Computer Science Journal of Moldova, vol.**23**, no.2(68), 2015

Finite automata over algebraic structures: models and some methods of analysis

Volodymyr V. Skobelev, Volodymyr G. Skobelev

Abstract

In this paper some results of research in two new trends of finite automata theory are presented. For understanding the value and the aim of these researches some short retrospective analysis of development of finite automata theory is given. The first trend deals with families of finite automata defined via recurrence relations on algebraic structures over finite rings. The problem of design of some algorithm that simulates with some accuracy any element of given family of automata is investigated. Some general scheme for design of families of hash functions defined by outputless automata is elaborated. Computational security of these families of hash functions is analyzed. Automata defined on varieties with some algebra are presented and their homomorphisms are characterized. Special case of these automata, namely automata on elliptic curves, are investigated in detail. The second trend deals with quantum automata. Languages accepted by some basic models of quantum automata under supposition that unitary operators associated with input alphabet commute each with the others are characterized.

Keywords: finite automata, finite rings, varieties, simulation, hash functions, elliptic curves, quantum automata.

1 Introduction

It is well known that 'an automaton' is one of the basic notions of computer science. Its significance was established in the fundamental paper of A.M. Turing [1] where it has been used as some formal model for informal notion of 'an algorithm' (i.e. either a digital transducer,

or an acceptor of a language). Foundations of finite automata (FA) theory were laid in the middle of XX century [2]. In its essence any finite automaton presents some formal model for processes that can be implemented on computers (under the subject to the limitation that the memory is finite).

Development of FA theory has been motivated not only by its internal problems, but also it has been carried out in close interaction with other areas of computer science. The last circumstance in many respects led to numerous applications of FA models. On the other hand, research of actual applied problems (including the ones in the area of modern information technologies) and emergence of some new paradigms for notion of 'computation' led to significant reconsideration problems in FA theory. As the result, the formation of some entirely new sections of this theory has been started.

In this paper we consider two of these new sections. The first one deals with FA defined via recurrence relations over some finite ring. In many ways this section owes its appearance to research in the field of information protection. Moreover, the necessity of investigation of these models is substantially caused by the problems of modern cryptography [3, 4]. The second section deals with quantum FA, i.e. with some section of quantum algorithms theory which is being developed intensively at present. In this context, an essential factor is that the notion 'quantum FA' is based on the new paradigm of computations called 'quantum computations' [5, 6].

2 Survey of finite automata theory

The following two stages can be naturally highlighted in the development of FA automata theory.

The first stage covers 50s–80s of the XX century.

Finite automaton considered as a transducer has been defined as a system $\mathtt{M} = (\mathtt{Q}, \mathtt{X}, \mathtt{Y}, \delta, \lambda)$ (where $\mathtt{Q}$, $\mathtt{X}$ and $\mathtt{Y}$ are respectively finite set of states, finite input alphabet and finite output alphabet, $\delta : \mathtt{Q} \times \mathtt{X} \to \mathtt{Q}$ is the transition function and $\lambda : \mathtt{Q} \times \mathtt{X} \to \mathtt{Y}$ is the output function). Moore and Mealy models of FA and some their variants associated

with FA functioning in time have been determined. The problems of analysis and synthesis for FA [7, 8, 9], the problem of completeness for FA [10,11] and problems of theory of experiments with FA [12] have been investigated within these models. Analysis of transformations of free semigroups carried out by FA [13] had a significant influence on formation of algebraic theory of FA [14,15] and automata-algebraic approach to software engineering [16].

It should be noted investigation of information-lossless FA [17, 18] which (possibly with some additional information) carry-out injective transformations of input semigroup into output semigroup. Some important subclass of information-lossless FA form reversible FA. These FA are characterized in that the input alphabet coincides with the output alphabet, and in each state it is carried out some bijective conversion of input symbols into output symbols. Reversible FA forms some powerful mathematical tool which enables us to investigate the deep inner connection between the FA theory and the theory of groups. Thus, these FA can be applied successfully in resolving of a wide range of theoretical and applied problems, both. It should be emphasized that just information-lossless FA demonstrate possibility for using of FA as some mathematical model for stream ciphers. Also, numerous applications in resolving of theoretical and applied problems were found for group FA. In these FA transition function carries out some permutation of the set of states for every fixed input symbol value.

Finite automaton considered as an acceptor has been defined as a system $\mathtt{M} = (\mathtt{Q}, \mathtt{X}, \delta, \mathtt{q}_{in}, \mathtt{Q}_{acc})$ (where $\mathtt{Q}$ and $\mathtt{X}$ are respectively finite set of states and finite input alphabet, $\delta : \mathtt{Q} \times \mathtt{X} \to \mathtt{Q}$ is the transition function, $\mathtt{q}_{in} \in \mathtt{Q}$ is the initial state and $\mathtt{Q}_{acc} \subseteq \mathtt{Q}$ is the set of accepting states). An input string is accepted by $\mathtt{M}$ if it transforms the initial state into the set of accepting states. The set of all such input strings is the language accepted by $\mathtt{M}$. It has been proved that for any fixed finite alphabet the set of languages $\mathfrak{L}_{DFA}$ accepted by FA acceptors equals to the set of regular languages (Kleene's theorem). It should be noted that any FA acceptor is some 1-way 1-head Turing Machine (TM) with input tape, i.e. information can only be read (1-way means that at every step the head of TM moves one cell to the right).

Non-deterministic FA acceptors have been investigated under supposition that any subset $\mathtt{Q}_{in} \subseteq \mathtt{Q}$ of initial states could be chosen and any ternary relation $\delta \subseteq \mathtt{Q} \times (\{\Lambda\} \cup \mathtt{X}) \times \mathtt{Q}$ (Λ is the empty symbol) could define admissible transitions. Accepted language has been defined as the set of strings that transform at least one initial state into the set of accepting states. It has been proved that the set of all languages accepted by these acceptors equals to the set $\mathfrak{L}_{DFA}$. Although every non-deterministic FA acceptor can be effectively transformed into equivalent deterministic one, this transformation can lead to a significant increase in cardinality for the set of states (there are known some examples when non-deterministic FA acceptor has n states while equivalent deterministic one has 2^n states). Possibly, just this factor has grounded application of non-deterministic FA acceptors algebra [9] for formation of one of the main classes of discrete event systems intended to automate industrial process control.

Nontrivial generalization of non-deterministic FA acceptors was the emergence of probabilistic FA [19, 20]. In this model for each state and each input symbol the probability of transition into each state is defined (thus, there is some deep inner link between probabilistic FA and finite Markov chains [21]). Formally, probabilistic FA is a system $\mathtt{M} = (\mathtt{Q}, \mathtt{X}, \{M_{\mathtt{x}}\}_{\mathtt{x} \in \mathtt{X}}, \mathtt{u}_0, \mathtt{Q}_{acc})$, where $\mathtt{Q} = \{\mathtt{q}_1, \ldots, \mathtt{q}_n\}$ is the set of states, $\mathtt{X}$ is finite input alphabet, $M_{\mathtt{x}}$ ($\mathtt{x} \in \mathtt{X}$) is some stochastic $n \times n$-matrix of transitions, $\mathtt{u}_0 = (\alpha_1^{(0)}, \ldots, \alpha_n^{(0)})^T$ ($\alpha_i^{(0)} \in \mathbb{R}_+$ ($i \in \mathbb{N}_n$), $\sum\limits_{i=1}^{n} \alpha_i^{(0)} = 1$) is the initial distribution of states, and $\mathtt{Q}_{acc} \subseteq \mathtt{Q}$ is the set of accepting states. The evolution of $\mathtt{M}$ on input string $\mathtt{x}_1 \ldots \mathtt{x}_l$ ($l \in \mathbb{Z}_+$) is defined by identity $(\alpha_1^{(l)}, \ldots, \alpha_n^{(l)})^T = M_{\mathtt{x}_l} \ldots M_{\mathtt{x}_1} \mathtt{u}_0$. This string is accepted by $\mathtt{M}$ with probability $\mathtt{P}_{\mathtt{M}}(\mathtt{x}_1 \ldots \mathtt{x}_l) = \sum \alpha_i^{(l)}$, where the sum is over all i such that $\mathtt{q}_i \in \mathtt{Q}_{acc}$. It is defined that probabilistic FA $\mathtt{M}$ accepts the language $\mathtt{L} \subseteq \mathtt{X}^+$ with: 1) probability p ($0.5 \leq p \leq 1$) if it accepts every string $\mathtt{w}_1 \in \mathtt{L}$ with probability not less than p, while any string $\mathtt{w}_2 \notin \mathtt{L}$ is accepted with probability not exceeding $1-p$; 2) error $(p_1; p_2)$ ($0 \leq p_1 < p_2 \leq 1$) if it accepts every string $\mathtt{w}_1 \in \mathtt{L}$ with probability not less than p_2, while any string $\mathtt{w}_2 \notin \mathtt{L}$ is accepted with probability not exceeding p_1. It should be noted that any probabilistic FA is some

1-way 1-head probabilistic TM with input tape.

