i,h^i)</u>, $i = 0,1,\ldots,q-1$ is a periodic automaton $V^+ = (S^+,\Sigma,M^+)$ with period equal to $T=q$, where S^+ is a sequence $\bar{S}^0,\bar{S}^1,\ldots,\bar{S}^{q-1}$; M^+ is a sequence $\bar{M}^0,\bar{M}^1,\ldots,\bar{M}^{q-1}$ whereas

$$\bar{S}^i = S^i \qquad \text{for } i = 0,1,\ldots,q-1$$

$$\bar{M}^i(s,\sigma) = M^{(i+1) \bmod q}(g^{(i+1) \bmod q}((g^{i-1})(s)),\ h^{(i+1) \bmod q}(\sigma))$$

for $s \in \bar{S}^i$ and $\sigma \in \Sigma$. A shifted generalized state-input extension of $\mathcal{A}^0$ will be denoted $V^+_{\mathcal{A}^0} = \operatorname{ext}^+_{(g^i,h^i)} \mathcal{A}^0$ (shortly SGSJE).

If $h^i \equiv h$ for every $i = 0,1,\ldots,q-1$ then SGSJE is called <u>shifted generalized state-input extension of $\mathcal{A}^0$ with fixed mappings on Σ</u> (shortly SGSJE_h).

If $h^i \equiv h \equiv id$ for every $i = 0,1,\ldots,q-1$ then SGSJE is called <u>shifted ordinary extension</u> or simply <u>shifted extension</u> (shortly SSE or $\operatorname{ext}^+_{g^i} \mathcal{A}^0$).

From above definitions it is easily seen that generalized state-input extension is a special kind of generalized periodic sum, namely

$$(\psi^i, \phi^i) = (g^{(i+1) \bmod q}_{(g^i)^{-1}}, h^i) \qquad \text{for } i = 0,1,\ldots,q-1.$$

Similarly, extension is a special kind of periodic sum of automata. A periodic automaton V will be called <u>state-input reducible</u> to ordinary automaton $\mathcal{A}$ iff V is a generalized state-input extension of $\mathcal{A}$. A periodic automaton V will be called <u>reducible</u> to ordinary automaton $\mathcal{A}$ iff V is an extension of $\mathcal{A}$.

Let $\mathcal{A} = (S,\Sigma,M)$ be an ordinary automaton. An automaton $h(\mathcal{A}) = (S,\Sigma,M_h)$ is called <u>h-transformation</u> of $\mathcal{A}$ iff h transforms Σ one-to-one and onto Σ and $M_h(s,\sigma) = M(s,h(\sigma))$ for every $s \in S$ and $\sigma \in \Sigma$. An ordinary automaton $\mathcal{A} = (S,\Sigma,M)$ is <u>linearly realizable</u> over the field GF(p) if and only if there exist two injections α_1 and α_2 mapping the sets S and Σ into the sets of n-ple and k-ple of elements from GF(p), respectively, and if there exist two matrices over the field GF(p) A,B such that

$$\alpha_1(M(s,\sigma)) = A\alpha_1(s) + B\alpha_2(\sigma) \qquad (1)$$

for every $s \in S$ and $\sigma \in \Sigma$, where + is additive operation in GF(p). If, instead of (1), the following equation is fullfilled

$$\alpha_1(M(s,\sigma) = A\alpha_1(s) + B\alpha_2(\sigma) + \phi_0 \qquad (2)$$

then we say that $\mathcal{A}$ has <u>extended linear realization</u>.

An automaton $\mathcal{A} = (S,\Sigma,M)$ is called <u>connected</u> if and only if for every ordered pair of states $(s,s') \in S$ there exist a sequence of states $s = s_0, s_1, \ldots, s_{\ell-1} = s'$ of an automaton $\mathcal{A}$ and a sequence of inputs $\sigma_0, \sigma_1, \ldots, \sigma_{\ell-1}$ such that

$$M(s_i,\sigma_i) = s_{i+1} \quad \text{or} \quad M(s_{i+1},\sigma_i) = s_i$$

Let $\mathcal{A}^1 = (S^1,\Sigma,M^1)$ and $\mathcal{A}^2 = (S^2,\Sigma,M^2)$ be two ordinary automata. By the direct sum $\mathcal{A}$ of $\mathcal{A}^1$ and $\mathcal{A}^2$ we understand an automaton (S,Σ,M) such that $S = S^1 \cup S^2$ and

$$\bigwedge_{s \in S} \bigwedge_{\sigma \in \Sigma} \quad M(s,\sigma) = \begin{cases} M^1(s,\sigma) & \text{if } s \in S^1 \\ M^2(s,\sigma) & \text{if } s \in S^2 \end{cases}$$

