数理解析研究所講究録
1166 巻 2000 年 244-252

1 方向確率的可逆および 1 方向量子 1 カウンタオートマトン

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
113-0033 東京都文京区本郷 7-3-1
{yamasaki, hirotada, tokunaga, imai}@is.s.u-tokyo.ac.jp

要旨 Kravtsev は 1 方向量子 1 カウンタオートマトン (1Q1CA) を提唱し, いくつかの非文脈自由言語が 1Q1CA によって受理されることを示した. 本論文ではまず, これらの言語全てが 1 方向確率的可逆 1 カウンタオートマトン (1PR1CA) でも受理でき, しかも受理確率は Kravtsev によるもとの 1Q1CA よりも高いことを示す. 次に, それぞれの $k \geq 2$ に対して $\{a_1^{m_1} \cdots a_k^{m_k} \mid m_1 = \cdots = m_k\}$ を受理する 1PR1CA が (従って 1Q1CA も) 存在することを示すと同時に, 量子干渉を用いると 1Q1CA では受理確率を真に高められることも示す. これらの言語は非文脈自由であるため, 1 方向決定性 1 カウンタオートマトン (1D1CA) では認識できない. 一方で, 1D1CA で認識可能な正則言語 $\{\{a,b\}^*a\}$ は 1Q1CA で認識できないことを示す.

One-way Probabilistic Reversible and Quantum One-counter Automata

Tomohiro Yamasaki, Hirotada Kobayashi, Yuuki Tokunaga, and Hiroshi Imai

Department of Information Science, Faculty of Science, University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
{yamasaki, hirotada, tokunaga, imai}@is.s.u-tokyo.ac.jp

Abstract Kravtsev introduced 1-way quantum 1-counter automata (1Q1CAs), and showed that several non-context-free languages can be recognized by bounded error 1Q1CAs. In this paper, we first show that each of these languages can be also recognized by bounded error 1-way probabilistic reversible 1-counter automata (1PR1CAs) with probability greater than that of corresponding Kravtsev's original 1Q1CA. Second, we show that there exists a bounded error 1PR1CA (and so 1Q1CA) which recognizes $\{a_1^{m_1} \cdots a_k^{m_k} \mid m_1 = \cdots = m_k\}$, for each $k \geq 2$. We also show that, in a quantum case, we can improve the accepting probability in a strict sense by using quantum interference. Third, we state a relation between 1-way deterministic 1-counter automata (1D1CAs) and 1Q1CAs. On one hand, all of above mentioned languages cannot be recognized by 1D1CAs because they are non-context-free. On the other hand, we show that a regular language $\{\{a,b\}^*a\}$ cannot be recognized by bounded error 1Q1CAs.

1 Introduction

It has been widely considered that quantum mechanism gives new great power for computation after Shor [8] 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 [6] 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. This means that 1QFAs are strictly less powerful than classical 1-way deterministic finite automata. This weakness comes from the restriction of reversibility. Since any quantum computation is performed by unitary operators and unitary operators are reversible, any transition function of quantum computation must be reversible. 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 $L_{i=j=k} = \{a^iba^jba^k \mid i = j = k,\ i,j,k \geq 0\}$, $L_{k=i\neq j \vee k=j\neq i} = \{a^iba^jba^k \mid k = i \neq j \vee k = j \neq i,\ i,j,k \geq 0\}$, and $L_{\text{exact2}} = \{a^iba^jba^k \mid$ exactly 2 of i,j,k are equal, $i,j,k \geq 0\}$, 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 and 1D1CAs.

We first show that all of these non-context-free languages can be also recognized by bounded error 1PR1CAs (and so 1Q1CAs). Moreover, the accepting probability of each of these 1PR1CAs is strictly greater than, or at least equal to, that of corresponding Kravtsev's original 1Q1CA.

Second, we show that there exists a bounded error 1PR1CA (and so 1Q1CA) which recognizes $L^{(k)}_{\text{ordered}} = \{a_1^* \cdots a_k^*\}$, for each $k \geq 2$. This result is in contrast to the case of no counter shown by Ambainis and Freivalds [2] and Ambainis et. al. [1]. We extend this result by showing that there exists a bounded error 1PR1CA (and so 1Q1CA) which recognizes $L^{(k)}_{m_1=\cdots=m_k} = \{a_1^{m_1} \cdots a_k^{m_k} \mid m_1 = \cdots = m_k\}$, for each $k \geq 2$. We also show that, in a quantum case, we can improve the accepting probability in a strict sense by using quantum interference.

