On some Class of Quantum Finite Automata

Volodymyr G. Skobelev
Dept. of Theory of Digital Automata
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
Kyiv, Ukraine
skobelevvg@mail.ru

Про Один Клас Квантових Скінченних Автоматів

Володимир Г. Скобелєв
Відділ теорії цифрових автоиатів
Інститут кібернетики імені В.М. Глушкова НАН України
Київ, Україна
skobelevvg@mail.ru

***Abstract*—Classes of languages accepted either with given probability, or with given mistake by basic models of finite quantum automata are characterized under supposition that unitary operators satisfy to commutative law.**

***Анотація*—Охарактеризомано класи мов, які розпізнають з заданою ймовірністю, обо з заданою помилкою скінченні квантові автомати за умови, що унітарні оператори задовільняють закону комутатівністі.**

Keywords—quantum finite automata; unitary operators; commutativity; accepted languages.

Ключові слова—квантові скінченні автомати; унітарні оператори; комутативність; розпізнаваємі мови.

I. INTRODUCTION

Success in the development of quantum algorithms theory has stimulated intensive formation of quantum automata (QA) theory. Very extraordinary situation takes place for finite QA theory (since we deal only with finite QA the word "finite" in word combination "finite QA" is omitted). A variety of different QA models intended to recognize languages in the given alphabet (i.e. all these models are acceptors) has been proposed. This means, at least, that QA models can be used for the decision of problems, in which this or that subtask can be reduced to recognition of some language. It is worth to note that all proposed QA models differ by complexity, as well as by recognizing capacities.

Each QA model is defined in terms of quantum Turing machine (QTM) in the following way. The set of the states of QTM is the set of unit vectors in the complex n -dimensional Euclidean space, in which some orthonormal basis is fixed. Elements of this orthonormal basis are the basic states for QA. Besides, some set of accepting basic states is fixed. Initially QTM is either in some fixed initial state, or in some fixed initial mixed state, which is some finite set of ordered pairs of the type (state, its probability), such that the sum of probabilities equals to 1. There is infinite to the right input tape partitioned into cells, enumerated by positive integers.

The number of heads of QTM is equal to some fixed positive integer k . Finite input alphabet is fixed. With each input string, which length does not exceed the integer k , it is associated some unitary operator acting in the complex n - dimensional Euclidean space. Analyzed input string is written, letter by letter, in the leftmost fragment of the tape, and initially k heads of QTM observe the first k cells of the tape.

When QTM heads observe current fragment of the tape, then only a single action of the following two types of actions can be performed. The first type of actions is measurement. It transforms current state (or current mixed state) of QTM into some basic state (or some set of basic states) of QA. The probability for QTM to be transformed into this or the other basic state depends only on the current state (or current mixed state) of QTM. The second type of actions is transformation of current state (or current mixed state) of QTM by unitary operator, which corresponds to the current fragment of the input string, and simultaneous shifting all k heads one cell to the right (i.e. we deal only with 1-way QTM).

Probability of QTM to accept analyzed input string is computed at the final stage. This computing is reduced to projection of final state (or final mixed state) of QTM into the subspace spanned by the accepting basic states. It is worth to note that any projection of current state of QTM is also considered as some variant of measurement. Since we deal with probability of accepting analyzed input string, two problems of language recognition for QA models can be considered, namely, recognition with given probability and recognition with given mistake.

The main problems that have been investigated for QA are the following ones: to describe in the explicit form the class of languages recognized by this or the other QA model, to compare recognizing capacities of different QA models, and to find criteria of states equivalence for this or the other QA model.

Unfortunately, the situation with the first problem is very far from its complete decision. Because of this situation it seems reasonable to investigate QA models under supposition that there are some additional requirements, which are natural, at least, from the mathematical point of view. Obviously, that this class of requirements includes the supposition that unitary operators satisfy to commutative law. The aim of the given paper is to investigate QA models under this assumption.

II. Basic QA Models

Let X $(|X|=m)$ be fixed input alphabet, C^n be complex n-dimensional Euclidean space, Q be fixed basis in it, $Q_{ac} \subseteq Q$ be the set of accepting states, and P_{ac} be the projection operator on the subspace spanned by the accepting basic states.

The following well known approach, which has been used in the theory of probabilistic automata, can be applied for definition of languages recognized by QTM:

A language $L \subseteq X^+$ is accepted by QTM with given 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 $1-p$.

A language $L \subseteq X^+$ is accepted by QTM with given mistake (p_1, p_2) $(0 < p_1 < p_2 < 1)$, 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.

A. Models of QA Defined via 1-Head QTM

We deal with 1-head QTA, which head at each instant move one cell to the right. With each input letter $x \in X$ it is associated some unitary operator U_x, acting in the complex n-dimensional Euclidean space C^n. Thus, for each input string $w = x_1 \ldots x_l$ it is uniquely defined unitary operator $U_w = U_{x_l} \ldots U_{x_1}$.