By the direct product $\mathcal{A}$ of $\mathcal{A}^1$ and $\mathcal{A}^2$ we understand an automaton (S,Σ,M) such that $S = S^1 \times S^2$ and $M = M^1 \times M^2$, and

$$\bigwedge_{(s_1,s_2) \in S^1 \times S^2} \bigwedge_{\sigma \in \Sigma} \quad M^1 \times M^2((s_1,s_2),\sigma) = (M^1(s_1,\sigma),M^2(s_2,\sigma))$$

A partition Π on the set of states S has substitution property if and only if

$$\bigwedge_{s_1,s_2 \in S} \quad s_1 \equiv s_2(\pi) \text{ implies } \bigwedge_{\sigma \in \Sigma} \quad M(s_1,\sigma) \equiv M(s_2,\sigma)(\pi)$$

2. Linear and extended linear realizability of fixed analog of extensions

If $\mathcal{A}^1 = (S^1,\Sigma,M^1)$ and $\mathcal{A}^2 = (S^2,\Sigma,M^2)$ are ordinary automata linearly realizable over the field GF(p), then the direct product and the direct sum are are also linearly realizable over GF(p) (the same is valid for extended linear realizability). Note that when automaton $\mathcal{A}^1 = (S^1,\Sigma,M^1)$ is linearly realizable over the field $GF(p_1)$ and automaton $\mathcal{A}^2 = (S^2,\Sigma,M^2)$ is linearly realizable over the field $GF(p_2)$ $(p_1 \neq p_2)$, then the direct product is not linearly realizable over the field GF(p) for some p. As an example we can give automaton $\mathcal{A}$ (Tab. 1) and automaton $\mathcal{B}$ (Tab. 2). Automaton $\mathcal{A}$ is linearly realizable over GF(3) and automaton $\mathcal{B}$ is linearly realizable over GF(2) but their direct product is linearly realizable over no GF(p).

S \ Σ	0	1
s_1	s_1	s_2
s_2	s_3	s_1
s_3	s_2	s_3

Tab. 1. Automaton $\mathcal{A}$.

S \ Σ	0	1
t_1	t_3	t_2
t_2	t_4	t_1
t_3	t_1	t_4
t_4	t_2	t_3

Tab. 2. Automaton $\mathcal{B}$.

Lemma 1. Let $\mathcal{A} = (S,\Sigma,M)$ be an ordinary automaton, $V_{\mathcal{A}} = (S',\Sigma,M')$ let there be a connected extension of $\mathcal{A}$ associated with isomorphisms $g^0,g^1,\ldots,g^{q-1}$, let $V^*_{\mathcal{A}} = (S^*,\Sigma,M^*)$ be a fixed analog of an extension $V_{\mathcal{A}}$, then the characteristic semigroup $\overline{I(\mathcal{A})}$ of $\mathcal{A}$ is a homomorphic image of the characteristic semigroup $\overline{I(V^*_{\mathcal{A}})}$ of $V^*_{\mathcal{A}}$.

Proof. If $\bar{x} \in \overline{I(\mathcal{A})}$, then $f_x^{\mathcal{A}} = M(s,x)$; similarly, if $y \in \overline{I(V^*_{\mathcal{A}})}$, then $f_y^{V^*_{\mathcal{A}}}(s') = M(s',y)$ for $s \in S$ and $s' \in S$. Function $f_x^{\mathcal{A}}$ maps S into S and function $f_y^{V^*_{\mathcal{A}}}$ maps S'_i into $S'_{i+|y| \pmod q}$ for every $s' \in S'_i$, $i = 0,1,\ldots,q-1$ where $S' = (S'_0,S'_1,\ldots,S'_{q-1})$. Now we introduce a mapping $h: S^* \to S^*$ defined as follows:

$$\bigwedge_{s \in S'_i} \quad \bigwedge_{\bar{x} \in \overline{I(\mathcal{A})}} \quad h(s) = g^{i+|x| \pmod q} f_x^{\mathcal{A}} (g^i)^{-1}(s)$$