Progress in error-correcting codes development [22, 23] and linear systems analysis [24] has stimulated research of FA presented via recurrence relations over finite fields [25].

The second stage in the development of FA automata theory started in 90s of the XX century.

Development of models for cryptographic protection of information had a great influence on FA theory. The following problems became actual. Firstly, it is analysis of pre-images of output strings produced by FA [26]. Secondly, it is analysis of linear and poly-linear recurrences over finite rings [27, 28]. These recurrences define some class of autonomous automata intended for design of generators of pseudo-random sequences used in modern ciphers. Thirdly, it is analysis of experiments with linear and bilinear automata defined via recurrence relations over finite fields [29]. Fourthly, it is investigation of complexity of FA identification [30]. This problem is caused by application of FA for analysis of computational security for stream ciphers [31, 32]. Fifthly, it is investigation of families of FA defined via algebraic recurrence relations over finite rings [33, 34]. If these FA are reversible, they can be used as mathematical models for some stream ciphers.

The problems listed above show that formation of some new section of algebraic theory of FA is carried out at present. Essentially new factor for this section is the transition from transformations of free semigroups to transformations of algebraic structures performed by FA defined via recurrence relations over finite algebraic structures. These researches are presented in Section 3 of the current paper.

Since 1997 a variety of quantum FA (QFA) models different in computational capacity have been investigated. All of them are acceptors and they are defined in terms of 1-way k-head ($k \geq 1$) quantum TM (QTM) with input tape. Accepting of languages was analyzed both from the point 'with given probability' and 'with given error'.

Basic QFA models with measurement of a state only at the last step are listed below ($\mathtt{X}$ ($|\mathtt{X}| = m$) is input alphabet and with every letter $\mathtt{x} \in \mathtt{X}$ some unitary operator $U_{\mathtt{x}}$ acting in n-dimensional complex space $\mathbb{C}^n$ is associated).

The model MO-1QFA [35] is 1-way 1-head QTM $\mathtt{M} = (\mathtt{Q}, \mathtt{X}, |\varphi\rangle, \mathtt{Q}_{acc})$, where $\mathtt{Q} = \mathrm{B}_n$ ($\mathrm{B}_n = \{|i\rangle | i \in \mathbb{N}_n\}$) is the set of basic states, the unit vector $|\varphi\rangle \in \mathbb{C}^n$ is the pure initial state and $\mathtt{Q}_{acc} \subseteq \mathrm{B}_n$ is the set of accepting states. Probability that $\mathtt{M}$ accepts a string $w = x_1 \dots x_l \in X^+$ equals to $\mathrm{P}(|\varphi\rangle, w) = \| P_{acc} U_w |\varphi\rangle \|^2$, where $U_w = U_{x_l} \dots U_{x_1}$ and P_{acc} is the projection operator on the subspace spanned by $\mathtt{Q}_{acc}$.

The model L-QFA [36] differs from the model MO-1QFA only that it deals with some initial mixed state $\{(|\varphi_i\rangle, \alpha_i)\}_{i \in \mathbb{N}_n}$ such that $|\varphi_i\rangle \in \mathbb{C}^n$ ($i \in \mathbb{N}_n$) are pair-wise different unit vectors, $\alpha_i > 0$ ($i \in \mathbb{N}_n$), and $\sum\limits_{i \in \mathbb{N}_n} \alpha_i = 1$ (α_i ($i \in \mathbb{N}_n$) is referred to as probability that at initial instant QTM $\mathtt{M}$ exists in the state $|\varphi_i\rangle$).

Probability that L-QFA $\mathtt{M}$ accepts a string $w \in X^+$ equals to $\mathrm{P}(\{(|\varphi_i\rangle, \alpha_i)\}_{i \in \mathbb{N}_n}, w) = \sum\limits_{i \in \mathbb{N}_n} \alpha_i \mathrm{P}(|\varphi_i\rangle, w)$.

The model kQFA [37] is 1-way k-head QTM $\mathtt{M} = (\mathtt{Q}, \mathtt{T}, |\varphi\rangle, \mathtt{Q}_{acc})$ (at any instant all heads move simultaneously by one cell to the right), where $\mathtt{T} = \mathtt{X}^k \cup \bigcup\limits_{i=1}^{k-1} \mathtt{X}^i \{\Lambda\}^{k-i}$. It is worth to note that similarly to the case when the model L-QFA was defined as some generalization of the model MO-1QFA, in [38] the model L-kQFA was defined as some generalization of the model kQFA.

Currently, analysis of QFA models is focused on detailed study of the set of accepted languages, as well as on resolving of the problem of identification of equivalent states. Some research of languages accepted by above listed models of QFA is presented in Section 4 of the current paper.

3 Automata over algebraic structures

Let $\mathcal{K} = (K, +, \cdot)$ be fixed finite ring and $\mathcal{M} = \{\mathtt{M}_{\mathbf{a}}\}_{\mathbf{a} \in \mathbf{A}}$ ($\mathbf{A} \subseteq K^l$) be any family of FA

$$\mathtt{M}_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbb{Z}_+),$$

where $\mathbf{f}_1 : K^{n_1+n_2+l} \to K^{n_1}$ and $\mathbf{f}_2 : K^{n_1+n_2+l} \to K^{n_3}$ are fixed mappings, and $\mathbf{a}$ are parameters. It is known that via any experiment with an automaton $\mathtt{M}_{\mathbf{a}}$ the values of parameters $\mathbf{a} \in \mathbf{A}$ not always can be identified uniquely. So naturally arises the problem of design of some algorithm that simulates any $\mathtt{M}_{\mathbf{a}} \in \mathcal{M}$ with some accuracy (from the standpoint of cryptography this means 'an attack on the algorithm'). This problem has been resolved in [39, 40]. The essence of proposed solution is as follows.

We fix a set of parameters $\mathbf{B} \subseteq K^{l_1}$ and three families of mappings $\{\varphi^{(1)}_{\mathbf{b}} : K^{n_1+n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$, $\{\varphi^{(2)}_{\mathbf{b}} : K^{n_1} \times \bigcup\limits_{j=1}^{r-1} (K^{n_3})^j \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$ and $\{\varphi^{(3)}_{\mathbf{b}} : K^{n_1+rn_3+n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$. Let $\mathcal{G}_{\mathbf{B}} = \{G_{\mathbf{b}}\}_{\mathbf{b}\in\mathbf{B}}$ be the set of mappings, such that $G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ $(\mathbf{b} \in \mathbf{B}, m \in \mathbb{N})$, where

$$\mathbf{y}_i = \begin{cases} \varphi^{(1)}_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1), & \text{if } i = 1 \\ \varphi^{(2)}_{\mathbf{b}}(\mathbf{q}_0, \mathbf{y}_1 \dots \mathbf{y}_{i-1}, \mathbf{x}_i), & \text{if } i = 2, \dots, r \\ \varphi^{(3)}_{\mathbf{b}}(\mathbf{q}_0, \mathbf{y}_{i-r} \dots \mathbf{y}_{i-1}, \mathbf{x}_i), & \text{if } r < i \le m \end{cases} .$$

Let $H_{\mathbf{b},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m)$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1}, m \in \mathbb{N})$. It is evident that each family $\mathcal{H}_{\mathbf{b}} = \{H_{\mathbf{b},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^{n_1}}$ $(\mathbf{b} \in \mathbf{B})$ defines some finite automaton over the ring $\mathcal{K}$. Fixing surjection $h : \mathbf{A} \to \mathbf{B}$ we associate some family $\mathcal{H}_{h(\mathbf{a})}$ with every automaton $\mathtt{M}_{\mathbf{a}} \in \mathcal{M}$.

