Superiority of exact quantum automata for promise problems

Andris Ambainis* and Abuzer Yakaryılmaz**

University of Latvia, Faculty of Computing, Raina bulv. 19, Riga, LV-1586, Latvia

{ambainis,abuzer}@lu.lv

October 26, 2018

Abstract. In this note, we present an infinite family of promise problems which can be solved exactly by just tuning transition amplitudes of a two-state quantum finite automata operating in realtime mode, whereas the size of the corresponding classical automata grow without bound.

Keywords: exact quantum computation, promise problems, succinctness, quantum finite automaton, classical finite automaton

1 Introduction

The exact quantum computation has been widely examined for partial (promise) and total functions (e.g. [BH97, BV97, BBC+98, BCdWZ99, Kla00, BdW03, MNYW05, FI09, YFSA10]). On the other hand, in automata theory, only two results have been obtained:

(i) Klauck [Kla00] has shown that realtime quantum finite automata (QFAs) cannot be more concise than realtime deterministic finite automata (DFAs) [1] in case of language recognition,

(ii) Murakami et. al. [MNYW05] have shown that there is a promise problem solvable by quantum pushdown automata but not by any deterministic pushdown automata.

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

** Yakaryılmaz was partially supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) with grant 108E142 and FP7 FET-Open project QCS.

[1] The proof was basically given for Kondacs-Watrous realtime QFA model [KW97] but it can be extended for any model of realtime QFAs including the most general ones [Cia01, BMP03, Hir10, YS11].

In this note, we consider succinctness of realtime QFAs for promise problems. We present an infinite family of promise problems which can be solved exactly by just tuning transition amplitudes of a two-state rtQFAs, whereas the size of the corresponding classical automata grow without bound.

2 Background

Throughout the paper,

(i) Σ denotes the input alphabet not containing left- and right-end markers (¢ and \$, respectively) and $\tilde{\Sigma} = \Sigma \cup \{¢, \$\}$,
(ii) ε is the empty string,
(iii) w_i is the i^{th} symbol of a given string w, and
(iv) $\tilde{w}$ represents the string ¢w\$, for $w \in \Sigma^*$.

Moreover, all machines presented in the paper operate in realtime mode. That is, the input head moves one square to the right in each step and the computation stops after reading \$.

A promise problem is a pair $A = (A_{yes}, A_{no})$, where $A_{yes}, A_{no} \subseteq \Sigma^*$ and $A_{yes} \cap A_{no} = \emptyset$ [Wat09]. A promise problem $A = (A_{yes}, A_{no})$ is solved exactly by a machine $\mathcal{M}$ if each string in A_{yes} (resp., A_{no}) is accepted (resp., rejected) exactly by $\mathcal{M}$. Note that, if $\overline{A_{yes}} = A_{no}$, this is the same as the recognition of a language (A_{yes}).

We give our quantum result with the most restricted of the known QFA model, i.e. *Moore-Crutchfield quantum finite automaton* (MCQFA) [MC00], (see [YS11] for the definition of the most general QFA model).

A MCQFA is a 5-tuple

$$\mathcal{M} = (Q, \Sigma, \{U_\sigma \mid \sigma \in \tilde{\Sigma}\}, q_1, Q_a),$$

where Q is the set of states, q_1 is the initial state, $Q_a \subseteq Q$ and is the set of accepting states, and U_σ's are unitary operators. The computation of a MCQFA on a given input string $w \in \Sigma^*$ can be traced by a $|Q|$-dimensional vector. This vector is initially set to $|v_0\rangle = (1 \ 0 \ \cdots \ 0)^T$ and evolves according to

$$|v_i\rangle = U_{\tilde{w}_i} |v_{i-1}\rangle, \qquad 1 \leq i \leq |\tilde{w}|.$$

At the end of the computation, w is accepted (resp., rejected) with probability $||P_a v_{|\tilde{w}|}||^2$ (resp., $||P_r v_{|\tilde{w}|}||^2$), where $P_a = \sum_{q \in Q_a} |q\rangle\langle q|$ and $P_r = I - P_a$. If we replace the unitary operation with a zero-one left stochastic operator, we obtains a realtime DFA (which we call simply a DFA).

