Algebra and Discrete Mathematics
Volume 10 **(2010)**. Number 1. pp. 97 – 103

RESEARCH ARTICLE

Groups of linear automata

Andriy Oliynyk

Communicated by V. I. Sushchansky

Abstract. The scalar automata as a special class of groups of linear automata over modules are introduced. The groups of scalar automata are classified.

1. The concept of a linear transformation of the infinite direct power of a module, defined by an automaton, was introduces by Ahil Nerode in [1]. He considered the notion of a linear automaton in much wider context than, for example, Samuel Eilenberg in [2, Chapter XVI]. In [3] linear automata over finite fields and groups of such automata were considered.

The paper is organized as follows. Firstly we recall main definitions concerning linear automata over modules. In this account we follow [2]. Then we introduce a special class of linear automata, so-called scalar automata. In such automata the module of inner states is equal to the module of letters and transition and output functions are the sums of multiplications by elements of the layer ring. We classify in Theorem 1 the groups of scalar automata. The proof is based on the technique presented in [3, Proposition 4.1] and developed in [4, Theorem 4.1] and [5, Proposition 1], where, in fact, groups of some scalar automata were calculated. As a corollary, we describe in Theorem 2 groups of linear automata over a finite field whose space of states is equal to this field. These results may be regarded as a contribution to the theory of self-similar groups ([6]).

2. Let R be a commutative ring with unit, R^* its group of invertible elements and M a nonzero module over R. Denote by M^n the direct sum $\underbrace{M \oplus \ldots \oplus M}_{n \text{ times}}$, $n \geq 1$. Let M^0 denotes the zero module. One have

2000 Mathematics Subject Classification: *20E08.*
Key words and phrases: *linear automaton, automaton group, wreath product.*

an isomorphic embedding of the module M^n into M^{n+1} via $w \mapsto (w, 0)$, $w \in M^n$. Then we obtain the direct system

$$M^0 \hookrightarrow M^1 \hookrightarrow M^2 \hookrightarrow \dots.$$

Its limit module will be denoted by M^*. Then $M^* = \bigcup_{n=0}^{\infty} M^n$. The module M^* is naturally identified with $R[t]$-module $M[t]$:

$$M^* \ni (m_0, \dots, m_n) \mapsto m_0 + \dots m_n t^n \in M[t], \quad n \geq 0.$$

Denote by M_i an isomorphic copy of module M, $i \geq 1$. The direct product $\prod_{i=1}^{\infty} M_i$ will be denoted by M^∞. This module is identified with $R[[t]]$-module $M[[t]]$ by the rule

$$M^\infty \ni (m_0, m_1, m_2, \dots) \mapsto \sum_{i=0}^{\infty} m_i t^i \in M[[t]].$$

Then M^* is a submodule of M^∞ as an $R[t]$-module.

Definition 1. *A linear automaton (a linear sequential machine as in [2, p.408]) over M is a tuple*

$$\mathcal{A} = \langle Q, M, \varphi, \psi \rangle,$$

where Q is an R-module (module of states of $\mathcal{A}$) and $\varphi : Q \oplus M \to Q$, $\psi : Q \oplus M \to M$ are homomorphisms of R-modules (transition and output functions of $\mathcal{A}$).

The transition and output functions of the linear automaton $\mathcal{A}$ can be extended inductively to the module $Q \oplus M^*$ as follows

$$\begin{aligned} \varphi(q, 0) &= q, & \varphi(q, (w, m)) &= \varphi(\varphi(q, w), m) \\ \psi(q, 0) &= 0, & \psi(q, (w, m)) &= \psi(\varphi(q, w), m), \end{aligned}$$

where $q \in Q$, $w \in Q \oplus X^*$ and $m \in M$. Such extended functions are homomorphisms of R-modules as well. A state $p \in Q$ is called accessible from a state $q \in Q$ if there exist $n \geq 0$ and $w \in M^n$ such that $\varphi(q, w) = p$.

Every state $q \in Q$ defines an endomorphism f_q of the R-module M^∞ by the rule

$$f_q((m_0, m_1, m_2, \dots)) = (\psi(q, m_0), \psi(q, (m_0, m_1)), \psi(q, (m_0, m_1, m_2)), \dots).$$

The modules M^* and M^n, $n \geq 0$, are invariant under f_q.