We note that $h(s) = f_{\bar{x}}^{V^*_{\mathcal{A}}}(s)$ because $V^*_{\mathcal{A}}$ is connected. We have proved that if $\bar{y} \in \overline{I(V^*_{\mathcal{A}})}$, then $\bar{y} \subseteq \bar{x} \in \overline{I(\mathcal{A})}$. On the other hand, we introduce a sequence of mappings $h^i: S \to S$ for $i=0,1,\ldots,q-1$ defined as follows:

$$\bigwedge_{s \in S} \qquad \bigwedge_{\bar{y} \in \overline{I(V^*_{\mathcal{A}})}} \qquad h^i(s) = (g^{i+|y| \pmod q)-1} f_y^{V^*_{\mathcal{A}}} g^i(s)$$

We note that $h^i(s) = f_y^{\mathcal{A}}(s)$ because $V^*_{\mathcal{A}}$ is connected. We define homomorphism ϕ of the semigroup $\overline{I(V^*_{\mathcal{A}})}$ onto the semigroup $\overline{I(\mathcal{A})}$ as follows:

$$\phi(\bar{y}) = \bar{x} \quad \text{iff} \quad \bar{y} \leq \bar{x}, \quad \text{where } \bar{y} \in \overline{I(V^*_{\mathcal{A}})},\ \bar{x} \in \overline{I(\mathcal{A})}$$

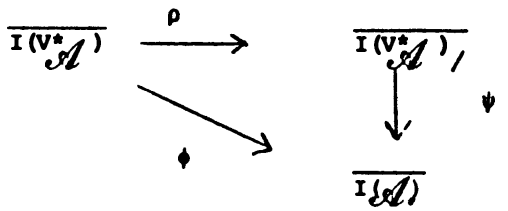
The equivalent definition of the homomorphism ϕ is following:

$$\bigwedge_{\bar{y} \in \overline{I(V^*_{\mathcal{A}})}} \phi(\bar{y}) = \bar{x} \quad \text{iff} \quad \bigwedge_{s \in S} \quad h^i_{\bar{x}}(s) = (g^{i+|y| \pmod q)-1} f_y^{V^*_{\mathcal{A}}} g^i(s)$$

$i=0,1,\ldots,q-1$. With the homomorphism ϕ a partition π on the semigroup $\overline{I(V^*_{\mathcal{A}})}$ is associated such that

$$\bar{y}_1 \equiv \bar{y}_2 \ (\pi) \quad \text{iff} \quad \phi(\bar{y}_1) = \phi(\bar{y}_2)$$

Obviously, the partition π has a substitution property. Therefore, according to the basic theorem on homomorphisms [1], there exists an isomorphism ψ such that



where ρ is a canonical homomorphism. Q.E.D.

Note that any fixed analog of an extension associated with q state isomorphisms of an ordinary automaton $\mathscr{A}$ is isomorphic to the direct product of $\mathscr{A}$ with a nonsingular, connected clock of period q. Hence, if in lemma 1 we reject the assumption of connectedness, we have immediately the following statement: $\mathscr{A}$ is epimorphic image of any fixed analog of extension of $\mathscr{A}$, and therefore there exists a set of homomorphisms from $\overline{I(V^*_{\mathscr{A}})}$ onto $\overline{I(\mathscr{A})}$.

Example 1. The characteristic semigroup $\overline{I(\mathscr{A})}$ for an automaton Fig. 1 is equal to

$$\overline{I(\mathscr{A})} = \{\overline{0},\overline{1},\overline{00},\overline{01},\overline{10},\overline{010}\}$$

and for an automaton $(V^*_{\mathscr{A}})_2$ is equal to $\overline{I(\mathscr{A})}$, as a special case of lemma 1. For $(V^*_{\mathscr{A}})_3$ the characteristic semigroup is equal to

$$\overline{I((V^*_{\mathscr{A}})_3)} = \{\overline{0},\overline{1},\overline{01},\overline{00},\overline{10},\overline{00},\overline{001},\overline{010},\overline{0000},\overline{0001},\overline{0010},\overline{00000},\overline{00001},\overline{00010},\overline{000001},\overline{000010},\overline{000000},\overline{0000010}\}.$$