The ordered pair $(\mathcal{G}_{\mathbf{B}}, h)$ is defined as simulation model for the family $\mathcal{M}$. It is supposed that equalities $H_{h(\mathbf{a}),\mathbf{q}_0}\big|_{\bigcup\limits_{i=1}^{r}(K^{n_2})^i} = F_{\mathbf{a},\mathbf{q}_0}\big|_{\bigcup\limits_{i=1}^{r}(K^{n_2})^i}$ $(\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$ hold, where $F_{\mathbf{a},\mathbf{q}_0} : (K^{n_2})^+ \to (K^{n_3})^+$ is the mapping realized by initial automaton $(\mathtt{M}_{\mathbf{a}}, \mathbf{q}_0)$. Semantics of these equalities is that simulation model $(\mathcal{G}_{\mathbf{B}}, h)$, connected to the input and the output channels of an automaton $\mathtt{M}_{\mathbf{a}}$ $(\mathbf{a} \in \mathbf{A})$ passes the first r output symbols, and then blocks the output channel of an automaton $\mathtt{M}_{\mathbf{a}}$ and simulates its behavior on the remaining tail of input string.

On the base of standard techniques of algorithms theory accuracy of simulation model $(\mathcal{G}_{\mathbf{B}}, h)$ has been defined for all combinations of notions 'in the worst case' and 'in average'. Asymptotically exact sim-

ulation models have been extracted and some sufficient conditions for existence of these models have been established in [39, 40].

It is evident that any hash function is some mapping of input semigroup into the set of states realized by some finite initial automaton. From the standpoint of cryptography analysis of hash functions families defined by outputless FA over finite ring is actual. This problem has been investigated in [41]. The main results are as follows.

Let $\mathcal{F}_{k,m}$ $(k \leq m)$ be the set of all mappings $\mathbf{f} : K^{k+m} \to K^k$, such that the following two equalities $|\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\}| = |K|^{m-k}$ and $\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \emptyset$ hold for all $\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k$ $(\mathbf{q} \neq \mathbf{q}')$. It is evident that any mapping $\mathbf{f} \in \mathcal{F}_{k,m}$ defines strongly connected outputless automaton $\mathtt{M}_{\mathbf{f}}$, such that K^k is the set of states and K^m is input alphabet.

Let $H_{\mathbf{f},\mathbf{q}_0}$ be the mapping of input semigroup $(K^m)^+$ into the set of states K^k realized by initial automaton $(\mathtt{M}_{\mathbf{f}}, \mathbf{q}_0)$. Thus, automaton $\mathtt{M}_{\mathbf{f}}$ defines the family of hash functions $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$.

The following theorems are true:

Theorem 1. [41]. *For any mapping* $\mathbf{f} \in \mathcal{F}_{k,m}$ *if* $\mathbf{q}_0 \neq \mathbf{q}_0'$ $(\mathbf{q}_0, \mathbf{q}_0' \in K^k)$, *then* $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) \neq H_{\mathbf{f},\mathbf{q}_0'}(\mathbf{u})$ *for any input string* $\mathbf{u} \in (K^m)^+$.

Corollary 1. [41]. *For any* $\mathbf{f} \in \mathcal{F}_{k,m}$ *if* $\mathbf{q}_0 \neq \mathbf{q}_0'$ $(\mathbf{q}_0, \mathbf{q}_0' \in K^k)$, *then* $H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}) \cap H^{-1}_{\mathbf{f},\mathbf{q}_0'}(\mathbf{q}) = \emptyset$ *for any* $\mathbf{q} \in K^k$.

Theorem 2. [41]. *For any mapping* $\mathbf{f} \in \mathcal{F}_{k,m}$ *and* $\mathbf{q}_0 \in K^k$ *equality* $|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t) \cap (K^m)^t| = |K|^{tm-k}$ $(\mathbf{q}_t \in K^k)$ *holds for all* $t \in \mathbb{N}$.

Let $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ be probability that input string $\mathbf{u}$ randomly selected in the set $(K^m)^t$ is some solution of the equation $H(\mathbf{u}) = \mathbf{q}$, and $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ be probability that for two different input strings $\mathbf{u}$ and $\mathbf{u}'$ randomly selected in the set $(K^m)^t$ equality $H(\mathbf{u}) = H(\mathbf{u}')$ holds.

The following theorems are true:

Theorem 3. [41]. *For any mapping* $\mathbf{f} \in \mathcal{F}_{k,m}$ and $\mathbf{q}_0, \mathbf{q} \in K^k$ *equality* $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q}) = |K|^{-k}$ *holds for all* $t \in \mathbb{N}$.

Theorem 4. [41]. *For any mapping* $\mathbf{f} \in \mathcal{F}_{k,m}$ *and* $\mathbf{q}_0 \in K^k$ *equality* $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}(1 - \frac{|K|^k - 1}{|K|^{mt} - 1})$ *holds for all* $t \in \mathbb{N}$.

Thus, the number $|K|^{-k}$ characterizes computing security for a fam-

ily of hash functions $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$. This implies some feasibility for using these families in resolving problems of information protection.

Applications of elliptic curves over finite fields for resolving problems of information transformation justify feasibility of research FA defined on varieties (i.e. on the sets of solutions of systems of algebraic equations) over finite ring. It allows to set internal connections between modern algebraic geometry, systems theory, FA theory and cryptology.

From standpoint of algebraic FA theory and its applications it is reasonable to deal with the set $\mathcal{V}_1(\mathcal{K})$ of all varieties $\mathbf{V} \subseteq K^n$ with some algebra $(\mathbf{V}, \mathcal{F}_1 \cup \mathcal{F}_2)$, where $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ and $\mathcal{F}_2 = \{\beta_1, \ldots, \beta_{k_2}\}$ are the sets of unary and binary operations, correspondingly. For any variety $\mathbf{V} \in \mathcal{V}_1(\mathcal{K})$ the algebra $(\mathbf{V}, \mathcal{F}_1 \cup \mathcal{F}_2)$ gives possibility to define the set $\mathcal{A}^{(1)}(\mathbf{V})$ of Mealy FA

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_2)) \end{cases} \quad (t \in \mathbb{Z}_+)$$

and the set $\mathcal{A}^{(2)}(\mathbf{V})$ of Moore FA

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}), \mathbf{v}_2) \end{cases} \quad (t \in \mathbb{Z}_+),$$

where $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ are fixed points, $i_1, i_2 \in \mathbb{Z}_{k_1+1}$ and $j_1, j_2 \in \mathbb{N}_{k_2}$ are fixed integers, $\mathbf{q}_0 \in \mathbf{V}$, and $x_{t+1} \in \mathbb{Z}_{k_1+1}$ $(t \in \mathbb{Z}_+)$. Thus, for any $\mathtt{M} \in \mathcal{A}^{(1)}(\mathbf{V}) \cup \mathcal{A}^{(2)}(\mathbf{V})$ values of x_t, $\mathbf{q}_t$ and $\mathbf{y}_t$ are, correspondingly, an input symbol, a state and an output symbol at instant t.

Let $\mathbf{V}, \mathbf{U} \in \mathcal{V}_1(\mathcal{K})$. We say that: 1) the variety $\mathbf{U}$ is a homomorphic image of the variety $\mathbf{V}$, if the algebra $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ is a homomorphic image of the algebra $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$; 2) varieties $\mathbf{U}$ and $\mathbf{V}$ are isomorphic if algebras $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ and $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ are isomorphic.

The next theorem is true:

Theorem 5. [42]. *Let $\mathbf{U}, \mathbf{V} \in \mathcal{V}_1(\mathcal{K})$. If $\mathbf{U}$ is a homomorphic image of $\mathbf{V}$, then there exist mappings $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$, such that homomorphic image of any automaton $\mathtt{M}_j \in \mathcal{A}^{(j)}(\mathbf{V})$ is the automaton $\Psi_j(\mathtt{M}_j)$.*

Corollary 2. [42]. *Let* $\mathbf{U}, \mathbf{V} \in \mathcal{V}_1(\mathcal{K})$. *If* $\mathbf{U}$ *and* $\mathbf{V}$ *are isomorphic varieties, then there exist mappings* $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$, *such that automata* $\mathtt{M}_j \in \mathcal{A}^{(j)}(\mathbf{V})$ and $\Psi_j(\mathtt{M}_j)$ *are isomorphic.*

Any elliptic curve γ over a finite field $\mathcal{K} = (K, +, \cdot)$ defines the abelian group $(G_\gamma, +_\gamma)$, where G_γ is the set of all points of γ including specified point $\mathcal{O}$ (this point serves as the neutral element of the group). Setting $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ $(1 \le k_1 < |G_\gamma|)$, where $\alpha_0(P) = \mathcal{O}$ $(P \in G_\gamma)$ and $\alpha_i(P) = \underbrace{P +_\gamma \ldots +_\gamma P}_{i \text{ times}}$ $(P \in G_\gamma)$ for all $i = 1, \ldots, k_1$, and $\mathcal{F}_2 = \{+_\gamma\}$, we get some algebra $(G_\gamma, \mathcal{F}_1 \cup \mathcal{F}_2)$. Thus, any elliptic curve γ defines some variety of above considered type.

