УДК 519.713+530.145

Скобелєв В.Г., д.ф.-м.н., д.т.н., професор

Аналіз скінченних 1-кубітових квантових автоматів унітарні оператори яких є оберненнями.

Інститут прикладної математики і механіки НАН України, 83114, м. Донецьк, вул. Рози Люксембург, 74,
e-mail: skbv@iamm.ac.donetsk.ua

V. G. Skobelev, Dr. (Phys.-Math., Tech.) Sci, Prof.

Analysis of finite 1-qubit quantum automata unitary operators of which are rotations.

Institute of Applied Mathematics and Mechanics of NAS of Ukraine, 83114, Rose Luxemburg str., 74,
e-mail: skbv@iamm.ac.donetsk.ua

У статті досліджено моделі скінченних 1-кубітовіх квантових автоматів у припущенні, що асоційовані унітарні оператори визначають обернення сфери Блоха навколо осі ординат, а вимірювання стану здійснюється лише в останній момент часу. Об'єктом дослідження є моделі MO-1QFA та k QFA $(k \geq 2)$, які здійснюють перетворення чистого початкового стану автомата, а також їх узагальнення L-QFA та L-k QFA $(k \geq 2)$, які здійснюють перетворення змішаного початкового стану автомата (тобто скінченної множини можливих початкових станів, кожний з котрих може мати місце з заданою ймовірністю). Предметом дослідження є мови, які вказані моделі розпізнають або з заданою ймовірністю, або з заданою похибкою. Структуру цих мов охарактеризовано у термінах фактор-множин, які визначено на основі вказаної властивості унітарних операторів. Встановлено критерії, при котрих вказані мови є скінченними множинами.

Ключові слова: скінченні 1-кубітові квантові автомати, обернення сфери Блоха навколо осі координат.

In the given paper there are investigated models of finite 1-qubit quantum automata under assumption that associated unitary operators are rotations of the Bloch sphere around the y-axe, and measurement of a state is produced at final instant only. The objects of investigation are models MO-1QFA and k QFA $(k \geq 2)$ intended for transformation of pure initial state of an automaton, and their generalizations L-QFA and L-k QFA $(k \geq 2)$, intended for transformation of initial mixed state of an automaton (i.e. for some finite set of admissible initial states, each of which can take the place with given probability). The subjects of investigation are languages accepted by investigated models either with given probability, or with given error. The structure of these languages is characterized in terms of the factor-sets that are determined by considered assumptions on unitary operators. Criteria under which characterized languages are finite ones are established.

Key Words: finite 1-qubit quantum automata, rotations of the Bloch sphere around some coordinate axe.

Статтю представив професор Буй Д.Б.

Introduction.

There were proposed a variety of finite quantum automata (QA) models (in what follows the word "finite" is omitted) intended to recognize languages in the given input alphabet [1-6]. Main efforts of researchers in QA theory are directed to determine the class of languages accepted by this or the other model of QA, to compare recognizing capacities of different models of QA each with the others, as well as with classic deterministic or probability automata, or to establish criteria of states equivalency for QA.

In [7] some QA models were characterized under assumption that unitary operators commute each with the others. Languages accepted by these models of QA either with given probability, or with given mistake were characterized in terms of the input factor-set determined via the above pointed property of unitary operators.

In the given paper we investigate some simple QA models, such that unitary operators are rotations of the Bloch sphere [8] around fixed coordinate axe, i.e. they commute each with the others.

It what follows it is supposed that for any number $\alpha \in \mathbf{R}_+$ unitary operator U_α is defined via identity

$$U_\alpha = \begin{pmatrix} \cos\ 0.5\,\alpha & -\sin\ 0.5\alpha \\ \sin\ 0.5\alpha & \cos\ 0.5\,\alpha \end{pmatrix}, \qquad (1)$$

i.e. unitary operator U_α $(\alpha \in \mathbf{R}_+)$ maps any unit vector $|\varphi> \in \mathbf{C}^2$ to the unit vector $U_\alpha(|\varphi>)$ represented by the point obtained by rotating of the radius vector from the center of the Bloch sphere to the point $|\varphi>$ through the angle $0{,}5\alpha$ around the y-axe.

It is worth to note that for any numbers $\alpha_1, \alpha_2 \in \mathbf{R}_+$ there hold identities

$$U_{\alpha_1} U_{\alpha_2} = U_{\alpha_2} U_{\alpha_1} = U_{\alpha_1+\alpha_2} = U_{(\alpha_1+\alpha_2)(\mathrm{mod}\ 4\pi)}.$$

In the given paper some models of QA are investigated under the following three assumptions:

1. The set of basic states is $Q = \mathsf{B}_2 = \{|0>, |1>\}$ (where $|0> = (1,0)^T$ and $|1> = (0,1)^T$), and the set of accepting states Q_{acc} is some one-element subset of the set Q, i.e. either $Q_{acc} = \{|0>\}$, or $Q_{acc} = \{|1>\}$.

2. Measurement of a state of QA is produced at final instant only.

3. For considered finite alphabet A some injection $\nu : A \to (0;4\pi)$ is fixed, and with each letter $a \in A$ it is associated unitary operator $U_{\nu(a)}$ defined by formula (1).

The rest of the paper is organized as follows. Chapter 1 consists of technical results. In chapter 2 investigated models of QA are defined. In chapter 3 languages accepted by investigated models of QA either with given probability, or with given mistake are characterized. The last chapter consists of some conclusion remarks.

