2Q-06 1方向確率可逆および量子1カウンタオートマトンについて

山崎智弘, 小林弘忠, 徳永裕己, 今井浩
東京大学大学院理学系研究科情報科学専攻

1 Introduction

It has been widely considered that quantum mechanism gives new great power for computation after Shor [6] showed the existence of quantum polynomial time algorithm for integer factoring problem. However, it has been still unclear why quantum computers are so powerful. In this context, it is worth considering simpler models such as finite automata.

Quantum finite automata were introduced by Moore and Crutchfield [5] and Kondacs and Watrous [3], independently. The latter showed that the class of languages recognizable by bounded error 1-way quantum finite automata (1QFAs) is properly contained in the class of regular languages.Ambainis and Freivalds [2] studied the characterizations of 1QFAs in more detail by comparing 1QFAs with 1-way probabilistic reversible finite automata (1PRFAs), since 1PRFAs are clearly special cases of 1QFAs. They showed that there exist languages, such as $\{a^*b^*\}$, which can be recognized by bounded error 1QFAs but not by bounded error 1PRFAs. However, as we show in this paper, this situation seems different in case of automata with one counter.

Kravtsev [4] introduced 1-way quantum 1-counter automata (1Q1CAs), and showed that several non-context-free languages can be recognized by bounded error 1Q1CAs. No clear comparisons with other automata such as 1-way deterministic 1-counter automata (1D1CAs) or 1-way probabilistic reversible 1-counter automata (1PR1CAs) were done in [4]. In this paper, we investigate the power of 1Q1CAs in comparison with 1PR1CAs.

2 Definitions

Definition 1 *A 1-way deterministic 1-counter automaton (1D1CA) is defined by a 6-tuple* $M = (Q, \Sigma, \delta, q_0, Q_{\rm acc}, Q_{\rm rej})$, *where* Q *is a finite set of states,* Σ *is a finite input alphabet,* q_0 *is the initial state,* $Q_{\rm acc} \subset Q$ *is a set of accepting states,* $Q_{\rm rej} \subset Q$ *is a set of rejecting states, and* $\delta : Q \times \Gamma \times S \to Q \times \{-1, 0, +1\}$ *is a transition function, where* $\Gamma = \Sigma \cup \{¢, \$\}$, *symbol* $¢ \notin \Sigma$ *is the left end-marker, symbol* $\$ \notin \Sigma$ *is the right end-marker, and* $S = \{0, 1\}$.

We assume that each 1D1CA has a counter which can contain an arbitrary integer and the counter value is 0 at the start of computation. $-1, 0, +1$ respectively, decreases by 1, retains the same and increases by 1 the counter value. Let $s = \mathrm{sign}(k)$, where k is the counter value and $\mathrm{sign}(k) = 0$ if $k = 0$, otherwise 1. We also assume that all inputs are started by ¢ and terminated by \$.

The automaton starts in q_0 and reads an input w from left to right. At the ith step, it reads a symbol w_i in the state q, checks whether the counter value is 0 or not (i.e. checks s) and finds an appropriate transition $\delta(q, w_i, s) = (q', d)$. Then it updates its state to q' and the counter value according to d. The automaton accepts w if it enters the final state in $Q_{\rm acc}$ and rejects if it enters the final state in $Q_{\rm rej}$.

Definition 2 *A 1-way probabilistic 1-counter automaton (1P1CA) is defined by a 6-tuple* $M = (Q, \Sigma, \delta, q_0, Q_{\rm acc}, Q_{\rm rej})$. *A transition function* δ *is defined as* $Q \times \Gamma \times S \times Q \times \{-1, 0, +1\} \to \mathbb{R}^+$.

The definition of a counter remains the same as for 1D1CAs.

A language L is said recognizable by a 1P1CA with probability p if there exists a 1P1CA which accepts any input $x \in L$ with probability at least $p > 1/2$ and rejects any input $x \notin L$ with probability at least p. We may use the term "accepting probability" for denoting this probability p.

Definition 3 *A 1-way probabilistic reversible 1-counter automaton (1PR1CA) is defined as a 1P1CA such that, for any* $q \in Q$, $\sigma \in \Gamma$ *and* $s \in \{0, 1\}$, *there is at most one state* $q' \in Q$ *such that* $\delta(q', \sigma, s, q, d)$ *is non-zero.*

Definition 4 *A 1-way quantum 1-counter automaton (1Q1CA) is defined by a 6-tuple* $M = (Q, \Sigma, \delta, q_0, Q_{\rm acc}, Q_{\rm rej})$. *A transition function* δ *is defined as* $Q \times \Gamma \times S \times Q \times \{-1, 0, +1\} \to \mathbb{C}^+$, *where* $\Gamma, ¢, \$$.

The definition of a counter remains the same as for 1D1CAs. The definition of the recognizability remains the same as for 1P1CAs.

The number of configurations of a 1Q1CA on any input x of length n is precisely $(2n+1)|Q|$, since there are $2n+1$ possible counter value and $|Q|$ internal states. For fixed M, let C_n denote this set of configurations.

A computation on an input x of length n corresponds to a unitary evolution in the Hilbert space $\mathcal{H}_n = l_2(C_n)$. For each $(q, k) \in C_n, q \in Q, k \in [-n, n]$, let $|q, k\rangle$ denote the basis vector in $l_2(C_n)$.