$\overline{I(\mathscr{A})}$ is isomorphic with the subsemigroup

$$I' = \{\overline{000},\overline{001},\overline{010},\overline{000000},\overline{000001},\overline{000010}\}$$

of $\overline{I((V^*_{\mathscr{A}})_3)}$ and isomorphism is given as follows:

$$\psi = \begin{pmatrix} \overline{0} & \overline{1} & \overline{00} & \overline{01} & \overline{10} & \overline{010} \\ \overline{000} & \overline{001} & \overline{000000} & \overline{000001} & \overline{000010} & \overline{010} \end{pmatrix}$$

Note that in this case $\overline{I(\mathscr{A})}$, $\overline{I((V^*_{\mathscr{A}})_2}$, $\overline{I((V^*_{\mathscr{A}})_3)}$ are groups because $\mathscr{A}$ is a permutation automaton. In general we can state that $\overline{I(\mathscr{A})}$ is isomorphic to the characteristic semigroup $\overline{I(V^*_{\mathscr{A}})}$ if and only if for every $\overline{y} \in \overline{I(V^*_{\mathscr{A}})}$ there exists $x \subseteq \overline{x} \in \overline{I(\mathscr{A})}$ such that $x \in \overline{y}$.

Now we characterize generalized state-input extension of $A^\bullet$ with fixed mappings on Σ with help of h-transformation of $A^\bullet$.

Lemma 2. Let $\mathcal{A}^\bullet = (S,\Sigma,M)$ be ordinary finite automaton and let $h(\mathcal{A}^\bullet) = (S,\Sigma,M_h)$ be its h-transformation; then fixed analogs of generalized state-input extension of $\mathcal{A}^\bullet$ with state-input isomorphisms (g^i,h^{-1}) and of state extension of $h(\mathcal{A}^\bullet)$ with state isomorphisms $\bar{g}^i$ are state isomorphic, namely

$$(\mathrm{ext}_{(g^i,h^{-1})}\mathcal{A}^\bullet)^* = (\mathrm{ext}_{g^i} h(\mathcal{A}^\bullet))^*.$$

Proof. Let $S = \{s_1,s_2,\ldots,s_n\}$ and $\bar{S} = \{\bar{s}_1,\bar{s}_2,\ldots,\bar{s}_n\}$ be sets of states of $\mathcal{A}^\bullet$ and $h(\mathcal{A}^\bullet)$, respectively. Let $\mathrm{ext}_{(g^i,h^{-1})}\mathcal{A}^\bullet = (S',\Sigma,M')$ and $\mathrm{ext}_{\bar{g}^i} h(\mathcal{A}^\bullet) = (\bar{S}',\Sigma,M_h')$ be generalized state-input extension of $\mathcal{A}^\bullet$ associated with fixed mappings on Σ and state extension of $h(\mathcal{A}^\bullet)$, respectively. Let $(\mathrm{ext}_{(g^i,h^{-1})}\mathcal{A}^\bullet)^* = (S'^*,\Sigma,M'^*)$ and $(\mathrm{ext}_{\bar{g}^i} h(\mathcal{A}^\bullet))^* = (\bar{S}'^*,\Sigma,M_h'^*)$ be their fixed analogs. We define state isomorphisms as follows $\theta : S'^* \to \bar{S}'^*$, $\theta(s_j^i) = \bar{s}_j^i$, for $i=0,1,\ldots,q-1$ and $j=1,2,\ldots,n$. Of course θ is one-to-one and onto ($s_j^i = g^i(s_j)$ and $\bar{s}_j^i = \bar{g}^i(\bar{s}_j)$, respectively).

Now we will prove an operation preserving property,

$$\theta(M^i(s_j^i,\sigma)) = \theta(g^{(i+1)\bmod q}\, M((g^i)^{-1}(s_j^i),h^{-1}(\sigma))) =$$

$$= \theta\,(g^{(i+1)\bmod q}\, M(s_j,h^{-1}(\sigma))) = \bar{g}^{(i+1)\bmod q}\, M_h(\bar{s}_j,hh^{-1}(\sigma))) =$$

$$= \bar{g}^{(i+1)\bmod q}\, M_h(\bar{s}_j,\sigma) = M_h^i(\bar{g}^i(\bar{s}_j),\sigma) = M_h^i(\bar{s}_j^i,\sigma) =$$

$$= M_h^i(\theta(s_j^i),\sigma).$$ Q.E.D.

From lemma 2 follows immediately that

$$(\mathrm{ext}_{(g^i,h)} \mathcal{A}^\circ)^* = (\mathrm{ext}_{g^{-i}} h^{-1}(\mathcal{A}^\circ))^*.$$

It means that different algebraic properties of generalized state-input extensions with fixed mappings on Σ can be studied with help of state extensions of h-transformations (compare [6],[10],[11]).

