Automata over parametric varieties in a finite ring

V.V. Skobelev

Mealy and Moore automata determined onto trajectories in some polynomially parametric variety in a finite ring are considered. Homomorphisms of investigated models are analyzed. Sets of deterministic and non-deterministic automata are characterized. Criteria for following sets of deterministic automata are established: group automata, automata with source-states, automata with flow-states, connected and strongly connected automata, automata with twins-states and automata with 1*-distinguishable states.*

Introduction

Applications of combinatorial-algebraic models in modern cryptography [1] has stimulated investigation of automata determined over finite algebraic systems. Besides, elliptic cryptography based onto elliptic curves over finite fields [2] indicates deep inner links between modern cryptography and algebraic geometry [3]. Thus, investigation of automata determined over varieties in a finite ring is actual for algebraic automata theory as well, as for its potential applications in modern cryptography. The aim of the given paper is investigation of automata determined onto trajectories in some polynomially parametric variety in a finite ring.

Basic notions

Let $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 2$) be any finite ring, $\mathcal{V}_{n,m}(\mathcal{K})$ ($n, m \in \mathbf{N}, m \leq n$) be the set of all varieties $\mathbf{V} = \{\mathbf{h}(\overrightarrow{\tau}) | \overrightarrow{\tau} \in K^m\}$ ($|\mathbf{V}| > 1$), where $\mathbf{h} = (h_1, \ldots, h_n)^T$ ($h_1, \ldots, h_n \in K[\tau_1, \ldots, \tau_m]$) and $\mathcal{F}_m$ be the set of easily computable $f : K^m \to K^m$.

Any $f \in \mathcal{F}_m$ determines on $\mathbf{V}$ the set $\mathcal{T}_{\mathbf{V},f}$ of trajectories $\mathbf{h}(P_0), \mathbf{h}(P_1), \ldots$ ($P_0 \in K^m$), where $P_{j+1} = f(P_j)$ for all $j \in \mathbf{Z}_+$. Let $\mathbf{h} \circ f$ be superposition of mappings f and $\mathbf{h}$, i.e. $(\mathbf{h} \circ f)(P) = \mathbf{h}(f(P))$ ($P \in K^m$).

Theorem 1. Any two distinct trajectories in $\mathcal{T}_{\mathbf{V},f}$ ($f \in \mathcal{F}_m$) start from different points if and only if there do not exist $P_0^{(1)}, P_0^{(2)} \in K^m$, such that $P_0^{(1)} \equiv P_0^{(2)}$ ($\ker \mathbf{h}$) and $P_0^{(1)} \not\equiv P_0^{(2)}$ ($\ker(\mathbf{h} \circ f)$).

We denote by $\mathcal{F}_{m,\mathbf{h}}$ the set of all $f \in \mathcal{F}_m$, such that

$$(\forall P, P' \in K^m)(P \equiv P' \,(\ker \mathbf{h}) \Rightarrow P \equiv P' \,(\ker(\mathbf{h} \circ f))).$$

Investigated models

Let $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$ and $\Theta = \{\theta_i\}_{i \in \mathbf{Z}_k}$ be some fixed family of elements of the set $\mathcal{F}_m$. We determine the sets $\mathcal{A}_{k,l}^{(1)}(\mathbf{V}, \Theta)$ and $\mathcal{A}_{k,l}^{(2)}(\mathbf{V}, \Theta)$ of Mealy and Moore automata, correspondingly, via systems of equations

$$\begin{cases} P_{t+1} = \theta_{x_{t+1}}(P_t) \\ \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{r}_{x_{t+1}}(\mathbf{q}_t) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

and

$$\begin{cases} P_{t+1} = \theta_{x_{t+1}}(P_t) \\ \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{r}(\mathbf{q}_{t+1}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

where $P_0 \in K^m$, $\mathbf{q}_0 = \mathbf{h}(P_0)$, $\mathbf{r}_i : K^n \to K^l$ ($i \in \mathbf{Z}_k$), $\mathbf{r} : K^n \to K^l$, and $x_{t+1} \in \mathbf{Z}_k$ ($t \in \mathbf{Z}_+$) (x_t, $\mathbf{q}_t$ and $\mathbf{y}_t$ are, correspondingly, input symbol, the state and output symbol at instant t).