Proposition 1. *The endomorphism $f_q : M^\infty \to M^\infty$ is an automorphism if and only if for each state $p \in Q$, accessible from q, the endomorphism $\lambda_q : M \to M$, defined by the rule $\lambda_q(m) = \psi(q, m), m \in M$, is an automorphism.*

Proof. It is a straightforward verification. □

An endomorphism (automorphism) $f : M^\infty \to M^\infty$ is called linear automaton endomorphism (automorphism) if there exist a linear automaton $\mathcal{A}$ and its state q such that $f = f_q$. Using Proposition 1 one can show that the automorphism inverse to linear automaton endomorphism is linear automaton automorphism as well. Denote the set of all linear automaton endomorphisms (automorphisms) of M^∞ by $End_{LA}(M^\infty)$ ($Aut_{LA}(M^\infty)$).

For two linear automata over M

$$\mathcal{A}_1 = \langle Q_1, M, \varphi_1, \psi_1 \rangle \text{ and } \mathcal{A}_2 = \langle Q_2, M, \varphi_2, \psi_2 \rangle$$

define their product $\mathcal{A}_1 \cdot \mathcal{A}_2$ as a tuple

$$\mathcal{A}_1 \cdot \mathcal{A}_2 = \langle Q_1 \oplus Q_2, M, \varphi, \psi \rangle,$$

where mappings $\varphi : Q_1 \oplus Q_2 \oplus M \to Q_1 \oplus Q_2$, $\psi : Q_1 \oplus Q_2 \oplus M \to M$ are defined by the rules

$$\varphi((q_1, q_2), m) = (\varphi_1(q_1, m), \varphi_2(q_2, \psi(q_1, m)))$$
$$\psi((q_1, q_2), m) = \psi_2(q_2, \psi(q_1, m)).$$

These functions are indeed homomorphisms of R-modules. Hence, a product of linear automata over M is a linear automaton over M as well. One can directly verify that for arbitrary states $q_1 \in Q_1$ and $q_2 \in Q_2$ the equality $f_{q_2}(f_{q_1}) = f_{(q_1,q_2)}$ holds. This equality immediately imply that the set $End_{LA}(M^\infty)$ is closed under superposition. Moreover, one can show that $End_{LA}(M^\infty)$ is closed under addition ([2, Proposition 6.1]). This means that the following proposition holds.

Proposition 2. *The set $End_{LA}(M^\infty)$ form a subring in the ring of endomorphisms of M^∞. The set $Aut_{LA}(M^\infty)$ form a group of units of $End_{LA}(M^\infty)$.*

A linear automaton $\mathcal{A} = \langle Q, M, \varphi, \psi \rangle$ is called permutational if for each state $q \in Q$ the mapping f_q is an automorphism. The group $G(\mathcal{A})$ of an invertible automaton $\mathcal{A}$ is the subgroup of $Aut_{LA}(M^\infty)$, generated by the set $\{f_q : q \in Q\}$.

3. Let us fix a module M over a commutative ring with unit R. A linear automaton $\mathcal{A} = \langle Q, M, \varphi, \psi \rangle$ will be called scalar if $Q = M$ and there exist $\alpha_1, \alpha_2, \beta_1, \beta_2 \in R$ such that

$$\varphi(q, m) = \alpha_1 q + \alpha_2 m, \quad \psi(q, m) = \beta_1 q + \beta_2 m \tag{1}$$

for arbitrary $q \in Q, m \in M$. It is easy to see that this scalar automaton is permutational if and only if the element β_2 is invertible in R.

For an element $r \in R$ let us denote by rM the image of the module M under the scalar endomorphism $r \cdot id$ of M. For an invertible $r \in R$ we will use notation $\langle r \rangle$ for the cyclic subgroup of R^* generated by r.

Theorem 1. *Let $\mathcal{A} = \langle Q, M, \varphi, \psi \rangle$ be a permutational scalar automaton over M whose transition and output functions are given by (1) for $\alpha_1, \alpha_2, \beta_1 \in R$, $\beta_2 \in R^*$. Then the group $G(\mathcal{A})$ is isomorphic to:*

1. *the group $\langle \beta_2 \rangle$ provided $\beta_1 = 0$;*
2. *the wreath product $\langle \beta_2 \rangle \wr (\beta_1 M, +)$ provided $\beta_1 \neq 0, \alpha_2 = 0$ and the order of β_2 in R^* is finite;*
3. *the restricted wreath product $\mathbb{Z} \bar{\wr} (\beta_1 M, +)$ provided $\beta_1 \neq 0$ whereas $\alpha_2 \neq 0$ or the order of β_2 in R^* is infinite.*