Firstly we consider basic QA models that start in fixed initial state $\mathbf{s}_0 \in C^n$, which is some unit column vector.

The model MO-1QFA [1] is 1-head QTM, with single measurement, carried out only on the final stage. An input string $w = x_1 \ldots x_l$ is accepted by this model with probability

$$P_{\text{MO-1FQA}}(\mathbf{s}_0, w) = \| P_{acc} U_w \mathbf{s}_0 \|^2 .$$

It has been established in [2] that the class of languages accepted with given mistake by the model MO-1QFA equals to the class of languages accepted by group finite automata.

The model MM-1QFA [3] differs from the model MO-1QFA in the following way. Two non-intersecting subsets Q_{rj} and Q_{nt} $(Q_{rj} \cup Q_{nt} \subseteq Q \setminus Q_{ac})$, correspondingly, of rejecting and of non-accepting basic states are fixed.

At any intermediate instant it is applied the relevant unitary operator, possibly followed by measurement in the basis Q. If the result of measurement is some state $\mathbf{s} \in Q_{nt}$ then the next instant starts, while if the result of measurement is some state $\mathbf{s} \in Q_{ac} \cup Q_{rj}$ then QTM halts. Analyzed input string is accepted, if $\mathbf{s} \in Q_{ac}$, and rejected, if $\mathbf{s} \in Q_{rj}$.

It is worth to note that the model MM-1QFA is based on well known "Decide and Halt" approach, which is intended to solve the class of problems of recognition called "promise problems". The class of languages accepted by the model MM-1QFA is not defined in explicit form, till now. It is only known that this class of languages includes properly the class of languages accepted by group finite automata, and it is included properly in the class of regular languages. Moreover, it has been established in [4] that the class of languages accepted by the model MM-1QFA is not closed under Boolean operations.

The model N-QFA [5] at any instant admits application of any sequence of unitary operators and projective measurements. Thus, exploring of ancilla qubits can be easily presented in this model. The class of languages accepted by the model N-QFA is not defined in explicit form, till now. It is only known that this class of languages satisfies to strict inclusions pointed above for the model MM-1QFA.

The model CL-QFA [6] is some generalization of the model N-QFA. In this model some regular language in the alphabet of igenvalues of Hermitian operators is used to determine projective measurements at intermediate instants. The class of languages accepted by the model CL-QFA is not defined in explicit form, till now. It is only known that any regular language can be accepted with given mistake by the model CL-QFA.

Now we consider basic QA model, called L-QFA [7]. This model is 1-head QTM, with single measurement carried out only on the final stage, and which starts in some fixed initial mixed state. Any mixed state is some set $\{(\mathbf{s}_i, p_i) \mid i = 1,\ldots,r\}$, where unit vectors $\mathbf{s}_i$ $(i = 1,\ldots,l)$ are pair-wise different, $p_i > 0$ for each $i = 1,\ldots,l$, and $p_1 + \ldots + p_r = 1$. An input string $w = x_1 \ldots x_l$ is accepted by the model L-QFA with probability

$$P_{\text{L-FQA}}\{(\mathbf{s}_i, p_i) \mid i = 1,\ldots,r\} = \\ = p_1 P_{\text{MO-1FQA}}(\mathbf{s}_1, w) + \ldots + p_r P_{\text{MO-1FQA}}(\mathbf{s}_r, w) .$$

This mixed state $\{(\mathbf{s}_i, p_i) \mid i = 1,\ldots,r\}$ can be presented by density operator

$$\rho = p_1 \mathbf{s}_1 \mathbf{s}_1^T + \ldots + p_r \mathbf{s}_r \mathbf{s}_r^T .$$

Thus, initial state of the model L-QFA is some density operator. Each unitary operator U transforms mixed state ρ

into the mixed state $U^{\dagger}\rho U$. It is known that the class of languages accepted by the model L-QFA equals to the class of languages accepted by invertible probabilistic finite automata.

By analogy with above considered generalizations of the model MO-1QFA, similar generalizations can be constructed for the model L-QFA. However, as far as I know, such generalizations have not been investigated in detail.

B. Model of QA Defined via k-Heads QTM

We deal with k-heads QTM, which heads at each instant, move simultaneously one cell to the right. It is supposed that with each input string $u = x_1 \ldots x_r$ $(1 \le r \le k)$ it is associated some unitary operator U_u acting in the space C^n. Thus, for each input string $w = x_1 \ldots x_l$ it is uniquely defined unitary operator $U_w = U(l) \ldots U(1)$, where $U(j) = U_{x_j \ldots x_{\min\{k+j-1,l\}}}$ for all $j = 1, \ldots, l$.