1. Technical results.

Let A be any finite alphabet, $k \in \mathbf{N}$ be some fixed integer, and $P : A \to \{0,1\}$ be some fixed predicate. We set

$$A_0 = \{a \in A \mid P(a) = 0\},$$
$$A_1 = \{a \in A \mid P(a) = 1\},$$
$$\mathsf{A}^{(k)} = \bigcup_{i=1}^{k-1} A_1^i A_0^{k-i} \cup A_1^k$$

and

$$\mathsf{S}_{A,P,k} = \{a_1 \dots a_l \in A^+ \mid l \in \mathbf{N}\ \&\ l \ge k\ \&$$
$$\&\ (\forall i = 1, \dots, l-k+1)(a_i \in A_1)\ \&$$
$$\&\ (\forall i = l-k+2, \dots, l)(a_i \in A_0\}. \qquad (2)$$

It is worth to note that there hold the following two statements:

1. For any integer $k \in \mathbf{N}$ it holds inclusion $A_1 A_0^{k-1} \subset \mathsf{S}_{A,P,k}$ (if $k = 1$ we get that $\mathsf{A}^{(1)} = A_1$ and $\mathsf{S}_{A,P,1} = A_1^+$, and thus inclusion $A_1 \subset \mathsf{S}_{A,P,k}$ holds).

2. For any integer $k \ge 2$ there hold identities $\bigcup_{i=2}^{k-1} A_1^i A_0^{k-i} \cap \mathsf{S}_{A,P,k} = \varnothing$ and $A_1^k \cap \mathsf{S}_{A,P,k} = \varnothing$.

Let $\nu : \mathsf{A}^{(k)} \to (0;4\pi)$ be some fixed injection. For any string $a_1 \dots a_l \in \mathsf{S}_{A,P,k}$ we set

$$\tilde{\nu}(a_1 \dots a_l) = \sum_{i=1}^{l-k+1} \nu(a_i \dots a_{i+k-1}). \qquad (3)$$

Equivalence $\varepsilon_{A,P,k}$ on the set $\mathsf{S}_{A,P,k}$ defined by formula

$$(w_1, w_2) \in \varepsilon_{A,P,k} \Leftrightarrow$$
$$\Leftrightarrow \tilde{\nu}(w_1) \equiv \tilde{\nu}(w_2)\ (\mathrm{mod}\ \ 4\pi)\quad (w_1, w_2 \in \mathsf{S}_{A,P,k}) \qquad (4)$$

determines the factor-set $\mathsf{S}_{A,P,k} / \varepsilon_{A,P,k}$, such that for each element $B \in \mathsf{S}_{A,P,k} / \varepsilon_{A,P,k}$ there exists unique number $\gamma_B \in [0;4\pi)$ such that

$$B = \{w \in \mathsf{S}_{A,P,k} \mid (\exists k \in \mathbf{Z}_+)(\tilde{\nu}(w) = \gamma_B + 4\pi k)\}. \qquad (5)$$

Let $U_{\mathsf{A}^{(k)}} = \{U_{\nu(\mathsf{a})} \mid \mathsf{a} \in \mathsf{A}^{(k)}\}$ be the set of unitary operators, where $U_{\nu(\mathsf{a})}$ $(\mathsf{a} \in \mathsf{A}^{(k)}\}$ is defined by formula (1). For any string $a_1 \dots a_l \in \mathsf{S}_{A,P,k}$ we set

$$U_{\tilde{\nu}(a_1 \dots a_l)} = \prod_{i=1}^{l-k+1} U_{\nu(a_i \dots a_{i+k-1})}. \qquad (6)$$

Thus, the set of unitary operators $U_{\mathsf{A}^{(k)}}$ generates the set of unitary operators

$$\tilde{U}_{\mathsf{A}^{(k)}} = \{U_{\tilde{\nu}(a_1 \dots a_l)} \mid a_1 \dots a_l \in \mathsf{S}_{A,P,k}\}.$$

Since for any string $a_1 \dots a_l \in \mathsf{S}_{A,P,k}$ it holds identity

$$U_{\tilde{\nu}(a_1 \dots a_l)} = U_{\tilde{\nu}(a_1 \dots a_l)(\mathrm{mod}\ 4\pi)}, \qquad (7)$$

we get that

$$\tilde{U}_{\mathsf{A}^{(k)}} = \{U_{\tilde{\nu}(a_1 \dots a_l)(\mathrm{mod}\ 4\pi)} \mid a_1 \dots a_l \in \mathsf{S}_{A,P,k}\}, \qquad (8)$$

and formulae (4), (5) and (8) imply that

$$\tilde{U}_{\mathsf{A}^{(k)}} = \{U_{\gamma_B} \mid B \in \mathsf{S}_{A,P,k} / \varepsilon_{A,P,k}\}. \qquad (9)$$

Now we consider in detail the case, when $k = 1$.

We get that $\mathsf{A}^{(1)} = A_1$, $\mathsf{S}_{A,P,1} = A_1^+$ and

$$U_{\mathsf{A}^{(1)}} \subseteq \tilde{U}_{\mathsf{A}^{(1)}}. \qquad (10)$$

Formulae (3) and (6) imply that for any string $a_1 \dots a_l \in \mathsf{S}_{A,P,1}$ there hold identities

$$\tilde{\nu}(a_1 \dots a_l) = \sum_{i=1}^{l} \nu(a_i) \qquad (11)$$

and

$$U_{\tilde{\nu}(a_1 \dots a_l)} = \prod_{i=1}^{l} U_{\nu(a_i)}. \qquad (12)$$

Since $\mathsf{S}_{A,P,1} = A_1^+$, then $w_1 w_2 \in \mathsf{S}_{A,P,1}$ for any strings $w_1, w_2 \in \mathsf{S}_{A,P,1}$, and formulae (11) and (12) imply that

$$U_{\tilde{\nu}(w_1 w_2)} = U_{\nu(w_1)} \cdot U_{\tilde{\nu}(w_2)} = U_{\tilde{\nu}(w_2)} \cdot U_{\tilde{\nu}(w_1)}. \qquad (13)$$

Thus, $(\tilde{U}_{A^{(1)}},\cdot)$ is commutative semigroup and formulae (7), (11) and (12) imply that the following theorem holds.