Proof. Let us fix a series $m(t) \in M[[t]], m(t) = \sum_{i=0}^{\infty} m_i t^i$. First of all for arbitrary $q \in Q$ we calculate the image $m(t)^{f_q}$. From the definition of output function we have the equality

$$m(t)^{f_q} = \beta_1 m_q(t) + \beta_2 m(t),$$

for $m_q(t) \in M[[t]], m_q(t) = \sum_{i=0}^{\infty} q_i t^i$ such that

$$q_0 = q, \qquad q_{i+1} = \varphi(q_i, m_i) = \alpha_1 q_i + \alpha_2 m_i, \quad i \geq 0.$$

Then by induction on i we obtain the equality

$$q_{i+1} = \alpha_1^{i+1} q + \alpha_2 \sum_{j=0}^{i} \alpha_1^{i-j} m_j, \quad i \geq 0.$$

Therefore

$$m(t)^{f_q} = \beta_1 q + \beta_1 \sum_{i=0}^{\infty} \left(\alpha_1^{i+1} q + \alpha_2 \sum_{j=0}^{i} \alpha_1^{i-j} m_j \right) t^{i+1} + \beta_2 m(t) =$$

$$\beta_1 q\sum_{i=0}^{\infty}\alpha_1^i t^i+\beta_1\alpha_2 t\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\alpha_1^{i-j}m_j\right)t^i+\beta_2 m(t)=$$

$$\beta_1 q(1-\alpha_1 t)^{-1}+\beta_1\alpha_2 t\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}\alpha_1^{i-j}t^{i-j}m_j t^j\right)+\beta_2 m(t)=$$

$$\beta_1 q(1-\alpha_1 t)^{-1}+\beta_1\alpha_2 t(1-\alpha_1 t)^{-1}m(t)+\beta_2 m(t)=$$

$$m(t)\left(\beta_2+\beta_1\alpha_2 t(1-\alpha_1 t)^{-1}\right)+\beta_1 q(1-\alpha_1 t)^{-1}.$$

Since $\beta_2\in R^*$ the series $P(t)=\beta_2+\beta_1\alpha_2 t(1-\alpha_1 t)^{-1}$ is invertible in $M[[t]]$.

Let now $\beta_1=0$. Then $m(t)^{f_q}=m(t)\beta_2$, $q\in Q$, and the group $G(\mathcal{A})$ is isomorphic to the cyclic group generated by the scalar endomorphism $\beta_2\cdot id$ of M . Since $\beta_2\in R^*$ and $M\neq 0$ the latter group is isomorphic to the subgroup $\langle\beta_2\rangle$ of M^* and we obtain the first statement of the theorem.

Assume in the sequel that $\beta_1\neq 0$. Then

$$m(t)^{f_q}=m(t)P(t)+\beta_1 q(1-\alpha_1 t)^{-1},\quad q\in Q.$$

This implies

$$m(t)^{f_q^{-1}}=m(t)P(t)^{-1}-\beta_1 P(t)^{-1}q(1-\alpha_1 t)^{-1},\quad q\in Q.$$

In particular, $m(t)^{f_0}=m(t)P(t)$ and $m(t)^{f_0^{-1}}=m(t)P(t)^{-1}$.

For each $q\in Q$, denote by h_q the product $f_0^{-1}f_q$. This product act as follows

$$m(t)^{h_q}=m(t)+\beta_1 q(1-\alpha_1 t)^{-1}.$$

Then the set $H=\{h_q: q\in Q\}$ form a subgroup of $G(\mathcal{A})$. This subgroup is isomorphic to the additive group $(\beta_1 M,+)$ of the R-module $\beta_1 M$. The group $G(\mathcal{A})$ is generated by H and f_0. Denote by H_i, $i\geq 1$, the isomorphic copy of H.

For arbitrary $k\in\mathbb{Z}$ we have

$$m(t)^{f_0^{-k}h_q f_0^k}=\left(m(t)P(t)^{-k}\right)^{h_q f_0^k}=$$

$$\left(m(t)P(t)^{-k}+\beta_1 q(1-\alpha_1 t)^{-1}\right)^{f_0^k}=$$

$$m(t)+\beta_1 q(1-\alpha_1 t)^{-1}P(t)^k, q\in Q.$$

Denote by W the normal closure in $G(\mathcal{A})$ of the set $\{f_0^{-k}h_q f_0^k: k\in\mathbb{Z}, q\in Q\}$. We will show, that depending on the order of the series $P(t)$ in $M[[t]]^*$, the group W is finite or infinite direct sum of H.