A unitary operator U^δ_σ for a symbol σ on $\mathcal{H}_n$ is defined as follows:

$$U^\delta_\sigma |q, k\rangle = \textstyle\sum_{q', d} \delta(q, \sigma, \mathrm{sign}(k), q', d) |q', k + d\rangle,$$

One-way probabilistic reversible and quantum one-counter automata

Tomohiro Yamasaki, Hirotada Kobayashi, Yuuki Tokunaga, Hiroshi Imai
Department of Information Science, Faculty of Science, University of Tokyo
7–3–1 Hongo, Bunkyo-ku, Tokyo 113–0033, Japan

3 Recognizability of $L_{k,\mathrm{eq}}$

Here we show that non-context-free language $L_{k,\mathrm{eq}} = \{a_1^n a_2^n \cdots a_k^n\}$ for each fixed $k \geq 2$, is recognizable by a bounded error 1PR1CA.

Theorem 1 *For each $k \geq 2$, there exists a 1PR1CA $M_{\mathrm{PR}}(L_{k,\mathrm{order}})$ for $L_{k,\mathrm{order}}$ with probability $1/2+1/(4k-6)$.*

It has been known that, while there exists a 1QFA which recognizes $L_{k,\mathrm{order}}$ with bounded error, any 1PRFA cannot recognize $L_{k,\mathrm{order}}$ with bounded error [2, 1]. In this point, Theorem 1 gives a contrastive result between no-counter and one-counter cases.

Theorem 2 *For each $k \geq 2$, there exists a 1PR1CA $M_{\mathrm{PR}}(L_{k,\mathrm{eq}})$ for $L_{k,\mathrm{eq}}$ with probability $1/2+1/(8k-10)$.*

4 Improving the accepting probability of 1Q1CA for $L_{k,\mathrm{eq}}$

In the previous section, we showed that $L_{k,\mathrm{eq}} = \{a_1^n a_2^n \cdots a_k^n\}$ is recognizable by a bounded error 1PR1CA. In this section, we show that, in a quantum case, we can improve the accepting probability in a strict sense by using quantum interference.

4.1 Quantum interference of states

Theorem 3 *By using quantum interference of the states, for each $k \geq 2$, $L_{k,\mathrm{eq}}$ can be recognized by a 1Q1CA $M_{\mathrm{Q1}}(L_{k,\mathrm{eq}})$ with probability p, where p is the root of $p^{(k+1)/(k-1)} + p = 1$ in the interval of $(1/2, 1)$.*

Proposition 1 *For each $k \geq 2$, $1/2+1/(8k-10) < p$, where p is the root of $p^{(k+1)/(k-1)} + p = 1$.*

4.2 Quantum interference of states and counter value

Here we consider quantum interference of not only the states, but also the counter value.

Theorem 4 *By using quantum interference of the states and the counter value, for fixed $k \geq 2$, $L_{k,\mathrm{eq}}$ can be recognized by a 1Q1CA $M_{\mathrm{Q2}}(L_{k,\mathrm{eq}})$ with probability $1/2 + (k-1)/2(k^2-k+1)$.*

Proposition 2 *For each $k \geq 3$, $p < 1/2 + (k-1)/2(k^2-k+1)$, where p is the root of $p^{(k+1)/(k-1)}+p = 1$.*

5 Relation between 1D1CAs and 1Q1CAs

As we have seen in previous sections, some non-context-free languages can be recognized by bounded error 1Q1CAs. This indicates the strength of 1Q1CAs. Conversely, we present the weakness of 1Q1CAs by showing that there is a regular language which can be recognized by a 1D1CA but not by a 1Q1CA with bounded error.

Theorem 5 *The language $\{\{a,b\}^* a\}$ cannot be recognized by a 1Q1CA with bounded error.*

6 Conclusions and open problems

In this paper, we showed that a family of non-context-free languages $L_{k,\mathrm{eq}} = \{a_1^n a_2^n \cdots a_k^n\}$ can be recognized by 1PR1CAs and 1Q1CAs. By using quantum interference of the states, we can improve the accepting probability. Further, by using quantum interference of not only the states but also the counter value, we can again improve the accepting probability.

These facts indicate that 1Q1CAs are more powerful than 1PR1CAs.

However, it is still open whether there exist languages which can be recognized with bounded error by 1Q1CAs but not by 1PR1CAs.

References

[1] A. Ambainis, R. Bonner, R. Freivalds, and A. Ķikusts. Probabilities to accept languages by quantum finite automata. In *Proceedings of the 5th Annual International Conference on Computing and Combinatorics (COCOON'99), Lecture Notes in Computer Science*, Vol. 1627, pp. 174–183, 1999.

[2] A. Ambainis and R. Freivalds. 1-way quantum finite automata: Strengths, weakness and generalizations. In *Proceedings of the 39th Annual Symposium on Foundation of Computer Science*, pp. 332–341, 1998.

[3] A. Kondacs and J. Watrous. On the Power of Quantum Finite State Automata. In *Proceedings of the 38th Annual Symposium on Foundation of Computer Science*, pp. 66–75, 1997.

[4] M. Kravtsev. Quantum finite one-counter automata. In *Proceedings of the 26th Conference on Current Trends in Theory and Practice of Informatics (SOFSEM'99), Lecture Notes in Computer Science*, Vol. 1725, pp. 431–440, 1999.

[5] C. Moore and J. Crutchfield. Quantum automata and quantum grammars. Technical Report 97-07-02, Santa-Fe Institute Working Paper, 1997.

[6] P. Shor. Algorithms for quantum computation: Discrete log and factoring. In *Proceedings of the 35th Annual Symposium on Foundation of Computer Science*, pp. 56–65, 1994.