Third, we state the relation between 1D1CAs and 1Q1CAs. On one hand, all of above mentioned languages cannot be recognized by 1D1CAs because they are non-context-free. On the other hand, we show that a regular language $\{\{a,b\}^*a\}$ cannot be recognized by bounded error 1Q1CAs.

2 Definitions

Definition 1 *A 1-way deterministic 1-counter automaton (1D1CA) is defined by a 6-tuple* $M = (Q, \Sigma, \delta, q_0, Q_{\text{acc}}, Q_{\text{rej}})$, *where* Q *is a finite set of states,* Σ *is a finite input alphabet,* q_0 *is the initial state,* $Q_{\text{acc}} \subset Q$ *is a set of accepting states,* $Q_{\text{rej}} \subset Q$ *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 $s = \text{sign}(k)$, where k is the counter value and $\text{sign}(k) = 0$ 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_{acc} and rejects if it enters the final state in Q_{rej}.

Definition 2 *A 1-way reversible 1-counter automaton (1R1CA) is defined as a 1D1CA 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* $\delta(q', \sigma, s) = (q, d)$.

Definition 3 *A 1-way probabilistic 1-counter automaton (1P1CA) is defined by a 6-tuple* $M = (Q, \Sigma, \delta, q_0, Q_{\text{acc}}, Q_{\text{rej}})$, *where* Q, Σ, q_0, Q_{acc}, *and* Q_{rej} *are the same as for 1D1CAs. A transition function* δ *is defined as* $Q \times \Gamma \times S \times Q \times \{-1, 0, +1\} \to \mathbb{R}^+$, *where* $\Gamma, ¢, \$$, *and* S *are the same as for 1D1CAs. For any* $q, q' \in Q, \sigma \in \Gamma, s \in \{0, 1\}, d \in \{-1, 0, +1\}$, δ *satisfies the following condition:*

$$\sum_{q',d} \delta(q, \sigma, s, q', d) = 1.$$

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 4 *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 5 *A 1-way quantum 1-counter automaton (1Q1CA) is defined by a 6-tuple $M = (Q, \Sigma, \delta, q_0, Q_{\mathrm{acc}}, Q_{\mathrm{rej}})$, where Q, Σ, q_0, Q_{acc}, and Q_{rej} are the same as for 1D1CAs. A transition function δ is defined as $Q \times \Gamma \times S \times Q \times \{-1,0,+1\} \to \mathbb{C}^+$, where $\Gamma, ¢, \$$, and S are the same as for 1D1CAs. For any $q, q' \in Q, \sigma \in \Gamma, s \in \{0,1\}, d \in \{-1,0,+1\}$, δ satisfies the following conditions:*

$$\sum_{q',d} \delta^\dagger(q_1, \sigma, s_1, q', d)\delta(q_2, \sigma, s_2, q', d) = \begin{cases} 1 & (q_1 = q_2) \\ 0 & (q_1 \neq q_2) \end{cases},$$

$$\sum_{q',d} \delta^\dagger(q_1, \sigma, s_1, q', +1)\delta(q_2, \sigma, s_2, q', 0) + \delta^\dagger(q_1, \sigma, s_1, q', 0)\delta(q_2, \sigma, s_2, q', -1) = 0,$$

$$\sum_{q',d} \delta^\dagger(q_1, \sigma, s_1, q', +1)\delta(q_2, \sigma, s_2, q', -1) = 0.$$

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_σ^δ for a symbol σ on $\mathcal{H}_n$ is defined as follows:

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

To describe concrete automata easily, we use simple 1Q1CAs. A 1Q1CA is said simple if for any $\sigma \in \Gamma, s \in \{0,1\}$, there is a unitary operator $V_{\sigma,s}$ on $l_2(Q)$ and a counter function $D : Q \times \Gamma \to \{-1,0,+1\}$ such that

$$\delta(q, \sigma, s, q', d) = \begin{cases} \langle q'|V_\sigma|q\rangle & \text{if } D(q', \sigma) = d \\ 0 & \text{otherwise} \end{cases},$$

where $\langle q'|V_{\sigma,s}|q\rangle$ is the coefficient of $|q\rangle \in V_{\sigma,s}|q\rangle$. For convenience, we also use this representation for 1D1CA, 1R1CA, and 1PR1CA.