The model kQFA [8] is k-heads QTM, with single measurement carried out only on the final stage. This model starts in some fixed initial state $\mathbf{s}_0 \in C^n$, which is some unit column vector. The class of languages accepted by the model kQFA is not defined in explicit form, till now. It is only known that this class of languages is closed under Boolean operations, but it is not closed under concatenation and iteration. Moreover, it has been established that for all integers $k \ge 1$ the class of languages accepted by the model kQFA is strictly included into the class of languages accepted by the model $(k+1)$QFA.

By analogy with above considered generalizations of the model MO-1QFA, similar generalizations can be constructed for the model kQFA. However, as far as I know, such generalizations have not been investigated in detail.

III. Main Results

A. Analysis of Models of QA Defined via 1-Head QTM

Let us characterize languages accepted by the models MO-1QFA and L-QFA under the supposition that unitary operators associated with input letters satisfy to commutative law. We remind that MO-1QFA and L-QFA are the models in which measurement is carried out only at a final stage.

Let $X = \{x_1, \ldots, x_m\}$ be the input alphabet of QA. Unitary operator associated with input letter $x_i \in X$ is denoted U_i. Since it is supposed that $U_i U_j = U_j U_i$ for all $i, j = 1, \ldots, m$, then to define the unitary operator for analyzed input sequence, it is sufficient to know only the number of occurrences of each letter in this input sequence, and unitary operators associated with these letters. Based on this factor we can present uniquely the unitary operator defined for any input string $w \in X^+$ in the standard form

$$sfuo(w) = U_1^{r_1} \ldots U_m^{r_m},$$

where r_i $(i = 1, \ldots, m)$ is the number of occurrences of the letter x_i in the input string w.

Let $\equiv$ be the equivalence relation on the set X^+ defined as follows:

$$w_1 \equiv w_2 \Leftrightarrow sfuo(w_1) = sfuo(w_2).$$

As a matter of fact, this equivalence relation is a congruence on the set X^+, since $w_1 \equiv w_2$ $(w_1, w_2 \in X^+)$ implies that $w_1 x \equiv w_2 x$ for all $x \in X$. We deal with the factor-set $X^+/\equiv$, as with a partition of the set X^+. It is evident that the following theorem holds.

Theorem. For each of the models, MO-1QFA and L-QFA, any language, accepted either with given probability, or with given mistake, is the union of some blocks of the partition $X^+/\equiv$.

It is of special interest the situation, when the equivalence relation $\equiv$ is finitary, i.e. when the partition $X^+/\equiv$ consists of finite number of blocks. Such situation arises, in particular, in the following important case.

Let us suppose that for each unitary operator U_i $(i = 1, \ldots, m)$ there exists some positive integer a_i, such that $U_i^{a_i} = I$, where I is the identity map acting in C^n.

Let a_i $(i = 1, \ldots, m)$ be the minimal positive integer, such that identity $U_i^{a_i} = I$ holds. The unitary operator defined for any input string $w \in X^+$ can be present uniquely in the reduced standard form

$$rsfuo(w) = U_1^{r_1 (\mathrm{mod}\, a_1)} \ldots U_m^{r_m (\mathrm{mod}\, a_m)},$$

where r_i $(i = 1, \ldots, m)$ is the number of occurrences of the letter x_i in the input string w. This factor implies that the equivalence relation $\equiv$ on the set X^+ can be defined in the following way:

$$w_1 \equiv w_2 \Leftrightarrow rsfuo(w_1) = rsfuo(w_2).$$

It is evident that the number for blocks of the partition $X^+/\equiv$ equals to the product $a_1 \cdot \ldots \cdot a_m$.

The following example justifies non-triviality of proposed constructions.

Example. Let us consider 1-qubit MO-1QFA. In this case any special unitary operator can be presented as some composition of rotations about the x-, y-, and z-axes of the Bloch sphere (see [9], for example). The word “special” means that the determinant of a matrix that defines unitary operator equals to 1. It is well known that to investigate QA, it is sufficient to deal only with special unitary operators.

Let us suppose that unitary operator associated with each input letter x_i $(i = 1, \ldots, m)$ is the rotation through the angle

$0.5\alpha_i$ $(\alpha_i \in (0, 4\pi))$ around the y-axe of the Bloch sphere. It is evident that these unitary operators satisfy to commutative law. Thus, any language recognized by considered model of QA, either with given probability, or with given error, is the union of some blocks of the partition $X^+/\equiv$. This partition is finitary if and only if each number $\alpha_i\pi^{-1}$ $(i = 1,\ldots,m)$ is some rational one. End of Example.