3 The main results

Let $A^k_{yes} = \{a^{i2^k} \mid i \text{ is a nonnegative } \textit{even} \text{ integer}\}$ and $A^k_{no} = \{a^{i2^k} \mid i \text{ is a positive } \textit{odd} \text{ integer}\}$ be two unary languages, where k is a positive integer. We will show that a two-state MCQFA can solve promise problem $A^k = (A^k_{yes}, A^k_{no})$, but any DFA (and so any PFA) must have at least $2N$ states to solve the same problem exactly.

Theorem 1. *Promise problem $A^k = (A^k_{yes}, A^k_{no})$ can be solved by a two-state MCQFA $\mathcal{M}_k$ exactly.*

Proof. We will use a well-known technique given in [AF98]. Let $N = 2^k$ and $\mathcal{M}_k = (Q, \Sigma, \{U_\sigma \mid \sigma \in \tilde{\Sigma}\}, q_1, Q_a)$, where $Q = \{q_1, q_2\}$, $\Sigma = \{a\}$, $Q_a = \{q_1\}$, $U_¢ = U_\$ = I$, and U_a is a rotation in $|q_1\rangle$-$|q_2\rangle$ plane with angle $\theta = \frac{\pi}{2N}$, i.e.,

$$U_a = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

The computation begins with $|q_1\rangle$ and after reading each block of N a's, the following pattern is followed by $\mathcal{M}_k$:

$$|q_1\rangle \xrightarrow{a^N} |q_2\rangle \xrightarrow{a^N} -|q_1\rangle \xrightarrow{a^N} -|q_2\rangle \xrightarrow{a^N} |q_1\rangle \xrightarrow{a^N} \cdots .$$

Therefore, it is obvious that $\mathcal{M}_k$ solves promise problem A^k exactly. □

Lemma 1. *Any DFA solving $A^k = (A^k_{yes}, A^k_{no})$ exactly must have at least 2^{k+1} states.*

Proof. Let $N = 2^k$ and $\mathcal{D}$ be a m-state DFA solving A^k exactly. We show that m cannot be less than $2N$.

Since both A^k_{yes} and A^k_{no} contain infinitely many unary strings, there must be a chain of t states, say $s_0, \ldots, s_{t-1}$ such that, for sufficiently long strings, $\mathcal{D}$ enters this chain in which $\mathcal{D}$ transmits from s_i to $s_{(i+1 \mod t)}$ when reading an a, where $0 \le i \le t-1$ and $0 < t \le m$.

Without lose of generality, we assume that $\mathcal{D}$ accepts the input if it is in s_0 before reading \$. Thus, $\mathcal{D}$ rejects the input if it is in $s_{(N \mod t)}$ before reading \$. Let S_a be the set of $\{s_{(i2N \mod t)} \mid i \ge 0\}$. Then, $\mathcal{D}$ accepts the input if it is in one of the states in S_a before reading \$. Note that $s_{(N \mod t)} \notin S_a$.

Let $d = \gcd(t, 2N)$, $t' = \frac{t}{d}$, and S' be the set $\{s_{id} \mid 0 \le i < t'\}$. Since $S_a \subseteq S'$ and $|S'| = t'$, we can easily follow $S_a = S'$ if we show $|S_a| \ge t'$.

Firstly, we show that each i satisfying ($i2N \equiv 0 \mod t$) must be a multiple of t': For such an i, there exists a j such that $i2N = jt$. By dividing both sides with $t = dt'$, we get $\frac{i}{t'}\frac{2N}{d} = j$. This implies that i must be a multiple of t' since left side must be an integer and $gcd(t', 2N) = 1$.

Secondly, we show that there is no i_1 and i_2, i.e. $t' > i_1 > i_2 \geq 0$, such that $(i_1 2N \equiv i_2 2N \mod t)$. If so, we have $(i_1 2N - i_2 2N \equiv 0 \mod t)$ and then $((i_1 - i_2)2N \equiv 0 \mod t)$. This implies that $(i_1 - i_2)$ must be a multiple of t'. This is a contradiction.

Thus, for each $i \in \{0, \ldots, t'-1\}$, we obtain a different value of $(i2N \mod t)$ and so $|S_a|$ contains at least t' elements.

If $\gcd(t, N) = d$, then $s_{(N \mod t)}$ also becomes a member of S_a. Therefore, $\gcd(t, N)$ must be different than $\gcd(t, 2N)$. This can only be possible whenever t is a multiple of $2N$. Therefore, m cannot be less than $2N$. □

Since a 2^{k+1}-state DFA solving promise problem A^k exactly can be constructed in a straightforward way, we obtain the following theorem.

