

# On the State Complexity of Semi-quantum Finite Automata<sup>\*</sup>

Shenggen Zheng<sup>1</sup>, Jozef Gruska<sup>1</sup>, and Daowen Qiu<sup>2</sup>

<sup>1</sup> Faculty of Informatics, Masaryk University, Brno, 602 00, Czech Republic  
zhengshenggen@gmail.com, gruska@fi.muni.cz

<sup>2</sup> Department of Computer Science, Sun Yat-sen University,  
Guangzhou 510006, China  
issqdw@mail.sysu.edu.cn

**Abstract.** Some of the most interesting and important results concerning quantum finite automata are those showing that they can recognize certain languages with (much) less resources than corresponding classical finite automata. This paper shows three results of such a type that are stronger in some sense than other ones because (a) they deal with models of quantum finite automata with very little quantumness (so-called semi-quantum one- and two-way finite automata); (b) differences, even comparing with probabilistic classical automata, are bigger than expected; (c) a trade-off between the number of classical and quantum basis states needed is demonstrated in one case and (d) languages (or the promise problem) used to show main results are very simple and often explored ones in automata theory or in communication complexity, with seemingly little structure that could be utilized.

## 1 Introduction

An important way to get deeper insights into the power of various quantum resources and operations is to explore the power of various quantum variations of the basic models of classical automata. Of a special interest is to do that for various quantum variations of the classical finite automata, especially for those that use limited amounts of quantum resources: states, correlations, operations and measurements. This paper aims to contribute to such a line of research.

There are several approaches how to introduce quantum features to classical models of finite automata. Two of them will be dealt with in this paper. The first one is to consider quantum variants of the classical *one-way (deterministic) finite automata* (1FA or 1DFA) and the second one is to consider quantum variants of the classical *two-way finite automata* (2FA or 2DFA). Already the

---

<sup>\*</sup> Work of the first and second authors was supported by the Employment of Newly Graduated Doctors of Science for Scientific Excellence project/grant (CZ.1.07./2.3.00/30.0009) of Czech Republic. Work of third author was supported by the National Natural Science Foundation of China (Nos. 61272058, 61073054).

very first attempts to introduce such models, by Moore and Crutchfields [18] as well as Kondacs and Watrous [14] demonstrated that in spite of the fact that in the classical case, 1FA and 2FA have the same recognition power, this is not so for their quantum variations (in case only unitary operations and projective measurements are considered as quantum operations). Moreover, already the first model of *two-way quantum finite automata* (2QFA), namely that introduced by Kondacs and Watrous, demonstrated that quantum variants of 2FA are much too powerful – they can recognize even some *non-context free languages* and are actually not really finite in a strong sense [14]. Therefore it started to be of interest to introduce and explore some “less quantum” variations of 2FA and their power [2, 3].

A “hybrid” – quantum/classical – variations of 2FA, namely, *two-way finite automata with quantum and classical states* (2QCFA), were introduced by Ambainis and Watrous [2]. For this model they showed, in an elegant way, that already an addition of a single qubit to the classical model can much increase its power. A 2QCFA is essentially a classical 2FA augmented with a quantum memory of constant size (for states of a fixed Hilbert space) that does not depend on the size of the (classical) input. In spite of such a restriction, 2QCFA have been shown to be even more powerful than *two-way probabilistic finite automata* (2PFA) [2, 26]. A one-way version of 2QCFA was studied in [25], namely *one-way finite automata with quantum and classical states* (1QCFA).

Number of states is a natural complexity measure for finite automata. In case of quantum finite automata by that we understand the number of the basis states of the quantum space – that is its dimension. In case of hybrid, that is quantum/classical, finite automata, it is natural to consider both complexity measures – number of classical and also number of quantum (basis) states – and, potentially, trade-offs between them.

State complexity is one of the important research fields of computer science and it has many applications, e.g., in natural language and speech processing, image generation and encoding, etc. Early in 1959, Rabin and Scott [21] proved that any  $n$ -state *one-way nondeterministic finite automaton* (1NFA) can be simulated by a  $2^n$ -state *one-way deterministic finite automaton* (1DFA). Salomaa [23] began to explore state complexity of finite automata in 1960s. The number of states of finite automata used in applications were usually small at that time and therefore investigations of state complexity of finite automata was seen mainly as a purely theoretical problem. However, the numbers of states of finite automata in applications can be huge nowadays, even millions of states in some cases [12]. It becomes therefore also practically important to explore state complexity of finite automata. State complexity of several variants of finite automata, both one-way and two-way, were deeply and broadly studied in the past thirty years [1–5, 8, 9, 16, 17, 24–26].

In this paper we explore the state complexity of semi-quantum finite automata and their space-efficiency comparing to the corresponding classical counterparts. We do that by showing that even for several very simple, and often considered,

languages or promise problems, a little of quantumness can much decrease the state complexity of the corresponding semi-quantum finite automata. The first of these problems will be one of the very basic problem that is explored in communication complexity. Namely, the promise version of strings equality problem [7].