For any $P_1, P_2 \in G_\gamma \backslash \{\mathcal{O}\}$ and $n, m \in \mathbb{N}_{k_1}$ recurrence relations

$$\begin{cases} q_{t+1} = nq_t +_\gamma x_t P_1 \\ y_{t+1} = mq_t +_\gamma x_t P_2 \end{cases} \quad (t \in \mathbb{Z}_+)$$

and

$$\begin{cases} q_{t+1} = nq_t +_\gamma x_t P_1 \\ y_{t+1} = mq_{t+1} \end{cases} \quad (t \in \mathbb{Z}_+),$$

where $x_{t+1} \in \mathbb{N}_{k_1}$, define the family $\mathcal{M}_{1,\gamma,k_1}$ of Mealy FA and the family $\mathcal{M}_{2,\gamma,k_1}$ of Moore FA, correspondingly.

The following theorems are true:

Theorem 6. [43]. *For any automaton* $\mathtt{M}_1 \in \mathcal{M}_{1,\gamma,k_1}$ *identification of its initial state (with the accuracy to the set of equivalent states) is reduced to searching any solution of equation* $mu = a_0$, *where an element* $a_0 \in G_\gamma$ *is determined as the result of some simple experiment of the length* 1 *with the automaton* $\mathtt{M}_1$.

Theorem 7. [43]. *For any automaton* $\mathtt{M}_2 \in \mathcal{M}_{2,\gamma,k_1}$ *identification of its initial state (with the accuracy to the set of equivalent states) is reduced to searching any solution of equation* $mnv = b_0$, *where an element* $b_0 \in G_\gamma$ *is determined as the result of some simple experiment of the length* 1 *with the automaton* $\mathtt{M}_2$.

Theorem 8. [43]. *Exact imitation model for the family* $\mathcal{M}_{1,\gamma,k_1}$ *of Mealy FA can be designed as the result of some multiple experiment of the multiplicity* 3 *and of the height not exceeding* $|G_\gamma| + 1$. *The total*

length of all input strings applied to the investigated automaton in this experiment does not exceed $|G_\gamma| + 1 + 0.5|G_\gamma| \cdot (|G_\gamma| + 3)$.

Theorem 9. [43]. *Exact imitation model for the family* $\mathcal{M}_{2,\gamma,k_1}$ *of Moore FA can be designed as the result of some multiple experiment of the multiplicity* 2 *and of the height not exceeding* $|G_\gamma|$. *The total length of all input strings applied to the investigated automaton in this experiment does not exceed* $|G_\gamma| + 0.5|G_\gamma| \cdot (|G_\gamma| + 1)$.

These results imply some feasibility for using the above considered families of FA in resolving problems of information protection.

4 Quantum Automata

QFA under supposition that unitary operators associated with input alphabet commute each with the others have been investigated in [44]. Languages accepted either with given probability, or with given error have been characterized as follows.

Let $\mathtt{X} = \{\mathtt{x}_1, \ldots, \mathtt{x}_m\}$ be the input alphabet of QFA. It is supposed that elements of the set $\mathcal{U} = \{U_i | i \in \mathbb{N}_m\}$ (U_i is unitary operator associated with $\mathtt{x}_i \in \mathtt{X}$) commute each with the others. With any input string $\mathtt{w} \in \mathtt{X}^l$ ($l \in \mathbb{N}$) the string $pr_{\mathcal{U}}(\mathtt{w}) = U_1^{r_1} \ldots U_m^{r_m}$ can be associated, where r_i ($i \in \mathbb{N}_m$) is the number of occurrences of $\mathtt{x}_i$ in $\mathtt{w}$.

Let $\equiv_{\mathtt{X},\mathcal{U}}$ be equivalence on the set $\mathtt{X}^+$ defined as follows: for any input strings $\mathtt{w}_1, \mathtt{w}_2 \in \mathtt{X}^+$

$$\mathtt{w}_1 \equiv_{\mathtt{X},\mathcal{U}} \mathtt{w}_2 \Leftrightarrow pr_{\mathcal{U}}(\mathtt{w}_1) = pr_{\mathcal{U}}(\mathtt{w}_2).$$

The following theorem is true:

Theorem 10. [44]. *Let* $\mathcal{U}$ *be any set of unitary operators that commute each with the others. Then any language accepted (either with given probability, or with given error) by the model MO-1QFA, as well as by the model L-QFA with measurement at final instant only is union of some elements of the factor-set* $\mathtt{X}^+/\equiv_{\mathtt{X},\mathcal{U}}$.

It is evident that with any element $B \in \mathtt{X}^+/\equiv_{\mathtt{X},\mathcal{U}}$ unique unitary operator U_B can be associated, such that $U_B = pr_{\mathcal{U}}(\mathtt{w})$ for all $w \in B$. Let $\equiv'_{\mathtt{X},\mathcal{U}}$ be any equivalence on the set $\mathtt{X}^+$, such that every element

of the factor-set $\mathtt{X}^+/\equiv'_{\mathtt{X},\mathcal{U}}$ is union of some elements $B \in \mathtt{X}^+/\equiv_{\mathtt{X},\mathcal{U}}$ to which the same unitary operator U_B is associated.

The following corollary is true.

Corollary 3. [44]. *Let $\mathcal{U}$ be any set of unitary operators that commute each with the others. Then any language accepted (either with given probability, or with given mistake) by the model MO-1QFA, as well as by the model L-QFA with measurement at final instant only is union of some elements of the factor-set $\mathtt{X}^+/\equiv'_{\mathtt{X},\mathcal{U}}$.*

Important special case of equivalence $\equiv'_{\mathtt{X},\mathcal{U}}$ on the set $\mathtt{X}^+$ takes place in the following situation.

Let $\mathcal{U} = \{U_i | i \in \mathbb{N}_m\}$ ($U_i \neq I$ for all $i \in \mathbb{N}_m$) be some set of unitary operators that commute each with the others, such that for every $i \in \mathbb{N}_m$ there exists some positive integer a_i that satisfies the identity $U_i^{a_i} = I$. In what follows it is assumed that a_i ($i \in \mathbb{N}_m$) is the minimal positive integer that satisfies this identity. We define equivalence $\equiv^{(1)}_{\mathtt{X},\mathcal{U}}$ on the set $\mathtt{X}^+$ in the following way: for any input strings $\mathtt{w}_1, \mathtt{w}_2 \in \mathtt{X}^+$ ($pr_{\mathcal{U}}(\mathtt{w}_i) = U_1^{r_{i1}} \dots U_m^{r_{im}}$ $(i = 1, 2)$)

$$\mathtt{w}_1 \equiv^{(1)}_{\mathtt{X},\mathcal{U}} \mathtt{w}_2 \Leftrightarrow$$

$$\Leftrightarrow U_1^{r_{11}(mod\, a_1)} \dots U_m^{r_{1m}(mod\, a_m)} = U_1^{r_{21}(mod\, a_1)} \dots U_m^{r_{2m}(mod\, a_m)}.$$

It is evident that the equivalence $\equiv^{(1)}_{\mathtt{X},\mathcal{U}}$ is some special case of equivalence $\equiv'_{\mathtt{X},\mathcal{U}}$. Moreover, the following identity holds: $|\mathtt{X}^+/\equiv^{(1)}_{\mathtt{X},\mathcal{U}}| = \prod_{i=1}^{m} a_i$.

Thus, the following corollary is true.

Corollary 4. [44]. *Let $\mathcal{U} = \{U_i | i \in \mathbb{N}_m\}$ ($U_i \neq I$ for all $i \in \mathbb{N}_m$) be some set of unitary operators that commute each with the others, such that for every $i \in \mathbb{N}_m$ there exists some positive integer a_i that satisfies the identity $U_i^{a_i} = I$. Then any language accepted (either with given probability, or with given mistake) by the model MO-1QFA, as well as by the model L-QFA with measurement at final instant only is union of some elements of the factor-set $\mathtt{X}^+/\equiv^{(1)}_{\mathtt{X},\mathcal{U}}$.*

Similar results can be established for models kQFA and L-kQFA under supposition that unitary operators associated with elements of

the set $\mathtt{X}^k$ commute each with the others. However, some technical difficulties arise with definition of equivalence on the set $\mathtt{T}^+$ due to the presence of elements of the set $\bigcup\limits_{i=1}^{k-1} \mathtt{X}^i\{\Lambda\}^{k-i}$.