Lemma 3. Let $\mathcal{A} = (S,\Sigma,M)$ and $h(\mathcal{A}) = (\overline{S},\Sigma,M_h)$ be finite automaton and its transformation, respectively. Then $\mathcal{A}$ is linearly realizable over GF(p) iff $h(\mathcal{A})$ is linearly realizable over GF(p) (the same statement is true for extended linear realizability).

Proof. Straightforward and therefore omitted.

Now we quote some additional definitions to be used later.

If S is a set, then functions which map S onto S and one-to-one are called permutations of S. The permutation f is called regular if its arbitrary power is equal to the identity permutation of S, it means that $f^n(s) = s$ for every $s \in S$; or if it does not leave any element of S fixed, it means that $f^n(s) \neq s$ for every $s \in S$ and $n=1,2,\ldots$. The group is called semiregular if it contains only regular permutation of S. We say that permutation group P on set S is a representation of group G if there exists a mapping of group G onto P $g \to \pi(g)$, where $g \in G$ and $\pi(g) \in P$ such that

$$\pi(g_1 g_2) = \pi(g_1)\pi(g_2).$$

Strictly speaking, group P is a homomorphic image of group G. If P is an isomorphic image of group G, then the representation is called faithful. If

every element of S can be mapped onto another arbitrary element of S by a permutation from P, then group P is called transitive and the representation of group G is called a transitive represantation. For an arbitrary subgroup H of group G, group G induces a group of permutations on the set of left cosets of subgroup H; for every $g \in G$

$$\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix} \quad \text{for } x \in G.$$

If H is a subgroup of group G and $g \to \pi(g)$ is the transitive representation of a group G as a permutation group of the left cosets of subgroup H, then elements of subgroup H which are mapped onto identity of the permutation group constitute the greatest normal subgroup N of group contained in H and denoted by N(H) and a permutation group is isomorphic with goutient group $G_{/N(H)}$. Therefore, a representation is faithful if and only if H does not contain normal subgroups except identity. Besides, an arbitrary faithful transitive representation of group G as a permutation group is given exactly up to isomorphism by such a subgroup H which does not contain normal subgroups excluding identity. If G is an abelian group, then all faithful transitive representations of group G as a permutation group are isomorphic because all subgroups are normal in G.

Theorem 1. Let $\mathcal{A} = (S,\Sigma,M)$ be an ordinary automaton, $V^*_{\mathcal{A}} = (S^*,\Sigma,M^*)$ a fixed analog of an extension $V_{\mathcal{A}} = (S',\Sigma,M')$ associated with q state isomorphisms; automaton $V^*_{\mathcal{A}}$ has extended linear realizability over GF(p) if and only if is linearly realizable over GF(p).

Proof. Of course a fixed analog of an extension of an automaton linearly realizable over GF(p) has extended linear realizability over GF(p), since any

autonomous, connected clock of period q is linearly realizable over any finite field.

On the other side, let us consider two possible different cases:

(i) if $\mathcal{A}$ is a nonpermutation automaton,

(ii) if $\mathcal{A}$ is a permutation automaton.

Case (i). Assume that $\mathcal{A}$ is a nonlinear automaton. Then from the assumption and from lemma 1[8] we have for some $\sigma_1 \in \Sigma$

$$M(s_1,\sigma_1)=M(s_2,\sigma_1) \text{ implies } \exists_{\sigma_2 \in \Sigma} \quad M(s_1,\sigma_2)\neq M(s_2,\sigma_2)$$

it means, that equality of the next-state pairs for some input symbols σ_1 does not imply equality of the next-state pairs for some other input symbol σ_2. On the base of property g^i, $i=0,1,\ldots,q-1$ we have

$$g^i(M(s_1,\sigma_1))=g^i(M(s_2,\sigma_1)) \text{ implies } M^i(g^i(s_1),\sigma_1)=M^i(g^i(s_2),\sigma_1) \text{ and, therefore}$$

$$M^i(g^i(s_1),\sigma_1)=M^i(g^i(s_2),\sigma_1) \text{ implies } M^i(g^i(s_1),\sigma_2)\neq M^i(g^i(s_2),\sigma_2)$$

Therefore, V^* is also a nonlinear automaton.