Theorem 1. For any finite alphabet A and any predicate $P: A \to \{0,1\}$ the semigroup $(\tilde{U}_{A^{(1)}},\cdot)$ is isomorphic to the semigroup $(G,\oplus)$, where

$$G = \{(\sum_{a\in A_1} m_a \nu(a)) \pmod{4\pi} \mid (\forall a \in A_1)(m_a \in \mathbf{Z}_+) \,\&\, (\exists a \in A^{(1)})(m_a \neq 0)\} \quad (14)$$

and

$$g_1 \oplus g_2 = (g_1 + g_2) \pmod{4\pi} \quad (g_1, g_2 \in G). \quad (15)$$

Corollary 1. For any finite alphabet A and any predicate $P: A \to \{0,1\}$ the semigroup $(\tilde{U}_{A^{(1)}},\cdot)$ is a finite group if and only if all numbers $\frac{\nu(a)}{\pi}$ $(a \in A^{(1)})$ are rational ones.

Proof. Since $A^{(1)} = A_1$, then we get that $0 < \nu(a) < 4\pi$ $(a \in A_1)$, and

$$0 < \frac{\nu(a)}{\pi} < 4 \quad (a \in A_1).$$

It is evident that formula (14) can be reduced to formula

$$G = \{(\sum_{a\in A_1} m_a \frac{\nu(a)}{\pi}) \pmod{4} \mid (\forall a \in A_1(m_a \in \mathbf{Z}_+) \,\&\, (\exists a \in A^{(1)})(m_a \neq 0)\} \quad (16)$$

Let all numbers $\frac{\nu(a)}{\pi}$ $(a \in A_1)$ be rational ones.

Then we get that $\frac{\nu(a)}{\pi} = \frac{k_a^{(1)}}{k_a^{(2)}}$ $(a \in A_1)$, where $k_a^{(1)}, k_a^{(2)} \in \mathbf{N}$, $k_a^{(1)} < 4k_a^{(2)}$ and $\mathrm{GCD}\{k_a^{(1)}, k_a^{(2)}\} = 1$.

Thus, formula (16) implies that

$$G = \{(\sum_{a\in A_1} m_a \frac{k_a^{(1)}}{k_a^{(2)}}) \pmod{4} \mid (\forall a \in A_1)(m_a \in \mathbf{Z}_+) \,\&\, (\forall a \in A_1)(m_a \le 4k_a^{(2)}) \,\&\, (\exists a \in A_1)(m_a \neq 0)\}. \quad (17)$$

Formula (17) in its turn implies that the following three conditions hold:

1. The set G is a finite one.

2. $0 \in G$ (since we get that it holds identity $(\sum_{a\in A_1} 4k_a^{(2)} \frac{k_a^{(1)}}{k_a^{(2)}}) \pmod{4} = 0$).

3. For any element $b = (\sum_{a\in A_1} m_a \frac{k_a^{(1)}}{k_a^{(2)}}) \pmod{4} \in G$ there exists the inverse element $-b \in G$. This element is defined by identity

$$-b = (\sum_{a\in A_1} (4k_a^{(2)} - m_a) \frac{k_a^{(1)}}{k_a^{(2)}}) \pmod{4}).$$

Thus, the semigroup $(G,\oplus)$ is a finite group.

Let there exists some $a \in A_1$, such that $\frac{\nu(a)}{\pi}$ is an irrational number.

Let us consider the sequence

$$\{(m\nu(a)) \pmod{4\pi}\}_{m\in\mathbf{N}} \quad (18)$$

of elements of the set G.

Let us suppose that the sequence (18) is finite one. Then there exist integers $m_1, m_2 \in \mathbf{N}$ $(m_1 > m_2)$, such that

$$m_1\nu(a) \pmod{4\pi} = m_2\nu(a) \pmod{4\pi} \Leftrightarrow$$
$$\Leftrightarrow ((m_1 - m_2)\nu(a)) \pmod{4\pi} = 0 \Leftrightarrow$$
$$\Leftrightarrow (\exists k \in \mathbf{N})((m_1 - m_2)\nu(a) = 4\pi k) \Leftrightarrow$$
$$\Leftrightarrow (\exists k \in \mathbf{N})(\frac{\nu(a)}{\pi} = \frac{4k}{m_1 - m_2}),$$

i.e. $\frac{\nu(a)}{\pi}$ is rational number. We get a contradiction.

Thus, the sequence (18) of elements of the set G is infinite. This factor implies that the semigroup $(G,\oplus)$ is infinite.

Q.E.D.

Now we consider factor-set $S_{A,P,1}/\varepsilon_{A,P,1}$.

Let $B_1, B_2 \in S_{A,P,1}/\varepsilon_{A,P,1}$. Then for any strings $w_1 \in B_1$ and $w_2 \in B_2$ we get

$$\tilde{\nu}(w_1w_2) \pmod{4\pi} = (\tilde{\nu}(w_1) + \tilde{\nu}(w_2)) \pmod{4\pi} =$$
$$= (\tilde{\nu}(w_1) \pmod{4\pi} + \tilde{\nu}(w_2) \pmod{4\pi}) \pmod{4\pi} =$$
$$= (\gamma_{B_1} + \gamma_{B_2}) \pmod{4\pi}. \quad (19)$$

Since $w_1w_2 \in S_{A,P,1}$, then formula (19) implies that for any elements $B_1, B_2 \in S_{A,P,1}/\varepsilon_{A,P,1}$ there exists single element $B \in S_{A,P,1}/\varepsilon_{A,P,1}$ such that inclusions $B_1B_2 \subseteq B$ and $B_2B_1 \subseteq B$ hold.