In [38] presented above approach has been worked out in detail for one of the most simple non-trivial models of QFA, namely 1-qubit QA under supposition that associated unitary operators are rotations of the Bloch sphere [5, 6] around the y-axe and measurement of a state is produced at final instant only. Criteria when investigated models MO-1QFA, L-QFA, kQFA and L-kQFA accept some language with given probability, as well as with given error has been established.

These results imply feasibility of investigation of the structure of the set of all finitely generated commutative semigroups of special unitary operators in $\mathbb{C}^2$ (the notion 'special' means that the determinant of a matrix that defines unitary operator equals to unit). This problem has been investigated in [45]. Main results are as follows.

Let $\mathcal{V}$ be the set of all special unitary operators $V : \mathbb{C}^2 \to \mathbb{C}^2$ and $\mathfrak{S}$ be the set of all finitely generated commutative semigroups $\mathcal{G} = (G, \cdot)$ ($G \subseteq \mathcal{V}$). The semigroup generated by elements $V_1, \ldots, V_k \in \mathcal{V}$ is denoted $(\langle V_1, \ldots, V_k\rangle, \cdot)$. Without loss of generality it can be suggested that for any semigroup $(\langle V_1, \ldots, V_k\rangle, \cdot) \in \mathfrak{S}$ ($k \geq 2$) the following condition holds: $(\forall r_1, r_2 \in \mathbb{N}_k)(r_1 \neq r_2 \Rightarrow (\forall n \in \mathbb{N})(V_{r_1}^n \neq V_{r_2}))$.

For any $\gamma \in [0, 4\pi)$ we denote $R_\gamma^{(1)}$, $R_\gamma^{(2)}$ and $R_\gamma^{(3)}$ rotations of the Bloch sphere through the angle 0.5γ around, correspondingly, the x-axe, the y-axe and the z-axe. It is worth to note that any special unitary operator $V \in \mathcal{V}$ can be presented as superposition $V = R_{\gamma_1}^{(3)} R_{\gamma_2}^{(2)} R_{\gamma_3}^{(3)}$ for some $\gamma_1, \gamma_2, \gamma_3 \in [0, 4\pi)$.

The set $\mathfrak{S}_1 = \{(\langle V\rangle, \cdot) | V \in \mathcal{V}\}$ consists of all commutative cyclic semigroups $\mathcal{G} \in \mathfrak{S}$. Setting $\mathfrak{S}_1^{(l)} = \{(\langle V\rangle, \cdot) | V \in \mathcal{V}^{(l)}\}$ ($l = 1, 2, 3$), where $\mathcal{V}^{(l)} = \{R_\gamma^{(l)} | \gamma \in [0, 4\pi)\}$ ($l = 1, 2, 3$), we extract in the set $\mathfrak{S}_1$ the sets of all commutative cyclic semigroups of rotation of the Bloch sphere through fixed angle around fixed coordinate axe. It is evident that $(\langle R_\gamma^{(l)}\rangle, \cdot)$ ($\gamma \in [0, 4\pi); l = 1, 2, 3$) is finite semigroup if and only if $\gamma (mod\, \pi) \in \mathbb{Q}_+$.

For any integer $k \geq 2$ we set

$$\mathfrak{S}_{2l}^{(k)} = \{(\langle R_{\gamma_1}^{(l)}, \ldots, R_{\gamma_k}^{(l)} \rangle, \cdot) | R_{\gamma_1}^{(l)}, \ldots, R_{\gamma_k}^{(l)} \in \mathcal{V}^{(l)} \&$$

$$\&(\forall r_1, r_2 \in \mathbb{N}_k)(\forall n \in \mathbb{N})(r_1 \neq r_2 \Rightarrow (R_{\gamma_{r_1}}^{(l)})^n \neq R_{\gamma_{r_2}}^{(l)})\} \quad (l = 1, 2, 3).$$

The set $\mathfrak{S}_2 = \bigcup\limits_{l=1}^{3} \bigcup\limits_{k=2}^{\infty} \mathfrak{S}_{2l}^{(k)}$ consists of all finitely generated commutative non-cyclic semigroups of rotation of the Bloch sphere around fixed coordinate axe. It is evident that $(\langle R_{\gamma_1}^{(l)}, \ldots, R_{\gamma_k}^{(l)} \rangle, \cdot) \in \mathfrak{S}_{2l}^{(k)}$ $(k \in \mathbb{N}$ $(k \geq 2)$ and $l = 1, 2, 3)$ is finite semigroup if and only if $\gamma_r (mod\, \pi) \in \mathbb{Q}_+$ for all integers $r \in \mathbb{N}_k$.

Now we investigate conditions under which two different special unitary operators of general form commute. Let

$$V_j = \begin{pmatrix} e^{i\alpha_j} \cos 0.5\gamma_j & -e^{-i\beta_j} \sin 0.5\gamma_j \\ e^{i\beta_j} \sin 0.5\gamma_j & e^{-i\alpha_j} \cos 0.5\gamma_j \end{pmatrix} \in \mathcal{V} \quad (j = 1, 2),$$

where $\alpha_j, \beta_j \in [0, 2\pi)$ $(j = 1, 2)$ and $\gamma_j \in [0, 4\pi)$ $(j = 1, 2)$. Then

$$V_1 V_2 = V_2 V_1 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} (e^{i2(-\beta_1 + \beta_2)} - 1) \sin 0.5\gamma_1 \sin 0.5\gamma_2 = 0 \\ e^{i\beta_1} \sin \alpha_1 \sin 0.5\gamma_2 \cos 0.5\gamma_1 = e^{i\beta_2} \sin \alpha_2 \sin 0.5\gamma_1 \cos 0.5\gamma_2 \end{cases} \tag{1}$$

It is sufficient to set these or the others restrictions on the structure of special unitary operator V_1 and determine corresponding restrictions on the structure of special unitary operator V_2. Thus, we can analyze the following cases.

Case 1. Let $\sin 0.5\gamma_1 = 0$ $(\gamma_1 \in [0, 4\pi))$, i.e. $\gamma_1 \in \{0, 2\pi\}$ and $\cos 0.5\gamma_1 = \pm 1$. We get $V_1 \in \mathcal{V}_1(\alpha_1) = \{\widetilde{R}_{\alpha_1}^{(3)}, -\widetilde{R}_{\alpha_1}^{(3)}\}$ $(\alpha_1 \in [0, 2\pi))$, where

$$\widetilde{R}_{\alpha_1}^{(3)} = \begin{pmatrix} e^{i\alpha_1} & 0 \\ 0 & e^{-i\alpha_1} \end{pmatrix} \quad (\alpha_1 \in [0, 2\pi)),$$

i.e. $\widetilde{R}_{\alpha_1}^{(3)}$ is rotation of the Bloch sphere through the angle $-\alpha_1$ around the z-axe.

The second identity in (1) takes the form

$$\sin\alpha_1 \sin 0.5\gamma_2 = 0 \quad (\alpha_1 \in [0, 2\pi), \gamma_2 \in [0, 4\pi)). \tag{2}$$

The following cases can take place.

Case 1.1. Let $\sin 0.5\gamma_2 = 0$ ($\gamma_2 \in [0, 4\pi)$), i.e. $\gamma_2 \in \{0, 2\pi\}$ and $\cos 0.5\gamma_2 = \pm 1$. We get $V_2 \in \mathcal{V}_1(\alpha_2)$.