Case (ii). Let $V^*_{\mathcal{A}}$ be a permutation automaton which is linearly realizable over GF(p) (of course an extension of a permutation automaton is also a permutation automaton). Then according to theorem L[9], the linear realization of V^* is characterized by a subgroup $K < \overline{I(V^*_{\mathcal{A}})}$ and a normal commutative subgroup $N \lhd \overline{I(V^*_{\mathcal{A}})}$ such that $K \cap N = \{1\}$ and besides, $\Sigma \subseteq Nx$ for every $\bar{x} \in \overline{I(V^*_{\mathcal{A}})}$ and $n^p = 1$ for every $n \in N$. Then the states of an automaton V^* are given by the

left cosets of subgroup H with regard to $\overline{I(V^*_{\mathcal{A}})}$. The next-state function M* is defined by the permutation on the set of left cosets of subgroup H; namely, for every $\overline{y} \in \overline{I(V^*_{\mathcal{A}})}$ we have

$$M^*(Hx,y) = \begin{pmatrix} Hx \\ Hxy \end{pmatrix}$$

for $\overline{x} \in \overline{I(V^*_{\mathcal{A}})}$. Automaton $\mathcal{A}$ is a homomorphic image of an automaton V* associated with a characteristic parition with the substitution property $\pi_2 = \{\overline{B_0},\overline{B_1},\ldots,\overline{B_{m-1}}\}$, where

$$B_j = \{g^i(s_j) : i=0,1,\ldots,q-1\}$$

and $j=0,1,\ldots,m-1$; $S = \{s_0,s_1,\ldots,s_{m-1}\}$. With π_2 is associated some subgroup $H < \overline{I(V^*_{\mathcal{A}})}$ such that its left cosets with regard to $\overline{I(V^*_{\mathcal{A}})}$ are equivalence classes of π_2. Let a mapping

$$\phi : \pi_2 \to \{Hx : \overline{x} \in \overline{I(V^*_{\mathcal{A}})}\}$$

be defined as follows:

$$\phi(B_i) = Hx \text{ if and only if } \phi(M(B_i,y)) = Hxy$$

for $\overline{y} \in \overline{I(V^*_{\mathcal{A}})}$; $i=0,1,\ldots,m-1$. It means that we ascribe for every block of π_2 the left coset of H with regard to $\overline{I(V^*_{\mathcal{A}})}$ if and only if transitive representation of the group $\overline{I(V^*_{\mathcal{A}})}$ by a permutation group induced by the subgroup H contains a permutation $Hx \to Hxy$ and simultanously $B_i \overset{y}{\to} M(B_i,y)$. H is a cyclic subgroup, because $V^*_{\mathcal{A}}$ is isomorphic to the direct product of $\mathcal{A}$ with a nonsingular, connected clock of period q. Besides the following implication holds:

$\mathcal{A}$ = Hom $V^*_{\mathcal{A}}$ implies $H \supseteq K$

because $H < \overline{I(V^*_{\mathcal{A}})}$ and $K < \overline{I(V^*_{\mathcal{A}})}$. Therefore K is also a cyclic subgroup of $\overline{I(V^*_{\mathcal{A}})}$. Let $H \cap N^\circ = N_1$, where N is a commutative subgroup of $\overline{I(V^*_{\mathcal{A}})}$ associated with linear realization of $V^*_{\mathcal{A}}$; N_1 is a subgroup for $\overline{I(V^*_{\mathcal{A}})}$ and besides N_1 is cyclic subgroup because all subgroups of the cyclic group are cyclic. The subgroup H as a cyclic group is abelian and, therefore, all its subgroups are normal. Hence automaton is linearly realizable over GF(p).

Q.E.D.

If automaton $\mathcal{A} = (S,\Sigma,M)$ is linearly realizable over GF(p) and $V^*_{\mathcal{A}} = (S^*,\Sigma,M^*)$ is a fixed analog of an extension $V_{\mathcal{A}} = (S',\Sigma,M')$ associated with q state isomorphisms, then $V^*_{\mathcal{A}}$ is described by the following equation:

$$\bigwedge_{s \in S} \bigwedge_{\sigma \in \Sigma} \alpha_1'(M^*(s,\sigma)) = A' \alpha_1'(s) + B' \alpha_2'(\sigma) + \phi_0'$$

where

$$A' = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & E \end{array}\right] \qquad B' = \left[\begin{array}{c} B \\ \hline 0 \end{array}\right] \qquad \phi_0' = \left[\begin{array}{c} \phi 0 \\ \hline 0 \end{array}\right]$$

$$\alpha_1' = (\alpha_1, \underbrace{00\ldots0}_{n_1}), \quad \alpha_2' = (\alpha_2, \underbrace{00\ldots0}_{n_2}) \text{ and } n_1 = [\log_p q]$$

α_1, α_2 - injections of linear realizability of $\mathcal{A}$ over GF(p),

A, B, ϕ_0 - matrices of linear realizability of $\mathcal{A}$ over GF(p),

E - matrix of linear realizability of a nonsingular, connected clock of peroid q.