This factor implies that we get some commutative semigroup $(S_{A,P,1}/\varepsilon_{A,P,1},\circ)$, where operation $\circ$ is defined as follows

$$(\forall B_1, B_2, B \in S_{A,P,1}/\varepsilon_{,P,1})(B_1 \circ B_2 = B \Leftrightarrow$$
$$\Leftrightarrow B_1B_2 \subseteq B).$$

Formula (19) implies that for any elements $B_1, B_2 \in S_{A,P,1}/\varepsilon_{A,P,1}$ it holds identity

$$\gamma_{B_1\circ B_2} = (\gamma_{B_1} + \gamma_{B_2}) \pmod{4\pi}, \quad (20)$$

i.e. for any elements $B_1, B_2 \in S_{A,P,1}/\varepsilon_{A,P,1}$

$$U_{\gamma_{B_1\circ B_2}} = U_{(\gamma_{B_1}+\gamma_{B_2}) \pmod{4\pi}}. \quad (21)$$

Theorem 2. For any finite alphabet A and any predicate $P : A \to \{0,1\}$ the semigroups $(\tilde{U}_{\mathrm{A}^{(1)}}, \cdot)$ and $(\mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}, \circ)$ are isomorphic.

Proof. Formula (7)-(9) imply that we can define some mapping

$$f : \mathrm{S}_{A,P,1} / \varepsilon_{A,P,1} \to \tilde{U}_{\mathrm{A}^{(1)}}$$

by identity

$$f(B) = U_{\gamma_B} \quad (B \in \mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}) . \qquad (22)$$

Formula (5) implies that for any elements $B_1, B_2 \in \mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}$ such that $B_1 \neq B_2$ we get

$$f(B_1) = U_{\gamma_{B_1}} \neq U_{\gamma_{B_2}} = f(B_2) ,$$

i.e. the mapping f is some injection. Formula (9) implies that the mapping f is some surjection. Thus, the mapping f is some bijection.

Formula (21) and (22) imply that for any elements $B_1, B_2 \in \mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}$ we get

$$f(B_1 \circ B_2) = U_{\gamma_{B_1 \circ B_2}} = U_{(\gamma_{B_1} + \gamma_{B_2}) (\mathrm{mod}\ 4\pi)} =$$

$$= U_{\gamma_{B_1} + \gamma_{B_2}} = U_{\gamma_{B_1}} U_{\gamma_{B_2}} = f(B_1) f(B_2) .$$

We get that the mapping f is some bijection, such that identity $f(B_1 \circ B_2) = f(B_1) f(B_2)$ holds for any elements $B_1, B_2 \in \mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}$. This factor implies that the mapping f determines some isomorphism of the semigroup $(\mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}, \circ)$ on the semigroup $(\tilde{U}_{\mathrm{A}^{(1)}}, \cdot)$. Thus, $(\mathrm{S}_{A,P,1} / \varepsilon_{A,P,1}, \circ)$ and $(\tilde{U}_{\mathrm{A}^{(1)}}, \cdot)$ are isomorphic semigroups.

Q.E.D.

2. Investigated models of QA.

We would deal with the following models of QA.

MO-1QFA is any 1-way 1-head quantum Turing machine (QTM) $\mathrm{M} = (Q, X, |\varphi_0>, |h>, \nu)$, such that $Q = \mathrm{B}_2$ is the set of basic states, X is finite input alphabet, some unit vector $|\varphi_0> \in \mathbf{C}^2$ is pure initial state, some vector $|h> \in \mathrm{B}_2$ is accepting state, and $\nu : X \to (0; 4\pi)$ is some injection. It is supposed that $U = \{U_{\nu(x)} \mid x \in X\}$ is the set of unitary operators, such that $U_{\nu(x)}$ $(x \in X)$ is defined by formula (1).

Let a string $w \in X^+$ be written in the input tape of MO-1QFA M. At initial instant QTM M exists in the state $|\varphi_0>$ and its head observes the first symbol of the string w.

If QTM M exists in the state $|\varphi>$ and observed symbol is $x \in X$ then the state $|\varphi>$ is transformed in the state $U_{\nu(x)}(|\varphi>)$ and the head moves by one cell to the right. If QTM M exists in the state $|\varphi>$ and observed symbol is Λ then the state $|\varphi>$ is measured in the basis B_2 and M halts.

If in the result of this measurement we get accepting state $|h>$ then a string w is accepted, otherwise it is rejected.

For any input string $w = x_1 \dots x_l \in X^+$ we set

$$\tilde{\nu}(w) = \sum_{i=1}^{l} \nu(x_i) .$$

Formulae (1) implies that for any input string $w = x_1 \dots x_l \in X^+$ holds identity

$$U_{\tilde{\nu}(w)} = U_{\nu(x_l)} \cdot \dots \cdot U_{\nu(x_1)} \qquad (23)$$

Thus, probability that MO-1QFA M accepts a string $w = x_1 \dots x_l \in X^+$ equals to

$$\mathrm{P}_{\mathrm{M}}(|\varphi_0>, w) = \| P_{acc} U_{\tilde{\nu}(w)} |\varphi_0> \|^2 , \qquad (24)$$

where $P_{acc} = |h><h|$ $(<h| = |h>^{\dagger}$ and $\dagger$ is the Hermitian conjugation), and $\| |\varphi> \| = \sqrt{<\varphi| \cdot |\varphi>}$.