We use a promise problem to model the promise version of strings equality problem. For the alphabet  $\Sigma = \{0, 1, \#\}$  and  $n \in \mathbf{Z}^+$ , let us consider the promise problem  $A_{EQ}(n) = (A_{yes}(n), A_{no}(n))$ , where  $A_{yes}(n) = \{x\#y \mid x = y, x, y \in \{0, 1\}^n\}$  and  $A_{no}(n) = \{x\#y \mid x \neq y, x, y \in \{0, 1\}^n, H(x, y) = \frac{n}{2}\}$ . ( $H(x, y)$  is the Hamming distance between  $x$  and  $y$ , which is the number of bit positions on which they differ.)

Klauck [13] has proved that, for any language, the state complexity of exact quantum/classical finite automata, which is a general model of one-way quantum finite automata, is not less than the state complexity of 1DFA. Therefore, it is interesting and important to find out whether the result still holds for interesting cases of promise problems or not<sup>1</sup>. Applying the communication complexity result from [7] to finite automata, for any  $n \in \mathbf{Z}^+$ , we prove that there exists a promise problem  $A_{EQ}(n)$  that can be solved exactly by a 1QCFA with  $n$  quantum basis states and  $\mathbf{O}(n)$  classical states, whereas the sizes of the corresponding 1DFA are  $2^{\Omega(n)}$ .

As the next we will consider state complexity of the language  $L(p) = \{a^{kp} \mid k \in \mathbf{Z}^+\}$ . It is well know that, for any  $p \in \mathbf{Z}^+$ , each 1DFA and 1NFA accepting  $L(p)$  has at least  $p$  states. Ambainis and Freivalds [3], proved, using a non-constructive method, that  $L(p)$  can be recognized by a one-way measure-once quantum finite automaton (MO-1QFA) with one-sided error  $\varepsilon$  with  $poly(\frac{1}{\varepsilon}) \cdot \log p$  basis states (where  $poly(x)$  is some polynomial in  $x$ ). This bound was improved to  $\mathbf{O}(\frac{\log p}{\varepsilon^3})$  in [6] and to  $4\frac{\log 2p}{\varepsilon}$  in [4]. That is the best result known for such a mode of acceptance and it is an interesting open problem whether this bound can be much improved. If  $p$  is a prime,  $L(p)$  can not be recognized by any one-way probabilistic finite automaton (1PFA) with less than  $p$  states [3]. For the case that  $p$  is not a prime, Mereghetti et al. [17] showed that the number of states of a 1PFA necessary and sufficient for accepting the language  $L(p)$  with isolated cut point is  $p_1^{\alpha_1} + p_2^{\alpha_2} + \dots + p_s^{\alpha_s}$ , where  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$  is the prime factorization of  $p$ . Mereghetti et al. [17] also proved that  $L(p)$  can be recognized by a 2 basis states MO-1QFA with isolated cut point. However, this mode of acceptance often leads to quite different state complexity outcome than one-sided error and error probability acceptance modes.

Concerning two-way finite automata, for any prime  $p$ ,  $p$  states are necessary and sufficient for accepting  $L(p)$  on *two-way deterministic finite automata* (2DFA) and *two-way nondeterministic finite automata* (2NFA) [16]. For the case that  $p$  is not prime, the number of states necessary and sufficient for accepting  $L(p)$  on 2DFA and 2NFA is  $p_1^{\alpha_1} + p_2^{\alpha_2} + \dots + p_s^{\alpha_s}$  [16], where  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$  is the prime factorization of  $p$ . Yakaryilmaz and Cem Say [24] showed that there exists

---

<sup>1</sup> Ambainis and Yakaryilmaz showed in [5] that there is a very special case in which the superiority of quantum computation to classical one cannot be bounded.

a 7-state *one-way finite automaton with restart* (1QFAR) which accepts  $L(p)$  with one-sided error  $\varepsilon$  and expected running time  $\mathbf{O}(\frac{1}{\varepsilon} \sin^{-2}(\frac{\pi}{p})|w|)$ , where  $|w|$  is the length of input  $w$ . For any  $n$ -state 1QFAR  $\mathcal{M}_1$  with expected running time  $t(|w|)$ , Yakaryilmaz and Cem Say [24] also proved that there exists a 2QCFA  $\mathcal{M}_2$  with  $n$  quantum basis states,  $\mathbf{O}(n)$  classical states, and with expected runtime  $\mathbf{O}(t(|w|))$ , such that  $\mathcal{M}_2$  accepts every input string  $w$  with the same probability as  $\mathcal{M}_1$  does. Therefore,  $L(p)$  can be recognized with one-sided error  $\varepsilon$  by a 2QCFA with 7 quantum basis states and a constant number of classical states.