3 Recognizability of some non-context-free languages

Kravtsev [4] showed that several non-context-free languages such as $L_{i=j=k} = \{a^i b a^j b a^k \mid i=j=k,\ i,j,k \geq 0\}$, $L_{k=i\neq j \vee k=j\neq i} = \{a^i b a^j b a^k \mid k=i\neq j \vee k=j\neq i,\ i,j,k \geq 0\}$, and $L_{\mathrm{exact2}} = \{a^i b a^j b a^k \mid$ exactly 2 of i,j,k are equal, $i,j,k \geq 0\}$, can be recognized by bounded error 1Q1CAs. In this section, we show that all of these languages can be also recognized by bounded error 1PR1CAs. Moreover, the accepting probability of each of these 1PR1CAs is strictly greater than, or at least equal to, that of corresponding Kravtsev's original 1Q1CAs. This also indicates the existence of a 1Q1CA for each of these languages whose accepting probability is strictly greater than, or

at least equal to, that of corresponding Kravtsev's original one, since a 1PR1CA is regarded as a special case of a 1Q1CA.

Let $L_{i=j} = \{a^i b a^j b a^k \mid i=j,\ i,j,k \geq 0\}$ and $L_{i=(j+k)/2} = \{a^i b a^j b a^k \mid i=(j+k)/2,\ i,j,k \geq 0\}$. The existence of a 1R1CA for each of these can be shown easily.

Lemma 1 *There exist 1R1CAs* $M^{(R)}_{L_{i=j}}, M^{(R)}_{L_{j=k}}, M^{(R)}_{L_{k=i}}$ *for* $L_{i=j}, L_{j=k}, L_{k=i}$, *respectively.*

Lemma 2 *There exist 1R1CAs* $M^{(R)}_{L_{i=(j+k)/2}}$, $M^{(R)}_{L_{j=(k+i)/2}}$, $M^{(R)}_{L_{k=(i+j)/2}}$ *for* $L_{i=(j+k)/2}$, $L_{j=(k+i)/2}$, $L_{k=(i+j)/2}$, *respectively.*

Proof: We show the case of $L_{i=(j+k)/2}$. Other cases of $L_{j=(k+i)/2}, L_{k=(i+j)/2}$ can be shown in similar ways.

Let the state set $Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_{\rm acc}, q_{\rm rej1}, q_{\rm rej2}, q_{\rm rej3}, q_{\rm rej4}, q_{\rm rej5}\}$, where q_0 is an initial state, $q_{\rm acc}$ is an accepting state, and $q_{\rm rej1}, q_{\rm rej2}, q_{\rm rej3}, q_{\rm rej4}, q_{\rm rej5}$ are rejecting states. Define the transition matrices $V_{\sigma,s}$ and the counter function D of $M^{(R)}_{L_{i=(j+k)/2}}$ as follows:

$$
\begin{array}{llll}
V_{\text{¢},0}|q_0\rangle = |q_1\rangle, & V_{\$,0}|q_1\rangle = |q_{\rm rej1}\rangle, & V_{a,0}|q_1\rangle = |q_1\rangle, & V_{b,0}|q_1\rangle = |q_2\rangle, \\
 & V_{\$,0}|q_2\rangle = |q_{\rm rej2}\rangle, & V_{a,0}|q_2\rangle = |q_{\rm rej2}\rangle, & V_{b,0}|q_2\rangle = |q_4\rangle, \\
 & V_{\$,0}|q_4\rangle = |q_{\rm acc}\rangle, & V_{a,0}|q_4\rangle = |q_{\rm rej4}\rangle, & V_{b,0}|q_4\rangle = |q_{\rm rej4}\rangle, \\
 & & & \\
D(q_1,a) = +1, & V_{\$,1}|q_1\rangle = |q_{\rm rej1}\rangle, & V_{a,1}|q_1\rangle = |q_1\rangle, & V_{b,1}|q_1\rangle = |q_2\rangle, \\
D(q_2,a) = -1, & V_{\$,1}|q_2\rangle = |q_{\rm rej2}\rangle, & V_{a,1}|q_2\rangle = |q_3\rangle, & V_{b,1}|q_2\rangle = |q_4\rangle, \\
D(q_4,a) = -1, & V_{\$,1}|q_3\rangle = |q_{\rm rej3}\rangle, & V_{a,1}|q_3\rangle = |q_2\rangle, & V_{b,1}|q_3\rangle = |q_5\rangle, \\
D(q,\sigma) = 0, & V_{\$,1}|q_4\rangle = |q_{\rm rej4}\rangle, & V_{a,1}|q_4\rangle = |q_5\rangle, & V_{b,1}|q_4\rangle = |q_{\rm rej4}\rangle, \\
\text{otherwise}, & V_{\$,1}|q_5\rangle = |q_{\rm rej5}\rangle, & V_{a,1}|q_5\rangle = |q_4\rangle, & V_{b,1}|q_5\rangle = |q_{\rm rej5}\rangle.
\end{array}
$$

Reversibility of this automaton can be checked easily. □

3.1 Recognizability of $L_{i=j=k}$, $L_{k=i\neq j \vee k=j\neq i}$, and $L_{\rm exact2}$

Kravtsev [4] showed the recognizability of $L_{i=j=k} = \{a^i b a^j b a^k \mid i=j=k,\ i,j,k \geq 0\}$ with probability $1-1/c$ for arbitrary chosen $c \geq 3$ by a 1P1CA and a 1Q1CA. This 1P1CA for $L_{i=j=k}$ is clearly reversible, and so, $L_{i=j=k}$ is recognized by 1PR1CA with probability $1-1/c$.