Let us characterize models of QA with measurements at intermediate instants (the models MM-1QFA, N-QFA, and CL-QFA), under supposition that unitary operators associated with input letters satisfy to commutative law.

In this case, when any of the models MM-1QFA, N-QFA, and CL-QFA is processing any given input string $w \in X^+$ of the length $l \geq 2$, different variants for computing, provided by QTM, are possible.

Each variant for computing, provided by QTM, can be determined in the following way. The number r $(0 \leq r < l)$ of measurements at intermediate instants is selected with given probability. Instants for intermediate measurements are fixed by inserting r symbols $|$ on a segment of the analyzed input string w between the first and last letters with given probability.Each maximal fragment of the analyzed input string, which does not contain the symbol $|$, is replaced with the standard form of the unitary operator defined for this fragment. Each symbol $|$ is replaced with measurement admissible on this intermediate step, with given probability, and measurement only on the final stage is also inserted.

It is evident, that if the partition $X^+/\equiv$ is finitary, then each maximal fragment of the analyzed input string, which does not contain the symbol $|$, can be replaced with the reduced standard form of the unitary operator defined for this fragment. Thus, for any of the models MM-1QFA, N-QFA, and CL-QFA, the set of all different variants for computing, provided by QTM, when processing any given input string $w \in X^+$ of the length $l \geq 2$, can be presented by some labeled rooted oriented tree.

B. Analysis of Models of QA Defined via k-Heads QTM

We consider two different cases.

The first case takes the place when either $k = 1$, or $k \geq 2$ and all unitary operators associated with input string of the length not exceeding the integer k satisfy to commutative law. In this case we get the situation similar to the one that has been analyzed previously for the model MO-1QFA. It means that the theorem holds in this case.

The second case takes the place when $k \geq 2$ and only unitary operators associated with input string of the length k satisfy to commutative law. In this situation the standard form of the unitary operator defined for any input string $w = x_1 \ldots x_l$ can be defined in the following way.

If $l \leq k$, then

$$sfuo(w) = U(l)\ldots U(1),$$

where $U(j) = U_{x_j \ldots x_{\min\{k+j-1,l\}}}$ for all $j = 1,\ldots,l$.

If $l > k$, then

$$sfuo(w) = U'U'',$$

where the unitary operator U' is the standard form for the product $U(l)\ldots U(l-k+1)$ constructed by the rules, similar to the ones that has been defined for the model MO-1QFA, and $U'' = U(l-k)\ldots U(1)$.

Since there is only finite number of input strings of the length less than k, the presence of the unitary operator U'' have no influence on the property "to be finitary" for the partition $X^+/\equiv$ of the set X^+.

IV. CONCLUSIONS

In the given paper basic models of finite quantum automata have been considered under the supposition that unitary operators satisfy to commutative law. The classes of languages accepted by these models either with given probability, or with given mistake have been characterized in terms of constructed partition of the set of all input strings.

Detailed analysis of these classes of languages is tightly connected with investigation the structure of the set of all finitely generated commutative semigroups of special unitary operators, acting in the complex n-dimensional Euclidean space. This is the subject for future research.

It is worth to note that this problem is sufficiently hard even in the case when $n = 2$, i.e. for 1-qubit finite quantum automata.

REFERENCES

[1] G. Moore, and J. Crutchfield, "Quantum automata and quantum grammars," in Theor. Comput. Sci., vol. 237, pp. 257-306, 2000.

[2] A. Brodsky, and N. Pipenger, "Characterizations of 1-way quantum finite automata" in Journal of Computing, No. 5, pp. 1456-1478, 2002.

[3] A. Kondacs, and J. Watrous, "On the power of quantum finite state automata", in Proceedings of the 38th IEEE Symposium on Foundations of Computer Science, pp. 66-75, 1997.

[4] A. Ambainis, A. Kikusts, and M. Valdats, "On some class of languages recognizable by 1-way quantum automata", in LNCS, vol. 2010, pp. 75-86, 2001.

[5] A. Nayak, "Optimal lower bounds for quantum automata and random access codes", in Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science, pp. 369-377, 1999.

[6] A. Bertoni., C. Mereghetti, and B. Palano, "Quantum computing: 1-way quantum automata", in LNCS, vol. 2710, pp. 1-20, 2003.

[7] A. Ambainis, M. Beaudry, M. Golovkins, A. Kikusts, M. Mercer, and D. Therian, "Algebraic results on quantum automata", in LNCS, vol. 2996, pp. 93-104, 2004.

[8] A. Belovs, A. Rosmanis, and J. Smotrovs, "Multi-letter reversible and quantum finite automata", in LNCS, vol. 4458, pp. 60-71, 2007.

[9] C.P. Williams. Explorations in Quantum Computing. Second Edition. Springer-Verlag London Limited, 2011.