QUANTUM FINITE AUTOMATA*

Andris Ambainis[1]

[1]Faculty of Computing, University of Latvia,
Raiņa bulv. 19, Rīga, LV-1586, Latvia.
Email: ambainis@lu.lv

Abstract
Quantum finite automata (QFAs) are quantum counterparts of the usual finite automata. 1-way QFAs recognize the same languages as conventional finite automata but can be exponentially more space-efficient.

In this talk, we describe the main results about quantum finite automata and some possible areas for future work. In particular, we will discuss:

- *the languages for which QFAs can be smaller than conventional finite automata;*
- *the models of QFAs that are between 1-way and 2-way QFAs;*
- *the connections between QFAs and quantum Markov chains.*

1. Introduction

Quantum computing combines quantum mechanics with computer science, by defining quantum mechanical counterparts of the usual models of computation (e.g., Boolean circuits, Turing machines or finite automata). The resulting models are typically more powerful than their conventional (or *classical*) counterparts, because quantum mechanics allows to implement a broader range of operations. For example, factoring is thought to be hard for conventional algorithms but quantum algorithms can factor large numbers in polynomial time [19]. Also, quantum algorithms can be exponentially faster than any classical algorithm for oracle problems [20].

Combining quantum mechanics with finite automata gives quantum finite automata (QFAs), first introduced by Moore and Crutchfield [16] and Kondacs and Watrous [13]. Both 1-way and 2-way quantum automata have been studied. For 1-way QFAs, all languages recognized by them are regular (and, if a sufficiently general model of QFAs is considered, all regular languages can be recognized by QFAs [18, 7, 15]) but QFAs can have exponentially less states

*The author was supported by ESF project 1DP/1.1.1.2.0/09/APIA/VIAA/044, FP7 Marie Curie Grant PIRG02-GA-2007-224886 and FP7 FET-Open project QCS.

than classical automata recognizing the same language. 2-way QFAs can recognize non-regular languages.

In this talk, we survey 3 research directions about QFAs:

1. Space efficiency of QFAs.

   QFAs can be exponentially smaller than any classical automaton recognizing the same language. This was first shown by Ambainis and Freivalds [2] who discovered that:

   - The language
     $$L_n = \{a^i | i \text{ is divisible by } n\}$$
     can be recognized by a QFA with $O(\log n)$ states.
   - If n is a prime then any probabilistic 1-way finite automaton for L_n has at least n states.

   The construction of QFAs recognizing L_n was subsequently simplified by [3].

   More generally, QFAs have advantage over classical automata for any periodic language in one letter alphabet. Let L be a language with a period n (i.e. $a^i \in L$ if and only if $a^{i+n} \in L$). Then, L can be recognized by a QFA with $O(\sqrt{n})$ states [14]. If l_1-norm of the Fourier transform of the characteristic function of L is small, a QFA with a smaller number of states can be constructed [6]. $O(\log n)$ state QFA for L_n of [2, 3] becomes a particular case of this construction.

   These results provide a very good understanding of the complexity of QFAs for languages in one letter alphabet. It would be interesting to come up with more examples of languages in larger alphabets where QFAs have advantage over classical automata.

   For promise problems (where the automaton has to accept words in L, reject words in L' and can behave arbitrarily on words not in $L \cup L'$), the gap between the number of states in QFAs and probabilistic automata can be unbounded. There exists a sequence of promise problems P_n such that P_n can be solved by a 2-state QFA but requires at least n states for classical automata [21].

   For language recognition, QFAs can always be simulated by DFAs with an exponential (or slightly more than exponential) increase in the number of states. The exact increase depends on whether a QFA operates on *pure* quantum states or *mixed* quantum states. A pure-state QFA with m states can be simulated by a c^m state DFA [2]. Thus, the gap between QFAs and classical automata that is achieved for L_n is optimal.

   A mixed-state QFA with m states can be simulated by a c^{m^2} state DFA [5]. It is open whether there exists a language for which such gap between the QFAs and DFAs can be achieved.

2. Between 1-way QFAs and 2-way QFAs.

   2-way QFAs have been studied since Kondacs and Watrous [13] who showed that the non-regular language $L = \{a^m b^m\}$ can be recognized by a 2-way QFA in linear time. In

contrast, 2-way DFAs cannot recognize L (because L is non-regular) and 2-way probabilistic finite automata can recognize L only in exponential time [9, 8].

2-way QFAs of [13] allow the automaton to be in a quantum state that consists of different locations on the input tape. It has been argued that such an automaton is not truly finite [2], since it maintains a quantum state of size $O(m)$ where m is the length of the input word.

This concern has lead to defining QCFAs, a model of automata in which the movements of automaton's head are classical but its internal state is quantum [4]. The quantum state of such automaton is always finite-dimensional. QCFAs still have advantage over the classical automata, being able to recognize $L = \{a^m b^m\}$ in polynomial time and palyndromes in exponential time [4]. More generally, QCFAs can recognize any language in the class $S_Q^=$ [22]. ($S_Q^=$ is the class of languages L for which there exists a probabilistic automaton M with rational transition amplitudes such that $x \in L$ if and only if M accepts x with probability exactly $1/2$.)