Here we show the recognizability of $L_{k=i\neq j \vee k=j\neq i} = \{a^i b a^j b a^k \mid k=i\neq j \vee k=j\neq i,\ i,j,k \geq 0\}$.

Theorem 1 *There exists a 1PR1CA* $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ *which recognizes* $L_{k=i\neq j\vee k=j\neq i}$ *with probability* $3/5$.

Proof: After reading the left end-marker ¢, $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ enters one of the following three paths, path-1, path-2, path-3, with probability $1/4, 1/4, 1/2$, respectively.

In path-1(path-2), $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ checks whether $j = k (k = i)$ or not, by behaving in the same way as $M^{(R)}_{L_{j=k}} (M^{(R)}_{L_{k=i}})$ except for the treatment of acceptance and rejection. The input is accepted with probability $4/5$ if $j = k (k = i)$ is satisfied, while it is always rejected if $j \neq k (k \neq i)$.

In path-3, $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ checks whether $i \neq (j+k)/2$ or not, by behaving in the same way as $M^{(R)}_{L_{i=(j+k)/2}}$ except for the treatment of acceptance and rejection. The input is accepted with probability $4/5$ if $i \neq (j+k)/2$ is satisfied, while it is always rejected if $i = (j+k)/2$.

Then the input $x \in L_{k=i\neq j\vee k=j\neq i}$ always satisfies the condition of path-3 and exactly one of the conditions of first two paths. Hence, $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ accepts it with probability $3/5$. On

the other hand, $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ rejects any input $x \notin L_{k=i\neq j\vee k=j\neq i}$ with probability at least 3/5. Indeed, when the input satisfies $i = j = k$, the conditions of path-1 and path-2 are satisfied while the condition of path-3 is not satisfied, hence, $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ rejects it with probability 3/5. Next, when i, j, k differ from one another, none of the conditions of path-1 and path-2 are satisfied, hence $M^{(PR)}_{L_{k=i\neq j\vee k=j\neq i}}$ rejects it with probability at least 3/5. Finally, when the input is not in the form of $a^iba^jba^k$, it is always rejected, obviously.

Reversibility of this automaton is clear by its construction. □

Corollary 1 *There exists a 1Q1CA* $M^{(Q)}_{L_{k=i\neq j\vee k=j\neq i}}$ *which recognizes* $L_{k=i\neq j\vee k=j\neq i}$ *with probability* 3/5.

Note that the accepting probability 3/5 of this 1Q1CA $M^{(Q)}_{L_{k=i\neq j\vee k=j\neq i}}$ for $L_{k=i\neq j\vee k=j\neq i}$ is greater than the original Kravtsev's 4/7.

Next we show the recognizability of $L_{\text{exact2}} = \{a^iba^jba^k \mid$ exactly 2 of i, j, k are equal, $i, j, k \geq 0\}$.

Theorem 2 *There exists a 1PR1CA* $M^{(PR)}_{L_{\text{exact2}}}$ *which recognizes* L_{exact2} *with probability* 4/7.

Proof: Omitted. Similar to the proof of Theorem 1. □

Corollary 2 *There exists a 1Q1CA* $M^{(Q)}_{L_{\text{exact2}}}$ *which recognizes* L_{exact2} *with probability* 4/7.

Note that the accepting probability 4/7 of this 1Q1CA $M^{(Q)}_{L_{\text{exact2}}}$ for L_{exact2} is greater than the original Kravtsev's $1/2 + \epsilon$.

3.2 Recognizability of $L^{(k)}_{m_1=\cdots=m_k} = \{a_1^{m_1}\cdots a_k^{m_k} \mid m_1=\cdots=m_k\}$

Here we show that another family of non-context-free languages $L^{(k)}_{m_1=\cdots=m_k} = \{a_1^{m_1}\cdots a_k^{m_k} \mid m_1=\cdots=m_k\}$ for each fixed $k \geq 2$, is also recognizable by bounded error 1PR1CAs.

First we show that $L^{(k)}_{\text{ordered}} = \{a_1^*\cdots a_k^*\}$, for each fixed $k \geq 2$, is recognizable by a 1PR1CA with bounded error.