Let $\mathbf{V}_j \in \mathcal{V}_{n_j,m_j}(\mathcal{K})$ $(j = 1, 2)$, $\Theta_j = \{\theta_i^{(j)}\}_{i\in\mathbf{Z}_{k_j}}$ be parametrization for $\mathbf{V}_j$. If there exist a pair of surjections $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 : \mathbf{V}_1 \to \mathbf{V}_2, \varphi_2 : K^{m_1} \to K^{m_2})$, such that $\varphi_2(\theta_i^{(1)}(\overrightarrow{\tau}_1)) = \theta_i^{(2)}(\varphi_2(\overrightarrow{\tau}_1))$ and $\varphi_1(\mathbf{h}_1(\overrightarrow{\tau}_1)) = \mathbf{h}_2(\varphi_2(\overrightarrow{\tau}_1))$ for all $\overrightarrow{\tau}_1 \in K^{m_1}$ and $i \in \mathbf{Z}_k$, then a pair $(\mathbf{V}_2, \Theta_2)$ is determined to be a homomorhic image of the pair $(\mathbf{V}_1, \Theta_1)$.

Theorem 2. If a pair $(\mathbf{V}_2, \Theta_2)$ is a homomorphic image of the pair $(\mathbf{V}_1, \Theta_1)$ then there exist mappings $\Psi_j : \mathcal{A}^{(j)}_{k_1,l_1}(\mathbf{V}_1, \Theta_1) \to \mathcal{A}^{(j)}_{k_2,l_2}(\mathbf{V}_2, \Theta_2)$ $(j = 1, 2)$ such that for any automaton $M \in \mathcal{A}^{(j)}_{k_1,l_1}(\mathbf{V}_1, \Theta_1))$ the automaton $\Psi_j(M) \in \mathcal{A}^{(j)}_{k_2,l_2}(\mathbf{V}_2, \Theta_2))$ is homomorphic image of an automaton M_j.

Theorem 3. 1. The set $\mathcal{A}^{(i)}_{k,l}(\mathbf{V}, \Theta)$ $(i = 1, 2)$ is the set of deterministic automata if and only if Θ is some family of elements of the set $\mathcal{F}_{m,\mathbf{h}}$.

2. The set $\mathcal{A}^{(i)}_{k,l}(\mathbf{V}, \Theta)$ $(i = 1, 2)$ is the set of non-deterministic automata if and only if Θ consists some element of the set $\mathcal{F}_m \backslash \mathcal{F}_{m,\mathbf{h}}$.

In the sequel only deterministic automata are considered. The set of all families $\Theta = \{\theta_i\}_{i\in\mathbf{Z}_k}$ of elements of the set $\mathcal{F}_{m,\mathbf{h}}$ is denoted by $\mathcal{W}_k$.

An automaton is a group one if every its input symbol determines some permutation of the set of states.

Let $\mathcal{F}^{(0)}_{m,\mathbf{h}}$ be the set of all $f \in \mathcal{F}_{m,\mathbf{h}}$, such that

$$(\forall P, P' \in K^m)(P \not\equiv P' \,(\ker \mathbf{h}) \Rightarrow P \not\equiv P' \,(\ker(\mathbf{h} \circ f))).$$

Theorem 4. 1. The set $\mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ $(\Theta \in \mathcal{W}_k)$ consists of group automata if and only if Θ is some family of elements of the set $\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

2. The set $\mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ $(\Theta \in \mathcal{W}_k)$ consists of group automata if and only if Θ consists some element of the set $\mathcal{F}_{m,\mathbf{h}} \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}$.

A state of an automaton is called to be:

1) a source-state, if there is no transition to it;

2) a flow-state, if no other state can be reached from it.

Two distinct states of an automaton are called to be twins-states if every input symbol transforms them into the same state and reaction of automaton is the same.

Let $K^m / \ker \mathbf{h} = \{B_1, \ldots, B_{|\mathbf{V}|}\}$.