From lemmas 1, 2, 3 and theorem 1 follows that $\mathcal{A}^\bullet$ is linearly realizable over GF(p) if and only if generalized state-input extension with fixed mappings on input alphabet $(\text{ext}_{(g^i,h^{-1})} \mathcal{A}^\bullet)^*$ has extended linear realizability over

GF(p).

Concluding remarks

In this paper we deal exclusively with linear and extended linear realizability of state extensions and generalized state-input extensions with fixed mappings on input alphabet of the ordinary finite automata. The motivation for studying generalized periodic sum of automata stems from the fact that some important computational processes can be investigated with help of algebraic methods commonly used in automata theory. Very loosely speaking, all processes having periodic structures can be studied with the help of generalized periodic sum model or its simplifications.

The following results have been established:

a) $\overline{I(\mathcal{A})} = \text{Hom}\ \overline{I(\text{ext}_{g^i}\mathcal{A})^*}$: characteristic semigroup $\overline{I(\mathcal{A})}$ of an automaton is isomorphic to homomorphic image of characteristic semigroup of the fixed analog of state extension of this automaton.

b) $(\text{ext}_{(g^i,h)}\mathcal{A})^* = (\text{ext}_{g^i}h^{-1}\mathcal{A}))^*$: fixed analog of generalized state-input extension with fixed mappings on input alphabet is state isomorphic to fixed analog of state extension of the h^{-1}-transformation.

c) $\mathcal{A}$ is linearly realizable (or has extended linear realizability) over GF(p) iff $(\text{ext}_{g^i}\mathcal{A})^*$ has extended linear realizability over GF(p) $(\text{ext}_{(g^i,h^{-1})}\mathcal{A})^*$ has extended linear realizability over GF(p)).

d) if $\mathcal{A}$ is linearly realizable over GF(p) than any extension of $\mathcal{A}$ is not linearly realizable over GF(p) (but it has extended linear realizability).

References

[1]. Clifford A.H.,Preston G.B. (1964), The Algebraic Theory of Semigroups, Vol. 1, pp. 35-36, American Mathematical Society, Providence, Rhode Island.

[2]. Deuel D.R. (1967), Time-varying linear sequential machines, Doctoral Dissertation, University of California at Berkeley.

[3]. Gill A. (1963), Time-varying sequential machines, J. Franklin Institute, 6,276, pp. 519-539.

[4]. Gill A., Flexer J.R. (1967), Periodic decomposition of sequential machines, J. Assoc. Comput. Mach., 4,14, pp. 666-676.

[5]. Grzymala-Busse J.W. (1969), On the periodic representation and the reducibility of periodic automata, J. Assoc. Comput. Mach., 3.16, pp. 432-441, Err. 4,17 (1970), pp. 739.

[6]. Grzymala-Busse J.W. (1974), On the automorphisms of periodic automata extensions, Bulletin de L'Academie Polonaise des Sciences, Serie des sciences math. astr. et phys. - Vol. XXII, 3, pp. 325-331.

[7]. Fleck A.C. (1962), Isomorphisms groups of automata, J. Assoc. Comput. Mach., 9,4, pp. 469-476.

[8]. Hartmanis J., Davis W.A. (1967), Homomorphic images of linear sequential machines, J. Comput. System Sciences, 1, pp. 155-165.

[9]. Hartmanis J., Walter H. (1973), Group-theoretic characterization of linear permutation automata, J. Comput. System Sciences, 7,2, pp. 168-189.

[10]. Mikołajczak B. (1974), Structural properties of the extensions of finite automata, Doctoral Dissertation, Technical University of Poznań, (in Polish).

[11]. Mikołajczak B. (1976), On some properties of cyclic automata and their extensions, Lecture Notes in Computer Science vol. 45, Mathematical Foundations of Computer Science, Gdańsk, Poland.