For each $k \geq 2$, let $L^{(k)}_{i|i+1} = \{\{a_1, \ldots, a_i\}^*\{a_{i+1}, \ldots, a_k\}^*\}$ for each $i, 1 \leq i \leq k-1$.

Lemma 3 *For each* $k \geq 2$, *there exists a 1R1CA* $M^{(R)}_{L^{(k)}_{i|i+1}}$ *for each* $L^{(k)}_{i|i+1}, 1 \leq i \leq k-1$.

Proof: Let the state set $Q = \{q_0, q_1, q_{\text{acc}}, q_{\text{rej}}\}$, where q_0 is an initial state, q_{acc} is an accepting state, and q_{rej} is a rejecting state. Define the transition matrices $V_{\sigma,s}$ and the counter function D of $M^{(R)}_{L^{(k)}_{i|i+1}}$ as follows:

$$V_{¢,0}|q_0\rangle = |q_1\rangle, \qquad V_{a_j,0}|q_1\rangle = |q_1\rangle, \quad 1 \leq j \leq i \qquad D(q_1, a_j) = +1, \quad i+1 \leq j \leq k$$
$$V_{a_j,1}|q_1\rangle = |q_{\text{rej}}\rangle, \quad 1 \leq j \leq i$$
$$V_{\$,0}|q_1\rangle = |q_{\text{acc}}\rangle, \qquad D(q, \sigma) = 0, \qquad \text{otherwise.}$$
$$V_{\$,1}|q_1\rangle = |q_{\text{acc}}\rangle, \qquad V_{a_j,0}|q_1\rangle = |q_1\rangle, \quad i+1 \leq j \leq k$$
$$V_{a_j,1}|q_1\rangle = |q_1\rangle, \quad i+1 \leq j \leq k$$

Reversibility of this automaton can be checked easily. □

Theorem 3 *For each* $k \geq 2$, *there exists a 1PR1CA* $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ *for* $L^{(k)}_{\text{ordered}}$ *with probability* $1/2 + 1/(4k-6)$.

Proof: After reading the left end-marker ¢, one of the following $k-1$ paths is chosen with the same probability $1/(k-1)$.

In the ith path, $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ checks whether the input is in $L^{(k)}_{\text{ordered}}$ or not, utilizing $M^{(R)}_{L^{(k)}_{i|i+1}}$, for $1 \le i \le k-1$. If the input is in $L^{(k)}_{i|i+1}$, $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ accepts it with probability p, while if the input is not in $L^{(k)}_{i|i+1}$, $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ always rejects it.

Since the input $x \in L^{(k)}_{\text{ordered}}$ satisfies the condition in any path, $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ accepts it with probability p. On the other hand, for any input $x \notin L^{(k)}_{\text{ordered}}$, there exists at least one path whose condition is not satisfied. Thus, the probability $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ is at most $p \cdot (k-2)/(k-1)$. Hence, if we take p such that $p \cdot (k-2)/(k-1) < 1/2 < p$, $M^{(PR)}_{L^{(k)}_{\text{ordered}}}$ recognizes $L^{(k)}_{\text{ordered}}$ with bounded error. To maximize the accepting probability, we solve $1 - p \cdot (k-2)/(k-1) = p$, which gives $p = 1/2 + 1/(4k-6)$.

Reversibility of this automaton is clear by its construction. □

Corollary 3 *For each $k \ge 2$, there exists a 1Q1CA $M^{(Q)}_{L^{(k)}_{\text{ordered}}}$ for $L^{(k)}_{\text{ordered}}$ with probability $1/2 + 1/(4k-6)$.*

It has been known that, while there exists a 1QFA which recognizes $L^{(k)}_{\text{ordered}}$ with bounded error, any 1PRFA cannot recognize $L^{(k)}_{\text{ordered}}$ with bounded error [2, 1]. In this point, Theorem 3 gives a contrastive result between no-counter and one-counter cases.

Before showing the recognizability of $L^{(k)}_{m_1=\cdots=m_k}$, we prove one more lemma. Let each $L^{(k)}_{\#a_i=\#a_{i+1}} = \{x \mid (\#\text{of } a_i \text{ in } x) = (\#\text{of } a_{i+1} \text{ in } x)\}$ for $1 \le i \le k-1$.