It remains an open problem to characterize the class of languages recognizable by QCFAs. There are also no results proving that concrete languages L are not recognizable by QCFAs. For example, can we show that $L = \{a^n b^{n^2}\}$ or $L = \{a^n b^{2^n}\}$ is not recognizable by QFAs?

3. QFAs and quantum Markov chains.

When analyzing probabilistic and quantum automata, it is often useful to consider the behaviour of an automaton on words x^n for large n. For 1-way automata, the automaton is then equivalent to a Markov chain, with reading the word x being one step of the automaton. In the impossibility results about QFAs, several lemmas are natural quantum counterparts of well known Markov chain results. The first result of this type is

Lemma 1. *[2, Lemma 1] Let x be a word. Let M be a 1-way QFA in the Kondacs-Watrous model and let $\mathcal{H}$ be the state space of M. Then, $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ where $\mathcal{H}_1, \mathcal{H}_2$ have the following properties:*

(a) All states in $\mathcal{H}_1$ are non-halting states and reading x in a state $|\psi\rangle \in \mathcal{H}_1$ leads to a state $|\psi'\rangle \in \mathcal{H}_1$.

(b) Let p_n be the probability of M entering a halting state if it starts in $|\psi\rangle \in \mathcal{H}_2$ and reads x^n. If $n \to \infty$, then $p_n \to 1$.

The corresponding Markov chain result is as follows [12]. For a classical Markov chain, its states can be partitioned into a set of *recurrent* states R and a set of *transient* states T. If a Markov chain starts in a recurrent state q, it returns to q with probability 1. For transient states q, the probability of returning to q after n steps tends to 0, as n tends to infinity.

The Lemma above is a counterpart of this result in a different mathematical setting. The subspace $\mathcal{H}_1$ corresponds to the set of recurrent states R. The subspace $\mathcal{H}_2$ corresponds to the set of transient states.

Some other results exploring the parallels between QFAs and Markov chains can be found in [1] and [10] but there is no systematic theory of quantum Markov chains yet. Developing such a theory is an important direction for future work.

References

[1] A. Ambainis, M. Beaudry, M. Golovkins, A. Ķikusts, M. Mercer, and D. Thérien. Algebraic results on quantum automata. *Theory of Computing Systems*, 39(1):165–188, 2006.

[2] A. Ambainis and R. Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. *Proceedings of FOCS'98*, pages 332–341.

[3] A. Ambainis and N. Nahimovs. Improved constructions of quantum automata. *Theoretical Computer Science*, 410(20):1916–1922, 2009.

[4] A. Ambainis and J. Watrous. Two–way finite automata with quantum and classical states. *Theoretical Computer Science*, 287(1):299–311, 2002.

[5] A. Ambainis, A. Yakaryilmaz. Automata and Quantum Computing, submitted for publication.

[6] A. Bertoni, C. Mereghetti, and B. Palano. Small size quantum automata recognizing some regular languages. *Theoretical Computer Science*, 340(2):394–407, 2005.

[7] M. P. Ciamarra. Quantum reversibility and a new model of quantum automaton. In *FCT*, volume 2138 of *LNCS*, pages 376–379, 2001.

[8] C. Dwork and L. Stockmeyer. A time complexity gap for two-way probabilistic finite-state automata. *SIAM Journal on Computing*, 19(6):1011–1123, 1990.

[9] R. Freivalds. Probabilistic two-way machines. *Proceedings of MFCS'81*, pages 33–45.

[10] M. Golovkins, M. Kravtsev, V. Kravcevs. Quantum Finite Automata and Probabilistic Reversible Automata: R-trivial Idempotent Languages. *Proceedings of MFCS'2011*, to appear. Also available at arXiv:1106.2530.

[11] P. Kaye, R. Laflamme, M. Mosca. *An Introduction to Quantum Computing.* Cambridge University Press, 2007.

[12] J. Kemeny, J. L. Snell. *Finite Markov chains.* Van Nostrand, Princeton, N.J. , 1960

[13] A. Kondacs and J. Watrous. On the power of quantum finite state automata. *Proceedings of FOCS'97*, pages 66–75.

[14] C. Mereghetti and B. Palano. On the size of one-way quantum finite automata with periodic behaviors. *Theoretical Informatics and Applications*, 36(3):277–291, 2002.

[15] C. Mereghetti and B. Palano. Quantum finite automata with control language. *Theoretical Informatics and Applications*, 40(2):315–332, 2006.

[16] C. Moore and J. P. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237(1-2):275–306, 2000.

[17] M. Nielsen, I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[18] K. Paschen. Quantum finite automata using ancilla qubits. Technical report, University of Karlsruhe, 2000.

[19] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. Earlier version in IEEE FOCS 1994. quant-ph/9508027.

[20] D. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26:1474-1483, 1997.

[21] A. Yakaryilmaz. Exact quantum algorithms for promise problems in automata theory. arXiv:1101.3837.

[22] A. Yakaryılmaz and A. C. C. Say. Succinctness of two-way probabilistic and quantum finite automata. *Discrete Mathematics and Theoretical Computer Science*, 12(2):19–40.