Let $\mathfrak{S}_3 = \bigcup\limits_{k=2}^{\infty} \mathfrak{S}_3^{(k)}$, where

$$\mathfrak{S}_3^{(k)} = \{(\langle V_1, \ldots, V_k\rangle, \cdot) | V_1, \ldots, V_k \in \bigcup_{\omega\in[0,2\pi)} \mathcal{V}_1(\omega) \&$$

$$\&(\forall r_1, r_2 \in \mathbb{N}_k)(\forall n \in \mathbb{N})(r_1 \neq r_2 \Rightarrow V_{r_1}^n \neq V_{r_2})\}.$$

For any fixed numbers $\alpha_{r_1}, \alpha_{r_2} \in [0, 2\pi)$ we get:

1) if $V_{r_1} = \widetilde{R}_{\alpha_{r_1}}^{(3)}$ and $V_{r_2} = \widetilde{R}_{\alpha_{r_2}}^{(3)}$ or $V_{r_1} = -\widetilde{R}_{\alpha_{r_1}}^{(3)}$ and $V_{r_2} = -\widetilde{R}_{\alpha_{r_2}}^{(3)}$, then identity $V_{r_1}^n = V_{r_2}$ holds for some integer $n \in \mathbb{N}$ if and only if relation $n\alpha_{r_1} - \alpha_{r_2} \equiv 0\,(mod\, 2\pi)$ holds;

2) if $V_{r_1} = \widetilde{R}_{\alpha_{r_1}}^{(3)}$ and $V_{r_2} = -\widetilde{R}_{\alpha_{r_2}}^{(3)}$, then identity $V_{r_1}^n = V_{r_2}$ holds for some integer $n \in \mathbb{N}$ if and only if $\pi^{-1}(n\alpha_{r_1} - \alpha_{r_2})$ is some odd integer;

3) if $V_{r_1} = -\widetilde{R}_{\alpha_{r_1}}^{(3)}$ and $V_{r_2} = \widetilde{R}_{\alpha_{r_2}}^{(3)}$, then identity $V_{r_1}^n = V_{r_2}$ holds for some $n \in \mathbb{N}$ if and only if either n and $\pi^{-1}(n\alpha_{r_1} - \alpha_{r_2})$ are odd integers, or n is some even integer and relation $n\alpha_{r_1} - \alpha_{r_2} \equiv 0\,(mod\, 2\pi)$ holds.

It is evident that the set $\mathfrak{S}_3$ consists of some finitely generated non-cyclic commutative semigroups and inclusion $\mathfrak{S}_3 \subset \mathfrak{S}_{23}^{(2)}$ holds.

Case 1.2. Let $\sin 0.5\gamma_2 \neq 0$ ($\gamma_2 \in [0, 4\pi)$), i.e. $\gamma_2 \in [0, 4\pi)\backslash\{0, 2\pi\}$. Identity (2) takes the form $\sin\alpha_1 = 0$ ($\alpha_1 \in [0, 2\pi)$), i.e. $\alpha_1 \in \{0, \pi\}$. We get $V_1 \in \{I, -I\}$.

Let $\mathcal{V}_2 = \{I, -I\}$ and $\mathcal{V}_3$ be the set of all special unitary operators $V_2 \in \mathcal{V}$, such that $\gamma_2 \in [0, 4\pi)\backslash\{0, 2\pi\}$ and $V_2^n \notin \mathcal{V}_2$ for all $n \in \mathbb{N}$. We get some set $\mathfrak{S}_4 = \{(\langle V_1, V_2\rangle, \cdot) | V_1 \in \mathcal{V}_2, V_2 \in \mathcal{V}_3\}$ of finitely generated non-cyclic commutative semigroups.

Case 2. Let

$$\begin{cases} \sin 0.5\gamma_1 \neq 0 \quad (\gamma_1 \in [0, 4\pi)) \\ \sin 0.5\gamma_2 \neq 0 \quad (\gamma_2 \in [0, 4\pi)) \end{cases},$$

i.e. $\gamma_j \in [0, 4\pi)\backslash\{0, 2\pi\}$ $(j = 1, 2)$. The first identity in (1) takes the form $e^{i2(-\beta_1+\beta_2)} - 1 = 0$ $(\beta_1, \beta_2 \in [0, 2\pi))$. Without loss of generality we can assume that $\beta_1 \leq \beta_2$. We get that either $\beta_1 = \beta_2$ and

$$V_j = \begin{pmatrix} e^{i\alpha_j} \cos 0.5\gamma_j & -e^{-i\beta_1} \sin 0.5\gamma_j \\ e^{i\beta_1} \sin 0.5\gamma_j & e^{-i\alpha_j} \cos 0.5\gamma_j \end{pmatrix} \quad (j = 1, 2),$$

or $\beta_2 = \beta_1 + \pi$ and

$$V_1 = \begin{pmatrix} e^{i\alpha_1} \cos 0.5\gamma_1 & -e^{-i\beta_1} \sin 0.5\gamma_1 \\ e^{i\beta_1} \sin 0.5\gamma_1 & e^{-i\alpha_1} \cos 0.5\gamma_1 \end{pmatrix},$$

$$V_2 = \begin{pmatrix} e^{i\alpha_2} \cos 0.5\gamma_2 & e^{-i\beta_1} \sin 0.5\gamma_2 \\ -e^{i\beta_1} \sin 0.5\gamma_2 & e^{-i\alpha_2} \cos 0.5\gamma_2 \end{pmatrix}.$$

The second identity in (1) takes the form

$$\sin\alpha_1 \sin 0.5\gamma_2 \cos 0.5\gamma_1 = \sin\alpha_2 \sin 0.5\gamma_1 \cos 0.5\gamma_2, \tag{3}$$

where $\gamma_1, \gamma_2 \in [0, 4\pi)\backslash\{0, 2\pi\}$. The following cases can take place.

Case 2.1. Let $\cos 0.5\gamma_1 = 0$ $(\gamma_1 \in [0, 4\pi)\backslash\{0, 2\pi\})$, i.e. $\gamma_1 \in \{\pi, 3\pi\}$. We get $V_1 \in \mathcal{V}_4(\beta_1) = \{J_{\beta_1}, -J_{\beta_1}\}$ $(\beta_1 \in [0, 2\pi))$, where

$$J_{\beta_1} = \begin{pmatrix} 0 & -e^{-i\beta_1} \\ e^{i\beta_1} & 0 \end{pmatrix} \quad (\beta_1 \in [0, 2\pi)).$$

Identity (3) takes the form

$$\sin\alpha_2 \cos 0.5\gamma_2 = 0 \quad (\gamma_2 \in [0, 4\pi)\backslash\{0, 2\pi\}, \alpha_2 \in [0, 4\pi)).$$

The following cases can take place.

Case 2.1.1. Let $\cos 0.5\gamma_2 = 0$, i.e. $\gamma_2 \in \{\pi, 3\pi\}$. Since $V_2 \in \mathcal{V}_4(\beta_1)$ and $V_2 \neq V_1$, then $V_2 = -V_1$. For any $\beta_1 \in [0, 2\pi)$ identity $J_{\beta_1}^2 = -I$ holds. We get some set $\mathfrak{S}_5 = \{(\langle V, -V\rangle, \cdot) | V \in \bigcup\limits_{\beta_1 \in [0,2\pi)} \mathcal{V}_4(\beta_1)\}$ of finite non-cyclic commutative semigroups.

Case 2.1.2. Let $\cos 0.5\gamma_2 \neq 0$, i.e. $\gamma_2 \in [0, 4\pi)\backslash\{0\pi, 2\pi, 3\pi\}$. Then $\sin\alpha_2 = 0$, i.e. $\alpha_2 \in \{0, \pi\}$. Since $e^{i\alpha_2} = \pm 1$, then

$$V_2 \in \mathcal{V}_5(\beta_1) = \bigcup_{\gamma_2 \in [0,4\pi)\backslash\{0\pi,2\pi,3\pi\}} \mathcal{V}_5(\gamma_2, \beta_1) \quad (\beta_1 \in [0, 2\pi)),$$

where $\mathcal{V}_5(\gamma_2,\beta_1)=\{U_j(\gamma_2,\beta_1)|j=1,\dots,4\}$, and

$$U_1(\gamma_2,\beta_1)=\begin{pmatrix}\cos 0.5\gamma_2 & -e^{-i\beta_1}\sin 0.5\gamma_2\\ e^{i\beta_1}\sin 0.5\gamma_2 & \cos 0.5\gamma_2\end{pmatrix},$$

$$U_2(\gamma_2,\beta_1)=\begin{pmatrix}\cos 0.5\gamma_2 & e^{-i\beta_1}\sin 0.5\gamma_2\\ -e^{i\beta_1}\sin 0.5\gamma_2 & \cos 0.5\gamma_2\end{pmatrix},$$

$U_3(\gamma_2,\beta_1)=-U_2(\gamma_2,\beta_1)$ and $U_4(\gamma_2,\beta_1)=-U_1(\gamma_2,\beta_1)$.