Lemma 4 *For each $k \ge 2$, there exists a 1R1CA $M^{(R)}_{L^{(k)}_{\#a_i=\#a_{i+1}}}$ for each $L^{(k)}_{\#a_i=\#a_{i+1}}$, $1 \le i \le k-1$.*

Proof: Let the state set $Q = \{q_0, q_1, q_{\text{acc}}, q_{\text{rej}}\}$, where q_0 is an initial state, q_{acc} is an accepting state, and q_{rej} is a rejecting state. Define the transition matrices $V_{\sigma,s}$ and the counter function D of $M^{(R)}_{L^{(k)}_{\#a_i=\#a_{i+1}}}$ as follows:

$$
\begin{array}{lll}
V_{¢,0}|q_0\rangle = |q_1\rangle, & V_{a_l,0}|q_1\rangle = |q_1\rangle, \quad 1 \le l \le k & D(q_1, a_i) = +1, \\
 & V_{a_l,1}|q_1\rangle = |q_{\text{rej}}\rangle, \quad 1 \le l \le k & D(q_1, a_j) = -1, \\
V_{\$,0}|q_1\rangle = |q_{\text{acc}}\rangle, & & \\
V_{\$,1}|q_1\rangle = |q_{\text{acc}}\rangle, & & D(q, \sigma) = 0, \text{ otherwise.}
\end{array}
$$

Reversibility of this automaton can be checked easily. □

Now we show the recognizability of $L^{(k)}_{m_1=\cdots=m_k} = \{a_1^{m_1} \cdots a_k^{m_k} \mid m_1 = \cdots = m_k\}$.

Theorem 4 *For each $k \ge 2$, there exists a 1PR1CA $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ for $L^{(k)}_{m_1=\cdots=m_k}$ with probability $1/2 + 1/(8k-10)$.*

Proof: After reading the left end-marker ¢, one of the following $2(k-1)$ paths, path-1-1, ..., path-1-$(k-1)$, path-2-1, ..., path-2-$(k-1)$, is chosen with the same probability $1/2(k-1)$.

In each path-1-i, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ checks whether the input string is in $L^{(k)}_{i|i+1}$ or not, utilizing $M^{(R)}_{L^{(k)}_{i|i+1}}$, for $1 \le i \le k-1$. If the input is in $L^{(k)}_{i|i+1}$, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ accepts it with probability p, while if the input is not in $L^{(k)}_{i|i+1}$, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ always rejects it.

In each path-2-i, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ checks whether the input is in $L^{(k)}_{\#a_i=\#a_{i+1}}$ or not, utilizing $M^{(R)}_{L^{(k)}_{\#a_i=\#a_{i+1}}}$, for $1 \leq i \leq k-1$. If the input is in $L^{(k)}_{\#a_i=\#a_{i+1}}$, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ accepts it with probability p, while if the input is not in $L^{(k)}_{\#a_i=\#a_{i+1}}$, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ always rejects it.

Since the input $x \in L^{(k)}_{m_1=\cdots=m_k}$ satisfies the condition in any path, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ accepts it with probability p. On the other hand, for any input $x \notin L^{(k)}_{m_1=\cdots=m_k}$, there exists at least one path whose condition is not satisfied. Thus, the probability $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ accepts it is at most $p \cdot (2k-3)/(2k-2)$. Hence, if we take p such that $p \cdot (2k-3)/(2k-2) < 1/2 < p$, $M^{(PR)}_{L^{(k)}_{m_1=\cdots=m_k}}$ recognizes $L^{(k)}_{m_1=\cdots=m_k}$ with bounded error. To maximize the accepting probability, we solve $1 - p \cdot (2k-3)/(2k-2) = p$, which gives $p = 1/2 + 1/(8k-10)$.

Reversibility of this automaton is clear by its construction. □

Corollary 4 *For each $k \geq 2$, there exists a 1Q1CA $M^{(Q)}_{L^{(k)}_{m_1=\cdots=m_k}}$ for $L^{(k)}_{m_1=\cdots=m_k}$ with probability $1/2 + 1/(8k-10)$.*

4 Improving the Accepting Probability of 1Q1CA for $L^{(k)}_{m_1=\cdots=m_k}$

In the previous subsection, we showed that $L^{(k)}_{m_1=\cdots=m_k} = \{a_1^{m_1} \cdots a_k^{m_k} \mid m_1 = \cdots = m_k\}$ is recognizable by a bounded error 1PR1CA. In this section, we also show that, in a quantum case, we can improve the accepting probability in a strict sense by using quantum interference. We utilize the following result.

Theorem 5 (Ambainis et. al. [1]) *$L^{(k)}_{\text{ordered}} = \{a_1^* \cdots a_k^*\}$ can be recognized by a 1QFA $M^{(1QFA)}_{L^{(k)}_{\text{ordered}}}$ with probability p, where p is the root of $p^{(k+1)/(k-1)} + p = 1$ in the interval of $(1/2, 1)$.*

By using $M^{(1QFA)}_{L^{(k)}_{\text{ordered}}}$, we prove the existence of a 1Q1CA which recognizes $L^{(k)}_{\text{ordered}}$. The following two lemmas can be shown easily.