Let $\alpha_2 = 0$. Then $P(t) = \beta_2$. Assume that β_2 has finite order equal to k in R^*. Then the orders of $P(t)$ in $M[[t]]^*$ and the subgroup $C = \langle f_0 \rangle$ are k as well. The subgroup W in this case consists of the transformations w acting by the rule

$$m(t)^w = m(t) + \beta_1(1 - \alpha_1 t)^{-1} \sum_{i=0}^{k-1} q_i \beta_2^i,$$

where $q_i \in Q$, $0 \le i \le k-1$. This means that the intersection of W and C is trivial and

$$W = \bigoplus_{i=0}^{k-1} H_i.$$

The subgroup C acts on W via conjugation, cyclically permuting components of each their element:

$$m(t)^{f_0^{-1} w f_0} = m(t) + \beta_1(1 - \alpha_1 t)^{-1} \sum_{i=0}^{k-1} q_i \beta_2^{(i+1) \bmod k}, w \in W.$$

Hence, the group $G(\mathcal{A})$ splits into the semidirect product $W \rtimes C$ which isomorphic to the wreath product $\langle \beta_2 \rangle \wr (\beta_1 M, +)$.

Let $\alpha_2 \neq 0$ or the order of β_2 in R^* is infinite. In both cases the orders of $P(t)$ in $M[[t]]^*$ and the subgroup C are infinite as well. Each transformation $w \in W$ has the form

$$m(t)^w = m(t) + \beta_1(1 - \alpha_1 t)^{-1} \sum_{i=-\infty}^{+\infty} q_i \beta_2^i, \quad q_i \in Q, i \in \mathbb{Z},$$

where all but finite number of q_i's equals 0. This implies that the intersection of W and C is trivial and

$$W = \bigoplus_{i=-\infty}^{+\infty} H_i.$$

The subgroup C acts by translations on W via conjugation:

$$m(t)^{f_0^{-1} w f_0} = m(t) + \beta_1(1 - \alpha_1 t)^{-1} \sum_{i=-\infty}^{+\infty} q_i \beta_2^{(i+1)}, w \in W.$$

Hence, the group $G(\mathcal{A})$ again splits into the semidirect product $W \rtimes C$ which isomorphic to the restricted wreath product $\mathbb{Z} \bar{\wr} (\beta_1 M, +)$. The proof is complete. □

Let now $\mathbb{F}_q$ be a finite field, $q = p^n$, p — prime, $n \geq 1$. Consider $\mathbb{F}_q$ as a regular module over itself.

Theorem 2. *Let $\mathcal{A}$ be a linear automaton over $\mathbb{F}_q$ such that its module of states is equal to $\mathbb{F}_q$. Then the group $G(\mathcal{A})$ is isomorphic to one of the following groups:*

1. *the cyclic group $\mathbb{Z}_m$, where $m|(q-1)$;*
2. *the wreath product $\mathbb{Z}_m \wr \mathbb{Z}_q$, $m|(q-1)$, $m \neq 1$;*
3. *the lamplighter group $\mathbb{Z} \bar{\wr} \mathbb{Z}_q$.*

Proof. Note, that linear automata mentioned in the theorem are indeed scalar automata. The result now implies from Theorem 1 and cyclicity of the group $\mathbb{F}_q^*$. □

References

[1] A. Nerode, *Linear automaton transformations*. Proc. Amer. Math. Soc., 9, 1958, 541–544.

[2] S. Eilenberg, *Automata, languages, and machines. Vol. A.* — New York : Academic Press, 1974, 446 p.

[3] R. I. Grigorchuk, V. V. Nekrashevich, V. I. Sushchanskii, *Automata, dynamical systems, and groups*, Tr. Mat. Inst. Steklova, 231 (Din. Sist., Avtom. i Beskon. Gruppy):134–214, 2000.

[4] P. V. Silva, B. Steinberg, *On a class of automata groups generalizing lamplighter groups*. Internat. J. Algebra Comput. 15, 2005, 1213–1234.

[5] L. Bartholdi, Z. Šunić, *Some solvable automaton groups*, Contemporary Mathematics 394, 2006, 11–29.

[6] V. V. Nekrashevych, *Self-similar groups*, volume 117 of Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2005.

Contact information

A. Oliynyk

Department of Mechanics and Mathematics
Kyiv Taras Shevchenko University
Volodymyrska, 60
Kyiv 01033
E-Mail: olijnyk@univ.kiev.ua
URL: http://algebra.kiev.ua/oliynyk/

Received by the editors: 31.10.2010
and in final form 31.10.2010.