Theorem 2. *The minimal DFA solving the promise problem $A^k = (A^k_{yes}, A^k_{no})$ exactly has 2^{k+1} states.*

4 Concluding remarks

In this paper, we identify a case in which the superiority of quantum computation to classical one cannot be bounded. For this purpose, we use an infinite family of two unary disjoint languages containing the strings of the form $(a^{2n})^*$ and $a^n(a^{2n})^*$, respectively, where n is a power of 2.

What happens if n is not an exact power of 2? For quantum case, we can still solve the same problem with 2 states. On the other hand, for the classical case, the minimum number of states is determined by the biggest factor of the number, which is a power of 2. Let $k, l > 0$. Let $N = 2^k(2l+1)$ and $A^N = (A^N_{yes}, A^N_{no})$ (where $A^N_{yes} = \{a^{iN} \mid i \text{ is a nonnegative } \textit{even} \text{ integer}\}$ and $A^N_{no} = \{a^{iN} \mid i \text{ is a positive } \textit{odd} \text{ integer}\}$) be a promise problem.

Corollary 1. *The minimal DFA solving promise problem $A^N = (A^N_{yes}, A^N_{no})$ exactly has 2^{k+1} states.* [2]

Therefore, if N is an odd integer, a DFA only needs 2 states to solve the related promise problems.

[2] The proof can be obtained by using almost the same technique given in Section 2.

References

AF98. Andris Ambainis and Rūsiņš Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *FOCS'98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 332–341, 1998.

BBC+98. Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *FOCS'98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 352–361, 1998.

BCdWZ99. Harry Buhrman, Richard Cleve, Ronald de Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. In *FOCS'99: Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 358–359, 1999.

BdW03. Harry Buhrman and Ronald de Wolf. Quantum zero-error algorithms cannot be composed. *Information Processing Letters*, 87:79–84, 2003.

BH97. Gilles Brassard and Peter Hoyer. An exact quantum polynomial-time algorithm for simon's problem. In *ISTCS'97: Proceedings of the Fifth Israel Symposium on the Theory of Computing Systems*, pages 12–23, 1997.

BMP03. Alberto Bertoni, Carlo Mereghetti, and Beatrice Palano. Quantum computing: 1-way quantum automata. In Zoltán Ésik and Zoltán Fülöp, editors, *Developments in Language Theory*, volume 2710 of *LNCS*, pages 1–20, 2003.

BV97. Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

Cia01. Massimo Pica Ciamarra. Quantum reversibility and a new model of quantum automaton. In *FCT'01: Proceedings of the 13th International Symposium on Fundamentals of Computation Theory*, pages 376–379, 2001.

FI09. Rūsiņš Freivalds and Kazuo Iwama. Quantum queries on permutations with a promise. In *CIAA'09: Proceedings of the 14th International Conference on Implementation and Application of Automata*, pages 208–216, 2009.

Hir10. Mika Hirvensalo. Quantum automata with open time evolution. *International Journal of Natural Computing Research*, 1(1):70–85, 2010.

Kla00. Hartmut Klauck. On quantum and probabilistic communication: Las vegas and one-way protocols. In *STOC'00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 644–651, 2000.

KW97. Attila Kondacs and John Watrous. On the power of quantum finite state automata. In *FOCS'97: Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 66–75, 1997.

MC00. Cristopher Moore and James P. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237(1-2):275–306, 2000.

MNYW05. Yumiko Murakami, Masaki Nakanishi, Shigeru Yamashita, and Katsumasa Watanabe. Quantum versus classical pushdown automata in exact computation. *IPSJ Digital Courier*, 1:426–435, 2005.

Wat09. John Watrous. Quantum computational complexity. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer, 2009.

YFSA10. Abuzer Yakaryılmaz, Rūsiņš Freivalds, A. C. Cem Say, and Ruben Agadzanyan. Quantum computation with devices whose contents are never read. In *Unconventional Computation*, volume 6079 of *Lecture Notes in Computer Science*, pages 164–174, 2010.

YS11. Abuzer Yakaryılmaz and A. C. Cem Say. Unbounded-error quantum computation with small space bounds. *Information and Computation*, 209(6):873–892, 2011.