Lemma 5 *For each $k \geq 3$, if $p^{(k+1)/(k-1)} + p = 1$, then $1/2 < p < 2/3$.*

Lemma 6 *For arbitrary $m \times m$ unitary matrices U_1, U_2, there exists an 2×2 block unitary matrix $N(U_1, U_2)$ such that*

$$N(U_1, U_2) = \frac{1}{\sqrt{2}} \underbrace{\begin{pmatrix} U_1 & * \\ U_2 & * \end{pmatrix}}_{\text{2blocks}},$$

where the blocks indicated by $*$ are determined to hold unitary of N.

Now, we prove the main theorem.

Theorem 6 *For each $k \geq 2$, $L^{(k)}_{m_1=\cdots=m_k}$ can be recognized by a 1Q1CA with probability p, where p is the root of $p^{(k+1)/(k-1)} + p = 1$ in the interval of $(1/2, 1)$.*

Proof: By using $M^{(1QFA)}_{L^{(k)}_{\mathrm{ordered}}}$, we can construct a 1Q1CA $M = (Q, \Sigma, \delta, q_1^1, Q_{\mathrm{acc}}, Q_{\mathrm{rej}})$ as follows. Let $Q = \{q_i^m \mid 1 \le i \le 3k, m = 1,2\}$, $\Sigma = \{a_i \mid 1 \le i \le k\}$, $Q_{\mathrm{acc}} = \{q_{2k}^m \mid m = 1,2\}$, and $Q_{\mathrm{rej}} = \{q_i^m \mid k+1 \le i \le 2k-1, 2k+1 \le 3k, m = 1,2\}$. For each $\sigma \in \Gamma$, we define the transition matrices $\{W_{\sigma,s}\}$ and the counter function D as follows:

$$W_{\mathfrak{c},0} = N\left(\begin{pmatrix} V_{\mathfrak{c}} & O \\ O & I_k \end{pmatrix}, \begin{pmatrix} V_{\mathfrak{c}} & O \\ O & I_k \end{pmatrix}\right), \text{ for } k \ge 3, \qquad W_{\mathfrak{c},0} = \begin{pmatrix} V_{\mathfrak{c}} & O \\ O & I_k \end{pmatrix} \oplus \begin{pmatrix} I_k & O \\ O & I_k \end{pmatrix}, \text{ for } k = 2,$$

$$W_{a_{2i-1},0} = \begin{pmatrix} V_{a_{2i-1}} & O \\ O & I_k \end{pmatrix} \oplus \begin{pmatrix} V_{a_{2i-1}} & O \\ O & I_k \end{pmatrix}, \qquad W_{a_{2i-1},1} = \begin{pmatrix} O & I_{2k} \\ I_k & O \end{pmatrix} \oplus \begin{pmatrix} V_{a_{2i-1}} & O \\ O & I_k \end{pmatrix},$$

$$W_{a_{2i},0} = \begin{pmatrix} V_{a_{2i}} & O \\ O & I_k \end{pmatrix} \oplus \begin{pmatrix} V_{a_{2i}} & O \\ O & I_k \end{pmatrix}, \qquad W_{a_{2i},1} = \begin{pmatrix} V_{a_{2i}} & O \\ O & I_k \end{pmatrix} \oplus \begin{pmatrix} O & I_{2k} \\ I_k & O \end{pmatrix},$$

$$W_{\$,0} = \begin{pmatrix} V_{\$} & O \\ O & I_k \end{pmatrix} \oplus \begin{pmatrix} V_{\$} & O \\ O & I_k \end{pmatrix}, \qquad W_{\$,1} = \begin{pmatrix} O & I_{2k} \\ I_k & O \end{pmatrix} \oplus \begin{pmatrix} O & I_{2k} \\ I_k & O \end{pmatrix},$$

$$\begin{aligned}
D(q_j^1, a_{2i-1}) &= +1, \text{ for } 1 \le j \le k, 1 \le i \le \lfloor k/2 \rfloor, \\
D(q_j^1, a_{2i}) &= -1, \text{ for } 1 \le j \le k, 1 \le i \le \lfloor k/2 \rfloor, \\
D(q_j^1, a_k) &= 0, \text{ for } 1 \le j \le k, k \text{ is odd}, \\
D(q_j^2, a_1) &= 0, \text{ for } 1 \le j \le k, \\
D(q_j^2, a_{2i}) &= +1, \text{ for } 1 \le j \le k, 1 \le i \le \lfloor (k-1)/2 \rfloor, \\
D(q_j^2, a_{2i+1}) &= -1, \text{ for } 1 \le j \le k, 1 \le i \le \lfloor (k-1)/2 \rfloor, \\
D(q_j^2, a_k) &= 0, \text{ for } 1 \le j \le k, k \text{ is even},
\end{aligned}$$