L-QFA differs from MO-1QFA so much that it deals with some initial mixed state $\{(|\varphi_i>, \alpha_i)\}_{i \in \mathbf{N}_n}$, such that $|\varphi_i> \in \mathbf{C}^2$ $(i \in \mathbf{N}_n)$ are pair-wise different unit vectors, $\alpha_i > 0$ $(i \in \mathbf{N}_n)$, and $\sum_{i \in \mathbf{N}_n} \alpha_i = 1$. The number α_i $(i \in \mathbf{N}_n)$ is referred as probability that at initial instant QTM M exists in the state $|\varphi_i>$.

Measurement of the state in the basis B_2 is when the head observes the symbol Λ.

If in the result of this measurement we get accepting state $|h>$ then a string $w \in X^+$ is accepted, otherwise it is rejected.

Thus, probability that L-QFA M accepts a string $w \in X^+$ equals to

$$\mathrm{P}_{\mathrm{M}}(\{(|\varphi_i>, \alpha_i)\}_{i \in \mathbf{N}_n}, w) = \sum_{i \in \mathbf{N}_n} \alpha_i \mathrm{P}_{\mathrm{M}}(|\varphi_i>, w) . \qquad (25)$$

k QFA $(k \in \mathbf{N})$ is any 1-way k-head QTM $\mathrm{M} = (Q, X, |\varphi_0>, |h>, \nu)$, such that $Q = \mathrm{B}_2$ is the set of basic states, X is finite input alphabet, some unit vector $|\varphi_0> \in \mathbf{C}^2$ is pure initial state, some vector $|h> \in \mathrm{B}_2$ is accepting state, $\nu : \mathrm{X} \to (0; 4\pi)$ is some injection, where

$$\mathrm{X} = \bigcup_{i=1}^{k-1} X^i \Lambda^{k-i} \cup X^k ,$$

and Λ^j $(j \in \mathbf{N})$ is the string $\underbrace{\Lambda \dots \Lambda}_{j \text{ times}}$.

It is supposed that $U = \{U_{\nu(\mathrm{u})} \mid \mathrm{u} \in \mathrm{X}\}$ is the set of unitary operators, such that $U_{\nu(\mathrm{u})}$ $(\mathrm{u} \in \mathrm{X})$ is defined by formula (1).

Let a string $w \in X^+$ be written in the input tape of k QFA $(k \in \mathbf{N})$ M. At initial instant QTM M exists in the state $|\varphi_0>$ and its k heads observe first k symbols of the string $w\Lambda^{k-1}$.

If QTM M exists in the state $|\varphi>$ and observed fragment is $\mathrm{u} \in \mathrm{X}$ then the state $|\varphi>$ is transformed in the state $U_{\nu(\mathrm{u})}(|\varphi>)$ and all heads move simultaneously by one cell to the right. If QTM M exists in the state $|\varphi>$ and observed fragment is Λ^k then the state $|\varphi>$ is measured in the basis B_2 and M halts.

If in the result of this measurement we get accepting state $|h>$ then a string w is accepted, otherwise it is rejected.

For any input string $w = x_1 \dots x_l \in X^+$ we set

$$\tilde{\nu}(w\Lambda^{k-1}) = \begin{cases} \sum\limits_{i=1}^{l} \nu(x_i \dots x_l \Lambda^{k-l+i-1}), & \text{if } 1 \le l < k \\ \nu(x_i \dots x_l) + \sum\limits_{i=2}^{l} \nu(x_i \dots x_l \Lambda^{k-l+i-1}), & \text{if } l = k \\ \sum\limits_{i=1}^{l-k+1} \nu(x_i \dots x_{i+k-1}) + \sum\limits_{i=l-k+2}^{l} \nu(x_i \dots x_l \Lambda^{k-l+i-1}), & \text{if } l > k \end{cases}.$$

Formulae (1) implies that for any input string $w = x_1 \dots x_l \in X^+$ holds identity

$$U_{\tilde{\nu}(w\Lambda^{k-1})} = \begin{cases} \prod\limits_{i=1}^{l} U_{\nu(x_i \dots x_l \Lambda^{k-l+i-1})}, & \text{if } 1 \le l < k \\ U_{\nu(x_i \dots x_l)} \cdot \prod\limits_{i=2}^{l} U_{\nu(x_i \dots x_l \Lambda^{k-l+i-1})}, & \text{if } l = k \\ \prod\limits_{i=1}^{l-k+1} U_{\nu(x_i \dots x_{i+k-1})} \cdot \prod\limits_{i=l-k+2}^{l} U_{\nu(x_i \dots x_l \Lambda^{k-l+i-1})}, & \text{if } l > k \end{cases} \quad (26)$$

Thus, probability that k QFA $(k \in \mathbf{N})$ M accepts a string $w \in X^+$ equals to

$$\mathrm{P}_{\mathrm{M}}(|\varphi_0>, w) = \| P_{acc} U_{\tilde{\nu}(w\Lambda^{k-1})} |\varphi_0> \|^2. \quad (27)$$

It is evident that if $k = 1$ then the model k QFA is just the model MO-1QFA. Thus in what follows the model k QFA $(k \in \mathbf{N})$ would be considered under supposition that $k \ge 2$.