Basic types of states of an automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ $(\Theta \in \mathcal{W}_k)$ can be characterized in the following way:

1) the set $\mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ consists of automata with source-states if and only if $\Theta = \{\theta_i\}_{i\in\mathbf{Z}_k}$ is some family of elements of the set $\mathcal{F}_{m,\mathbf{h}} \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}$, such that there exists $j \in \mathbf{N}_{|\mathbf{V}|}$, such that $\bigcup\limits_{i\in\mathbf{Z}_k} Val\ \theta_i \subset K^m \backslash B_j$;

2) the set $\mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ consists of automata with flow-states if and only if $\Theta = \{\theta_i\}_{i\in\mathbf{Z}_k}$ is some family of elements of the set $\mathcal{F}_{m,\mathbf{h}} \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}$, such that there exists $j \in \mathbf{N}_{|\mathbf{V}|}$, such that $\bigcup\limits_{i\in\mathbf{Z}_k} Val\ (\theta_i|_{B_j}) \subset B_j$;

3) there are twins-states in an automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta)$ if and only if there exist $P_1, P_2 \in K^m$, such that the following three conditions hold: (i) $P_1 \not\equiv P_2$ $(\ker \mathbf{h})$; 2) $\theta_i(P_1) \equiv \theta_i(P_2)$ $(\ker \mathbf{h})$ for all $i \in \mathbf{Z}_k$; 3) $P_1 \equiv P_2$ $(\bigcap\limits_{i\in\mathbf{Z}_k} \ker(\mathbf{r}_i \circ \mathbf{h}))$;

4) there are twins-states in an automaton $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ if and only if there exist $P_1, P_2 \in K^m$, such that the following two conditions hold: 1) $P_1 \not\equiv P_2$ $(\ker \mathbf{h})$; 2) $\theta_i(P_1) \equiv \theta_i(P_2)$ $(\ker \mathbf{h})$ for all $i \in \mathbf{Z}_k$.

For any automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathcal{W}_k)$ we determine the following or-graph $G_M = (K^m/\ker \mathbf{h}, \Gamma_M)$: $(B_{j_1}, B_{j_2}) \in \Gamma_M$ $(j_1, j_2 \in \mathbf{N}_{|\mathbf{V}|})$ if and only if there exist $r \in \mathbf{Z}_k$, such that $\theta_r(B_{j_1}) \subseteq B_{j_2}$.

The following propositions hold:

1) an automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ is connected (correspondingly, strongly connected) if and only if or-graph G_M is connected (correspondingly, strongly connected);

2) the number of components of connectivity (correspondingly, of strongly connectivity) of transition graph of an automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ is the same as the number of components of connectivity (correspondingly, of strongly connectivity) of the or-graph G_M;

3) the diameter (correspondingly, the radius) of transition graph of an automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ is the same as the diameter (correspondingly, the radius) of the or-graph G_M.

An automaton is called to be 1-distinguishable, if any two its distinct states can be distinguished by some input symbol.

The following propositions hold:

1) an automaton $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathcal{W}_k)$ is 1-distinguishable if and only if the identity $\ker \mathbf{h} = \bigcap\limits_{i \in \mathbf{Z}_k} \ker(\mathbf{r}_i \circ \mathbf{h})$ holds;

2) an automaton $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathcal{W}_k)$ is 1-distinguishable if and only if the identity $\ker \mathbf{h} = \bigcap\limits_{i \in \mathbf{Z}_k} \ker(\mathbf{r} \circ \mathbf{h} \circ \theta_i)$ holds.

Conclusion

In the given paper Mealy and Moore automata determined onto trajectories in some polynomially parametric variety in a finite ring are analyzed.

In terms of detailed analysis of structures of a variety $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$ and of a set of trajectories $\mathcal{T}_{\mathbf{V},f}$ the following two trends of research naturally arise: 1) detailed analysis of properties of surjections $\Phi = (\varphi_1, \varphi_2)$; 2) detailed analysis of structure of basic subsets of the set of automata $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$.

Taking into account potential application of investigated models in the process of design of stream ciphers the third trend of research can be connected with detailed analysis of subsets of reversible automata $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$.

The author is grateful to academician A.A. Letichevskij for his help and advice in the process of research.

References

[1] Yu. S. Charin , V.I. Bernik, and G.V. Matveev, Mathematical and computer backgrounds of cryptology, Novoje znanie, Minsk, 2003 (in Russan).

[2] O.N. Vasilenko, Number-theoretical algorithms in cryptography, MCNMO, Moskow, 2003 (in Russan).

[3] I.R. Shapharevich, Backgrounds of algebraic geometry, Vol. 1 and 2, Moskow, Nauka, 1988 (in Russan).

Authors

Volodymyr Volodymyrovych Skobelev — researcher, department of control systems theory, Institute of Applied Mathematics and Mechanics of National Academy of Sciences of Ukraine, Donetsk, Ukraine; E-mail: *vv_skobelev@iamm.ac.donetsk.ua*