where each V_σ is the transition matrix of $M^{(1QFA)}_{L^{(k)}_{\mathrm{ordered}}}$ and the columns of the transition matrices correspond to the states in order of $q_1^1, q_2^1, \ldots, q_k^1, q_1^2, q_2^2, \ldots, q_k^2$ (i.e. the order of the basis states is $q_1^1, q_2^1, \ldots, q_k^1, q_1^2, q_2^2, \ldots, q_k^2$). Let δ be defined in the manner described in Section 2.

If the input string is of the form $a_1^n a_2^n \ldots a_k^n$, in each of two paths, the input is accepted. Thus, the probability of accepting is $(p/2) \cdot 2 = p$.

If $k = 2$, the input string is of the form $a_1^{m_1} a_2^{m_2}$, and $m_1 \ne m_2$, in the first path, the input string is rejected and the states in the second path are never entered. Thus, the input is always rejected.

If $k \ge 3$, the input string is of the form $a_1^{m_1} a_2^{m_2} \ldots a_k^{m_k}$, and there exists at least one pair of (i,j) such that $m_i \ne m_j$, in at least one of two paths, the counter value is not 0 upon reading the right end-marker. Thus, the probability of accepting is at most $(p/2) \cdot 1 = p/2$. By Lemma 5, the probability of rejecting is at least $1 - p/2 > 1 - (2/3) \cdot (1/2) = 2/3 > p$.

Finally, if the input string is not of the form $a_1^* a_2^* \ldots a_k^*$, in each of two paths, the input string is rejected with probability at least p, since each path is equivalent to $M^{(1QFA)}_{L^{(k)}_{\mathrm{ordered}}}$ when the counter is left out of consideration. Therefore, the probability of rejecting is at least p. □

Proposition 1 *The accepting probability p of M is greater than $1/2 + 1/(8k-10)$, the accepting probability of $M^{(Q)}_{L^{(k)}_{m_1=\cdots=m_k}}$.*

Proof: Omitted. □

5 Relation between 1D1CAs and 1Q1CAs

As we have seen in Section 3, 4, and 5, some non-context-free languages can be recognized by bounded error 1Q1CAs. It is clear that 1D1CAs cannot recognize any non-context-free languages, since 1D1CAs are special cases of 1-way pushdown automata. 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 7 *The language $\{\{a,b\}^*a\}$ cannot be recognized by a 1Q1CA with bounded error.*

Proof: Nayak [7] showed that, for each fixed $n \geq 0$, any general 1-way QFA recognizing $\{wa \mid w \in \{a,b\}^*, |w| \leq n\}$ must have $2^{\Omega(n)}$ basis states. Thus a 1Q1CA for $\{\{a,b\}^*a\}$ should have at least $2^{\Omega(n)}$ quantum basis states if the input length is n. However, the number of basis states of a 1Q1CA for a language of length n has precisely $(2n+1)|Q|$. Since $(2n+1)|Q| < 2^{\Omega(n)}$ for sufficiently large n, it proves the theorem. □

6 Conclusions and Open Problems

In this paper, we proved that there are non-context-free languages which can be recognized by 1PR1CAs and 1Q1CAs, but cannot be recognized by 1D1CAs. We also showed that there is a regular language which can be recognized by a 1D1CA, but cannot be recognized by a 1Q1CA.

One interesting question is what languages are recognizable by 1Q1CAs but not by 1PR1CAs. Similarly, what are the languages recognizable by 1Q1CAs but not by 1P1CAs?

Another question is concerning to a 2-counter case. It is known that a 2-way deterministic 2-counter automaton can simulate a deterministic Turing machine [5]. How about the power of 2-way quantum 2-counter automata, or 2-way quantum 1-counter automata?

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] M. L. Minsky. Recursive unsolvability of post's problem of 'tag' and other topics in the theory of turing machines. *Annals of Math.*, Vol. 74:3, pp. 437–455, 1961.

[6] C. Moore and J. Crutchfield. Quantum automata and quantum grammars. Technical Report 97-07-02, Santa-Fe Institute Working Paper, 1997. Also available at `http://xxx.lanl.gov/archive/quant-ph/9707031`.

[7] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundation of Computer Science*, pp. 369–376, 1999.

[8] 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.