Similarly to the case when the model L-QFA was defined as some generalization of the model MO-1QFA we can define the model L-k QFA $(k \ge 2)$ in the following way. L-k QFA $(k \ge 2)$ differs from k QFA so much that it deals with some initial mixed state $\{(|\varphi_i>, \alpha_i)\}_{i \in \mathbf{N}_n}$, such that $|\varphi_i> \in \mathbf{C}^2$ $(i \in \mathbf{N}_n)$ are pair-wise different unit vectors, $\alpha_i > 0$ $(i \in \mathbf{N}_n)$, and $\sum\limits_{i \in \mathbf{N}_n} \alpha_i = 1$. Thus, probability that L-k QFA $(k \ge 2)$ M accepts a string $w \in X^+$ is defined by formula (25) under supposition that $\mathrm{P}_{\mathrm{M}}(|\varphi_0>, w)$ is defined by formula (27).

Any model of QA can be interpreted either as acceptor of a language with given probability, or as acceptor of a language with given mistake. Formally, the language $L \subseteq X^+$ is accepted:

1) with probability p $(0.5 < p \le 1)$, if any string $w \in L$ is accepted with probability not less then p, while any string $w \notin L$ is accepted with probability not exceeding $1 - p$;

2) with mistake $(p_1; p_2)$ $(0 \le p_1 < p_2 < 1)$, if any string $w \in L$ is accepted with probability not less then p_2, while any string $w \notin L$ is accepted with probability not exceeding p_1.

Formula (2) implies that for any integer $k \ge 2$ only some partial semigroup can be determined by the factor-set $\mathrm{S}_{A,P,k} / \varepsilon_{A,P,k}$ as well as by the set of unitary operators $\tilde{U}_{\mathrm{A}(k)}$. Moreover, formula (6) implies that these partial semigroups are not isomorphic. Besides, partial semigroup determined by the factor-set $\tilde{U}_{\mathrm{A}(k)}$ is not isomorphic to the semigroup $(G, \oplus)$.

These factors characterize essential inherent difference between models MO-1QFA and k QFA $(k \ge 2)$ from algebraic point of view.

It is worth to note that if all numbers $\frac{\nu(a)}{\pi}$ $(a \in \mathrm{X})$ are rational ones then the factor-set $\mathrm{S}_{A,P,k} / \varepsilon_{A,P,k}$ as well as the set of unitary operators $\tilde{U}_{\mathrm{A}(k)}$ are finite ones.

3. Main results.

In accordance with [9] for any set S which elements are subsets we would use denotation $\cup S$ instead of $\bigcup\limits_{s \in S} s$, where it is convenient.

Firstly, we characterize the sets of languages accepted by models MO-1QFA and L-QFA defined in Section 2.

In terms of Section 1 in this case we get that $A = X \cup \{\Lambda\}$, and the predicate $P: A \to \{0,1\}$ is defined in the following way: $P(x) = 1$ $(x \in X)$ and $P(\Lambda) = 1$.

Thus, we get that $\mathrm{A}^{(1)} = X$ and $\mathrm{S}_{A,P,1} = X^+$.

Equivalence $\varepsilon_{A,P,1}$ on the set X^+ would be denoted by $\sim_1$, and we get that

$$\tilde{U}_X = \{U_{\gamma_B} \mid B \in X^+ / \sim_1\}. \quad (28)$$

For any element $B \in X^+ \setminus \sim_1$ we set

$$\mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) = \| P_{acc} U_{\gamma_B} |\varphi_0> \|^2. \quad (29)$$

Theorem 3. MO-1QFA M accepts a language L with probability p $(0.5 < p \le 1)$ if and only if the following two identities hold

$$L = \cup\{B \in X^+ / \sim_1 | \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \ge p\}$$

and

$$X^+ \setminus L = \cup\{B \in X^+ / \sim_1 | \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \le 1 - p\}.$$

Proof. Formulae (7), (11), (12) and (23) imply that for any element $B \in \mathsf{S}_{A,P,1} / \sim_1$ and any string $w \in B$ there hold identities

$$U_{\tilde{\nu}(w)} = U_{\tilde{\nu}(w)(\mathrm{mod}\ 4\pi)} = U_{\gamma_B}. \quad (30)$$

Formulae (24), (29) and (30) in its turn imply that for any element $B \in \mathsf{S}_{A,P,1} / \sim_1$ and any string $w \in B$ it holds identity

$$\mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) = \mathsf{P}_{\mathrm{M}}(|\varphi_0>, w). \quad (31)$$

Formula (31) and definition of a language accepted with given probability by MO-1QFA imply that theorem 3 holds.

Q.E.D.

Corollary 1 and theorem 3 imply that the following corollary holds.

Corollary 2. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in X)$ are rational ones then a language accepted with any given probability by MO-1QFA M is union of some elements of finite factor-set $X^+ \setminus \sim_1$.

Theorem 4. MO-1QFA M accepts a language L with mistake $(p_1; p_2)$ $(0 \le p_1 < p_2 < 1)$ if and only if the following two identities hold

$$L = \cup\{B \in X^+ / \sim_1 | \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \ge p_2\}$$

and

$$X^+ \setminus L = \cup\{B \in X^+ / \sim_1 | \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \le p_1\}.$$

Proof. Formula (31) and definition of a language accepted with given mistake by MO-1QFA imply that theorem 4 holds.

Q.E.D.

Corollary 1 and theorem 4 imply that the following corollary holds.

Corollary 3. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in X)$ are rational ones then a language accepted with any given mistake by MO-1QFA M is union of some elements of finite factor-set $X^+ \setminus \sim_1$.

Theorem 5. L-QFA M accepts a language L with probability p $(0.5 < p \le 1)$ if and only if the following two identities hold

$$L = \cup\{B \in X^+ / \sim_1 | \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \ge p_2\}$$

and

$$X^+ \setminus L = \cup\{B \in X^+ / \sim_1 \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \le p_1\}.$$

Proof. By definition of L-QFA M formula (31) can be applied for this model.

Formulae (25), (27) and (31), and definition of a language accepted with given probability by L-QFA imply that theorem 5 holds.