It is evident that:

1) if $\beta_1=0$, then $U_1(\gamma_2,\beta_1)$ is rotation of the Bloch sphere through the angle $0.5\gamma_2$ around the y-axe;

2) if $\beta_1=1.5\pi$, then $U_2(\gamma_2,\beta_1)$ is rotation of the Bloch sphere through the angle $0.5\gamma_2$ around the x-axe.

We get some set

$$\mathfrak{S}_6=\bigcup_{\beta_1\in[0,2\pi)}\ \bigcup_{\gamma_2\in[0,4\pi)\setminus\{0\pi,2\pi,3\pi\}}\mathfrak{S}_6(\gamma_2,\beta_1)$$

of finitely generated non-cyclic commutative semigroups, where

$$\mathfrak{S}_6(\gamma_2,\beta_1)=\{(\langle V_1,V_2\rangle,\cdot)|V_1\in\mathcal{V}_4(\beta_1)\&$$

$$\&V_2\in\mathcal{V}_5(\gamma_2,\beta_1)\&(\forall n\in\mathbb{N})(V_2^n\neq V_1)\}.$$

Case 2.2. Let

$$\begin{cases}\cos 0.5\gamma_1\neq 0 & (\gamma_1\in[0,4\pi))\\ \cos 0.5\gamma_2\neq 0 & (\gamma_2\in[0,4\pi))\end{cases},$$

i.e. (see case 2) $\gamma_1,\gamma_2\in[0,4\pi)\setminus\{0,\pi,2\pi,3\pi\}$. The following cases can take place.

Case 2.2.1. Let $\sin\alpha_1=0$ ($\alpha_1\in[0,2\pi)$), i.e. $\alpha_1\in\{0,\pi\}$. Identity (3) takes the form $\sin\alpha_2=0$ ($\alpha_2\in[0,2\pi)$), i.e. $\alpha_2\in\{0,\pi\}$. We get that:

1) if $\beta_2=\beta_1$, then

$$V_j=\begin{pmatrix}\pm\cos 0.5\gamma_j & -e^{-i\beta_1}\sin 0.5\gamma_j\\ e^{i\beta_1}\sin 0.5\gamma_j & \pm\cos 0.5\gamma_j\end{pmatrix}\quad(j=1,2);$$

2) if $\beta_2 = \beta_1 + \pi$, then

$$V_1 = \begin{pmatrix} \pm\cos 0.5\gamma_1 & -e^{-i\beta_1}\sin 0.5\gamma_1 \\ e^{i\beta_1}\sin 0.5\gamma_1 & \pm\cos 0.5\gamma_1 \end{pmatrix},$$

$$V_2 = \begin{pmatrix} \pm\cos 0.5\gamma_2 & e^{-i\beta_1}\sin 0.5\gamma_2 \\ -e^{i\beta_1}\sin 0.5\gamma_2 & \pm\cos 0.5\gamma_2 \end{pmatrix}.$$

It is evident that $V_1 \in \mathcal{V}_6(\gamma_1, \beta_1) = \{U_1(\gamma_1, \beta_1), U_3(\gamma_1, \beta_1)\}$ and $V_2 \in \mathcal{V}_5(\gamma_2, \beta_1)$. We get some set $\mathfrak{S}_7 = \bigcup\limits_{\beta_1 \in [0,2\pi)} \mathfrak{S}_7(\beta_1)$ of finitely generated non-cyclic commutative semigroups, where

$$\mathfrak{S}_7(\beta_1) = \bigcup_{\gamma_1,\gamma_2 \in [0,4\pi)\setminus\{0,\pi,2\pi,3\pi\}} \{(\langle V_1, V_2\rangle, \cdot) | V_1 \in \mathcal{V}_6(\gamma_1, \beta_1) \&$$

$$\& V_2 \in \mathcal{V}_5(\gamma_2, \beta_1) \& (\forall n \in \mathbb{N})(V_1^n \neq V_2 \& V_2^n \neq V_1)\}.$$

Case 2.2.2. Let

$$\begin{cases} \sin\alpha_1 \neq 0 & (\alpha_1 \in [0, 2\pi)) \\ \sin\alpha_2 \neq 0 & (\alpha_2 \in [0, 2\pi)) \end{cases},$$

i.e. $\alpha_j \in [0, 2\pi)\setminus\{0, \pi\}$ $(j = 1, 2)$. Identity (3) takes the form

$$\frac{\sin\alpha_1}{\sin\alpha_2} = \pm\tan 0.5\gamma_1 \cot 0.5\gamma_2,$$

where $\gamma_1, \gamma_2 \in [0, 4\pi)\setminus\{0, \pi, 2\pi, 3\pi\}$ and $\alpha_1, \alpha_2 \in [0, 2\pi)\setminus\{0, \pi\}$.

Let $\mathfrak{S}'(\beta_1)$ be the set of all subsets $\{V_1, V_2\}$ of special unitary operators, such that:

1) unitary operators V_j $(j = 1, 2)$ are defined by formula

$$V_j = \begin{pmatrix} e^{i\alpha_j}\cos 0.5\gamma_j & -e^{-i\beta_1}\sin 0.5\gamma_j \\ e^{i\beta_1}\sin 0.5\gamma_j & e^{-i\alpha_j}\cos 0.5\gamma_j \end{pmatrix} \quad (j = 1, 2),$$

where $\gamma_1, \gamma_2 \in [0, 4\pi)\setminus\{0, \pi, 2\pi, 3\pi\}$ and $\alpha_1, \alpha_2 \in [0, 2\pi)\setminus\{0, \pi\}$;

2) identity $\frac{\sin\alpha_1}{\sin\alpha_2} = \tan 0.5\gamma_1 \cot 0.5\gamma_2$ holds;

3) disequalities $V_1^n \neq V_2$ $(n \in \mathbb{N})$ and $V_2^n \neq V_1$ $(n \in \mathbb{N})$ hold.

Similarly, let $\mathfrak{S}''(\beta_1)$ be the set of all subsets $\{V_1, V_2\}$ of special unitary operators, such that:

1) unitary operators V_j $(j = 1, 2)$ are defined by formulae

$$V_1 = \begin{pmatrix} e^{i\alpha_1}\cos 0.5\gamma_1 & -e^{-i\beta_1}\sin 0.5\gamma_1 \\ e^{i\beta_1}\sin 0.5\gamma_1 & e^{-i\alpha_1}\cos 0.5\gamma_1 \end{pmatrix},$$

$$V_2 = \begin{pmatrix} e^{i\alpha_2}\cos 0.5\gamma_2 & e^{-i\beta_1}\sin 0.5\gamma_2 \\ -e^{i\beta_1}\sin 0.5\gamma_2 & e^{-i\alpha_2}\cos 0.5\gamma_2 \end{pmatrix}.$$

where $\gamma_1, \gamma_2 \in [0, 4\pi)\backslash\{0, \pi, 2\pi, 3\pi\}$ and $\alpha_1, \alpha_2 \in [0, 2\pi)\backslash\{0, \pi\}$;

2) identity $\frac{\sin\alpha_1}{\sin\alpha_2} = -\tan 0.5\gamma_1 \cot 0.5\gamma_2$ holds;

3) disequalities $V_1^n \neq V_2$ $(n \in \mathbb{N})$ and $V_2^n \neq V_1$ $(n \in \mathbb{N})$ hold.

We get some set

$$\mathfrak{S}_8 = \bigcup_{\beta_1 \in [0,2\pi)} \{(\langle V_1, V_2\rangle, \cdot) | \{V_1, V_2\} \in \mathfrak{S}'(\beta_1)\} \cup$$

$$\cup \bigcup_{\beta_1 \in [0,2\pi)} \{(\langle V_1, V_2\rangle, \cdot) | \{V_1, V_2\} \in \mathfrak{S}''(\beta_1)\}$$

of finitely generated non-cyclic commutative semigroups.

Summarizing all the above, we conclude that the following theorem is true:

Theorem 11. *The following inclusion holds:* $\mathfrak{S} \supseteq \bigcup\limits_{j=1}^{8} \mathfrak{S}_j$.

Unfortunately, it is still unknown, if the identity $\mathfrak{S} = \bigcup\limits_{j=1}^{8} \mathfrak{S}_j$ holds.

5 Conclusions

In the given paper some research in two new trends of FA theory has been presented.