Q.E.D.

Corollary 1 and theorem 5 imply that the following corollary holds.

Corollary 4. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in X)$ are rational ones then a language accepted with any given probability by L-QFA M is union of some elements of finite factor-set $X^+ \setminus \sim_1$.

Theorem 6. A language L is accepted with mistake (p_1, p_2) $(0 \le p_1 < p_2 < 1)$ by L-QFA M if and only if the following two identities hold

$$L = \cup\{B \in X^+ / \sim_1 | \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \ge p_2\}$$

and

$$X^+ \setminus L = \cup\{B \in X^+ / \sim_1 \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \le p_1\}.$$

Proof. Formulae (25) and (31), and definition of a language accepted with given mistake by L-QFA imply that theorem 6 holds.

Q.E.D.

Corollary 1 and theorem 6 imply that the following corollary holds.

Corollary 5. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in X)$ are rational ones then a language accepted with any given mistake by L-QFA M is union of some elements of finite factor-set $X^+ \setminus \sim_1$.

Now we characterize the sets of languages accepted by models k QFA $(k \ge 2)$ and L-k QFA $(k \ge 2)$ defined in Section 2.

In terms of Section 1 in this case we get that $A = X \cup \{\Lambda\}$ and the predicate $P: A \to \{0,1\}$ is defined in the following way: $P(x) = 1$ $(x \in X)$ and $P(\Lambda) = 1$.

Thus, we get that $\mathsf{A}^{(k)} = \mathrm{X}$, i.e. $\mathsf{A}^{(k)} = \bigcup_{i=1}^{k-1} X^{i} \Lambda^{k-i} \cup X^{k}$, where Λ^{j} $(j \in \mathbf{N})$ is the string $\underbrace{\Lambda \ldots \Lambda}_{j \text{ times}}$, and $\mathsf{S}_{A,P,k} = X^{+} \Lambda^{k-1}$.

Equivalence $\varepsilon_{A,P,k}$ on the set $X^{+} \Lambda^{k-1}$ would be denoted by $\sim_{k}$, and we get that

$$\tilde{U}_{\mathrm{X}} = \{U_{\gamma_B} \mid B \in X^{+} \Lambda^{k-1} / \sim_1\}. \qquad (32)$$

For any element $B \in X^{+} \Lambda^{k-1} \setminus \sim_k$ we set

$$\mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) = \| P_{acc} U_{\gamma_B} |\varphi_0> \|^2. \qquad (33)$$

Theorem 7. k QFA $(k \geq 2)$ M accepts a language L with probability p $(0.5 < p \leq 1)$ if and only if the following two identities hold

$$L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \mid \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \geq p\}$$

and

$$X^{+} \setminus L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \mid \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \leq 1 - p\}.$$

Proof. Formulae (7), (11), (12) and (23) imply that for any element $B \in X^{+} \Lambda^{k-1} / \sim_k$ and any string $w \in B$ there hold identities

$$U_{\tilde{\nu}(w)} = U_{\tilde{\nu}(w)(\mathrm{mod}\ 4\pi)} = U_{\gamma_B}. \qquad (34)$$

Formulae (24), (33) and (34) in its turn imply that for any element $B \in X^{+} \Lambda^{k-1} / \sim_k$ and any string $w \in B$ it holds identity

$$\mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) = \mathsf{P}_{\mathrm{M}}(|\varphi_0>, w). \qquad (35)$$

Formula (35) and definition of a language accepted with given probability by k QFA $(k \geq 2)$ imply that theorem 7 holds.

Q.E.D.

Theorem 7 implies that the following corollary holds.

Corollary 6. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in \mathrm{X})$ are rational ones then a language accepted with any given probability by k QFA $(k \geq 2)$ M is union of some elements of finite factor-set $X^{+} \Lambda^{k-1} \setminus \sim_k$.

Theorem 8. k QFA $(k \geq 2)$ M accepts a language L with mistake (p_1, p_2) $(0 \leq p_1 < p_2 < 1)$ if and only if the following two identities hold

$$L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \mid \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \geq p_2\}$$

and

$$X^{+} \setminus L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \mid \mathsf{P}_{\mathrm{M}}(|\varphi_0>, B) \leq p_1\}.$$

Proof. Formula (35) and definition of a language accepted with given mistake by k QFA $(k \geq 2)$ imply that theorem 7 holds.

Q.E.D.

Theorem 8 implies that the following corollary holds.

Corollary 7. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in \mathrm{X})$ are rational ones then a language accepted with any given mistake by k QFA $(k \geq 2)$ M is union of some elements of finite factor-set $X^{+} \Lambda^{k-1} \setminus \sim_k$.

Theorem 9. L-k QFA $(k \geq 2)$ M accepts a language L with probability p $(0.5 < p \leq 1)$ if and only if the following two identities hold

$$L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \mid \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \geq p\}$$

and

$$X^{+} \setminus L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \leq 1 - p\}.$$

Proof. By definition of L-k QFA $(k \geq 2)$ formula (35) can be applied for this model.

Formulae (25), (27) and (35), and definition of a language accepted by L-k QFA $(k \geq 2)$ with given probability imply that theorem 9 holds.

Q.E.D.

Theorem 9 implies that the following corollary holds.

Corollary 8. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in \mathrm{X})$ are rational ones then a language accepted with any given probability by L-k QFA $(k \geq 2)$ M is union of some elements of finite factor-set $X^{+} \Lambda^{k-1} \setminus \sim_k$.

Theorem 10. L-k QFA $(k \geq 2)$ M accepts a language L with mistake (p_1, p_2) $(0 \leq p_1 < p_2 < 1)$ if and only if the following two identities hold

$$L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \mid \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \geq p_2\}$$

and

$$X^{+} \setminus L = \cup \{B \in X^{+} \Lambda^{k-1} / \sim_k \sum_{i \in \mathbf{N}_n} \alpha_i \mathsf{P}_M(|\varphi_i>, B) \leq p_1\}.$$

Proof. Formulae (25), (27) and (35), and definition of a language accepted by L-k QFA $(k \geq 2)$ with given mistake imply that theorem 10 holds.

Q.E.D.

Theorem 10 implies that the following corollary holds.

Corollary 9. If all numbers $\frac{\nu(a)}{\pi}$ $(a \in \mathrm{X})$ are rational ones then a language accepted with any

given mistake by L-k QFA $(k \geq 2)$ M is union of some elements of finite factor-set $X^{+}\Lambda^{k-1}\setminus\sim_{k}$.

Conclusions.

In this paper the simplest models of 1-qubit QA are investigated. These models of QA are determined by assumptions that measurement of a state is produced at final instant only, and associated unitary operators are rotations of the Bloch sphere around the y-axe (and thus, associated unitary operators commute each with the others). Investigated models of 1-qubit QA are MO-1QFA, L-QFA, k QFA $(k \geq 2)$ and L-k QFA $(k \geq 2)$ (we think that the last model was not considered earlier at all, and is firstly determined in the given paper).

The structure of languages accepted either with given probability, or with given mistake is characterized for investigated 1-qubit models of QA in terms of the factor-set determined by considered assumptions on unitary operators. Criteria under which characterized languages are finite ones are established.

It is evident that we get similar results if instead of rotations of the Bloch sphere around the y-axe we consider rotations of this sphere either around the x-axe, or around the z-axe. Indeed, rotations of the Bloch sphere around the x-axe are unitary operators of the form

$$V_{\beta} = \begin{pmatrix} \cos\ 0.5\,\beta & -i\sin\ 0.5\,\beta \\ i\sin\ 0.5\,\beta & \cos\ 0.5\,\beta \end{pmatrix}, \qquad (36)$$

and rotations of the Bloch sphere around the z-axe are unitary operators of the form

$$W_{\gamma} = \begin{pmatrix} e^{-i0.5\,\gamma} & 0 \\ 0 & e^{i0.5\,\gamma} \end{pmatrix}. \qquad (37)$$

Thus, if we substitute instead of formula (1) either formula (36), or formula (37), we get the same results as the ones established in the given paper.

More complicated cases take the place if the set of associated unitary operators consists of rotations of the Bloch sphere around different coordinate axes. Investigation of these cases in detail determines some trend for future investigation.

Список використаних джерел

1. *Moore C., Crutchfield J.* Quantum automata and quantum grammars // Theor. Comput. Sci. – 2000. – Vol. 237. – P. 257-306.
2. *Bertoni A., Mereghetti C., Palano B.* Quantum computing: 1-way quantum automata // LNCS. – 2003. – Vol. 2710. – P. 1-20.
3. *Ambainis A., Beaudry M., Golovkins M., at all*. Algebraic results on quantum automata // LNCS. – 2004. – Vol. 2996. – P. 93-104.
4. *Belovs A., Rosmanis A., Smotrovs J*. Multi-letter reversible and quantum finite automata // LNCS. – 2007. – Vol. 4588. – P. 60-71.
5. *Qiu D., Li L., Zou H. at all*. Multi-letter quantum finite automata decidability of the equivalence and minimization of states // Acta Informatica. – 2011. – Vol. 48. – P. 271-290.
6. *Skobelev V.G.* Theory of finite quantum automata (a survey) // Tr. Inst. Prikl. Math. Mech. of NAS of Ukraine – 2012. – Vol. 25. – P. 196-209.
7. *Skobelev V.G.* Quantum automata with operators that commutes // Visn., Ser. Fiz.-Mat. Nayky, Kyiv Univ. im. Tarasa Shevchenka. – 2013. – N 2. – P. 234-238.
8. Williams C.P. Explorations in quantum computing. – London: Springer Verlag, 2011. – 717 p.
9. *Cohn P.M.* Universal algebra. – Moscow: Mir, 1968. – 352 p.

References

1. MOORE C., CRUTCHFIELD J. (2000) *Quantum automata and quantum grammars*. Theor. Comput. Sci. (237). p. 257-306.
2. BERTONI A., MEREGHETTI C., PALANO B. (2003) *Quantum computing: 1-way quantum automata*. LNCS. (2710). p. 1-20.
3. AMBAINIS A., BEAUDRY M., GOLOVKINS M., AT ALL. (2004) *Algebraic results on quantum automata*. LNCS. (2996). p. 93-104.
4. BELOVS A., ROSMANIS A., SMOTROVS J. (2007) *Multi-letter reversible and quantum finite automata*. LNCS. (4588). p. 60-71.
5. QIU D., LI L., ZOU H. AT ALL. (2011) *Multi-letter quantum finite automata decidability of the equivalence and minimization of states*. Acta Informatica. (48), p. 271-290.
6. SKOBELEV V.G. (2012) *Theory of finite quantum automata (a survey)* Tr. Inst. Prikl. Math. Mech. of NAS of Ukraine (25). p. 196-209..
7. SKOBELEV V.G. (2013) *Quantum automata with operators that commutes*. Bulletin of Taras Shevchenko. National University of Kyiv. Series Physics & Mathematics. (2). p. 234-238.
8. WILLIAMS, C.P. (2011) *Explorations in quantum computing*. London: Springer Verlag,.
9. COHN, P.M. (1968) *Universal algebra*. Moscow: Mir.

Надійшла до редколегії 29.01.14