The first trend deals with investigation of FA families defined on algebraic structures over finite rings. The presented results justify some feasibility for using these families in resolving problems of information protection. Based on this viewpoint, the following further research can

be pointed. Firstly, searching non-trivial FA families for which any asymptotically accurate simulation model is much more complicated than a system of equations defining the family itself. Secondly, characterization of families of reversible FA for which transition to any simulation model results in essential loss of accuracy. Thirdly, detailed investigation into computational security of specific families of hash-functions determined by outputless automata over finite rings. Fourthly, detailed investigation into computational security of FA families defined on elliptic curves over finite fields.

The second trend deals with investigation of languages accepted by QFA models under supposition that unitary operators associated with input alphabet commute each with the others. In this direction, some progress in investigation of 1-qubit QFA have been achieved. However, no similar results are known for l-qubit QFA ($l \geq 2$). Possibly, the reason is that no visual geometric model which is similar to Bloch sphere is known for $l \geq 2$. Characterization of l-qubit QFA ($l \geq 2$) under supposition that unitary operators associated with input alphabet commute each with the others forms some trend for future research.

References

[1] A.M. Turing *On computable numbers, with an application to the Entscheidungsproblem.* Proc. London Math. Soc., ser. 2, vol. 42 (1936), pp. 230–265.

[2] *Automata studies* (Ed. by C.E. Shannon, J. McCarthy). Princeton University Press, 1956.

[3] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. *Handbook of applied cryptography.* CRC Press, 2001.

[4] J. Kaz, Y. Lindell. *Introduction to modern cryptography.* CRC Press, 2007.

[5] M.A. Nielsen, I.L. Chuang. *Quantum computation and quantum information.* Cambrige University Press, 2010.

[6] C.P. Williams. *Explorations in quantum computing.* Springer-Verlag London Limited, 2011.

[7] V.M. Glushkov. *Synthesis of digital automata.* Moskow, Nauka, 1962. [in Russian]

[8] Z. Kohavi. *Switching and finite automata theory.* New York, McGraw-Hill, 1970.

[9] B.A. Trachtenbrot, Y.M. Barzdin. *Finite automata. Behavior and synthesis.* North-Holland, 1973.

[10] A.A. Letichevskii. *Completeness conditions for finite automata.* USSR Computational Mathematics and Mathematical Physics, vol. 1, issue 3 (1962), pp. 829–840.

[11] M.I. Kratko. *Undecidability of completeness for finite automata.* Doklady AN SSSR, vol. 155, No 1 (1964), pp. 35–37. [in Russian]

[12] A. Gill. *Introduction to the theory of finite-state machines.* New York, McGraw-Hill, 1962.

[13] V.M. Glushkov. *The abstract theory of automata.* Russian Mathematical Surveys, vol. 16, No 5 (1961) , pp.1–53.

[14] S. Eilenberg. *Automata, languages and machines. Vol. A.* New York, Academic Press, 1974.

[15] S. Eilenberg. *Automata, languages and machines. Vol. B.* New York, Academic Press, 1976.

[16] V.M. Glushkov, G.E. Tseitlin, E.L. Yushchenko. *Algebra, languages, programming.* Kiev, Naukova Dumka, 1978. [in Russian]

[17] D.A. Huffman. *Canonical forms for information-lossless finite state logical machines.* IRE Transactions Circuit Theory. Special Supplement, vol. CT-6 (1959), pp. 41–59.

[18] S. Even. *On information-lossless automata of finite order.* IEEE Transactions on Electronic Computers, vol. C-14, 4 (1965), pp. 561–569.

[19] M.O. Rabin *Probabilistic automata.* Information and Control, No 3 (1963), pp. 230–245.

[20] A. Paz A. *Introduction to probabilistic automata.* New York, Academic Press, 1971.

[21] J.G. Kemeny, T.L. Snell. *Finite Markov chains.* Princeton, NJ: D. Van Nostrand, 1960.

[22] E.R. Berlekamp. *Algebraic coding theory.* New York, McGraw-Hill, 1968.

[23] W.W. Peterson, E.J. Weldon, Jr. *Error-correcting codes.* The M.I.T. Press, Cambridge, MA, 1972.

[24] L.A. Zadeh, C.A. Desoer. *Linear system theory.* New York, McGraw-Hill, 1963.

[25] A. Gill. *Linear sequential circuits – analysis, synthesis, and applications.* New York, McGraw-Hill, 1966.

[26] B.A. Sevastyanov, V.P. Chistyakov. *On the number of input sequences corresponding to the output sequences of a finite automaton.* Review of Applied and Industrial Mathematics, vol. 1, Moskow, TVP (1994), pp. 96–107. [in Russian]

[27] V.L. Kurakin, A.S. Kuz'min, A.A. Nechaev. *Pseudo-random and polylinear sequences.* Memoires in Discrete Mathematics, vol. 1, Moskow, TVP (1997), pp. 139–202. [in Russian]

[28] V.L. Kurakin, A.S. Kuz'min, A.A. Nechaev. *Properties of linear and polylinear recurrencies over Galois rings (I).* Memoires in Discrete Mathematics, vol. 2, Moskow, TVP (1998), pp. 191–222. [in Russian]

[29] D.V. Speransky. *Experiments with linear and bilinear finite automata.* Saratov, Saratov State University, 2004. [in Russian]

[30] A.V. Babash. *Approximate models for finite automata.* Review of Applied and Industrial Mathematics, vol. 12 (2005), pp. 108–117. [in Russian]

[31] N. Courtois, W. Meier. *Algebraic attack on stream ciphers with linear feedback.* LNCS, vol. 2656 (2003), pp. 345–349.

[32] V.N. Trenkaev, R.G. Kolesnikov. *Automata approach to attack on symmetric ciphers.* Bulletin of Tomsk State University. Appendix, No 23, (2007), pp. 130–135.

[33] V.V. Skobelev, V.G. Skobelev. *Ciphersystems analysis.* Donetsk, IAMM of NASU, 2009. [in Russian].

[34] V.V. Skobelev, N.M. Glazunov, V.G. Skobelev. *Varieties over rings. Theory and applications.* Donetsk, IAMM of NASU, 2011. [in Russian].

[35] C. Moore, J. Crutchfield. *Quantum automata and quantum grammars.* Theor. Comput. Sci., vol. 237 (2000), pp. 257–306.

[36] A. Ambainis, M. Beaudry, M. Golovkins, at al. *Algebraic results on quantum automata.* LNCS, vol. 2996 (2004), pp. 93–104.

[37] A. Belovs, A. Rosmanis A., J. Smotrovs. *Multi-letter reversible and quantum finite automata.* LNCS, vol. 4588 (2007), pp. 60–71.

[38] V.G. Skobelev. *Analysis of finite 1-qubit quantum automata unitary operators of which are rotations.* Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka, No. 2 (2014), pp. 194–201.

[39] V.V. Skobelev. *Simulation of automata over a finite ring by the automata with a finite memory.* Journal of Automation and Information Sciences, vol. 44, issue 5 (2012), pp. 57–66.

[40] V.V. Skobelev. *Analysis of the problem of recognition of automaton over some ring.* Dopov. Nats. Akad. Nauk Ukr., Mat., Pryr., Tekh. Nauky, No 9 (2012), pp. 29–35.

[41] V.V. Skobelev. *Analysis of families of hash functions defined by automata over a finite ring.* Cybern. Syst. Anal., vol. 49, No. 2 (2013), pp. 209–216.

[42] V.V. Skobelev. *Analysis of automata models determined on varieties ovef finite ring.* Journal of Automation and Information Sciences, vol. 45, issue 8 (2013), pp. 21–31.

[43] V.V. Skobelev. *Automata on algebraic structures.* Donetsk, IAMM of NASU, 2013. [in Russian]

[44] V.G. Skobelev. *Quantum automata with operators that commutes.* Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka, Special Issue (2013), pp. 34–41.

[45] V.G. Skobelev. *On the structure of the set of all finitely generated semigroups of special unitary operators in the space* $\mathbb{C}^2$. Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka, No. 3 (2014), pp. 182–187.

Volodymyr V. Skobelev, Volodymyr G. Skobelev Received September 16 , 2015

Volodymyr V. Skobelev
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
40 Glushkova ave., Kyiv, Ukraine, 03187
Phone: +38 063 431 86 05
E-mail: vvskobelev@incyb.kiev.ua

Volodymyr G. Skobelev
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
40 Glushkova ave., Kyiv, Ukraine, 03187
Phone: +38 063 431 86 05
E-mail: skobelevvg@mail.ru