In this paper we prove that the language  $L(p)$  can be recognized with one-sided error  $\varepsilon$  in a linear expected running time  $\mathbf{O}(\frac{1}{\varepsilon} p^2 |w|)$  by a 2QCFA  $\mathcal{A}(p, \varepsilon)$  with 2 quantum basis states and a constant number of classical states. We also show that the number of states needed for accepting  $L(p)$  on a polynomial time 2PFA is at least  $\sqrt[3]{(\log p)/b}$ , where  $b$  is a constant.

The problem of checking whether the length of input string is equal to a given constant  $m \in \mathbf{Z}^+$ , is extensively studied in literatures as well. For any  $m \in \mathbf{Z}^+$  and any finite alphabet  $\Sigma$ , it is obvious that the number of states of a 1DFA for accepting the language  $C(m) = \{w \mid w \in \Sigma^m\}$  is at least  $m$ . Freivalds [9] showed that there is an  $\varepsilon$  error probability 1PFA accepting  $C(m)$  with  $\mathbf{O}(\log^2 m)$  states. Ambainis and Freivalds [3] proved that  $C(m)$  can be recognized by an MO-1QFA with  $\mathbf{O}(\log m)$  quantum basis states. Yakaryilmaz and Cem Say [24] showed that there exists a 7-state 1QFAR  $\mathcal{M}$  which accepts  $C(m)$  with one-sided error  $\varepsilon$  and the expected running time  $\mathbf{O}((\frac{1}{\varepsilon})^m |w|)$ . Thus, for  $w \in C(m)$ , the expected running time of  $\mathcal{M}$  is an exponential of  $m$ . The 1QFAR  $\mathcal{M}$  can only work efficiently on a very small  $m$ .

In this paper we prove that the language  $C(m)$  can be recognized with one-sided error  $\varepsilon$  in a polynomial expected running time  $\mathbf{O}(\frac{1}{\varepsilon} m^2 |w|^4)$  by a 2QCFA  $\mathcal{A}(m, \varepsilon)$  with 2 quantum basis states and a constant number of classical states. The expected running time is a polynomial of  $m$ . We show also that the number of states needed for accepting  $C(m)$  on a polynomial 2PFA is at least  $\sqrt[3]{(\log m)/b}$ , where  $b$  is a constant.

Since 1QCFA and 2QCFA have both quantum and classical states, it is interesting to ask when there is some trade-off between these two kinds of states. We prove such a trade-off property for the case a 1QCFA accepts the language  $L(p)$ . Namely, it holds that for any integer  $p$  with prime factorization  $p = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$  ( $s > 1$ ), for any partition  $I_1, I_2$  of  $\{1, \dots, s\}$ , and for  $q_1 = \prod_{i \in I_1} p_i^{\alpha_i}$  and  $q_2 = \prod_{i \in I_2} p_i^{\alpha_i}$ , the language  $L(p)$  can be recognized with a one-sided error  $\varepsilon$  by a 1QCFA  $\mathcal{A}(q_1, q_2, \varepsilon)$  with  $\mathbf{O}(\log q_1) = \mathbf{O}(\sum_{i \in I_1} \alpha_i \log p_i)$  quantum basis states and  $\mathbf{O}(q_2) = \mathbf{O}(\prod_{i \in I_2} p_i^{\alpha_i})$  classical states.

The paper is structured as follows. In Section 2 Semi-quantum finite automata models involved are described in some details. State complexities for the string equality problems will be discussed in Section 3. State succinctness for two families of regular languages is explored in Section 4. A trade-off property for 1QCFA is demonstrated in Section 5.

## 2 Models

We introduce in this section the models of 1QCFA and 2QCFA. Concerning some basic concepts and also notations on quantum information processing for this paper we refer the reader to Section 2.1 in [27]. Concerning more on quantum information processing we refer the reader to [22], and concerning more on classical and quantum automata [10, 11, 19].

2QCFA were introduced by Ambainis and Watrous [2] and explored also by Yakaryilmaz, Qiu, Zheng and others [24–26]. Informally, a 2QCFA can be seen as a 2DFA with an access to a quantum memory for states of a fixed Hilbert space upon which at each step either a unitary operation is performed or a projective measurement and the outcomes of which then probabilistically determine the next move of the underlying 2DFA.

**Definition 1.** *A 2QCFA  $\mathcal{A}$  is specified by a 9-tuple*

$$\mathcal{A} = (Q, S, \Sigma, \Theta, \delta, |q_0\rangle, s_0, S_{acc}, S_{rej}) \tag{1}$$

where:

1.  $Q$  is a finite set of orthonormal quantum basis states.
2.  $S$  is a finite set of classical states.
3.  $\Sigma$  is a finite alphabet of input symbols and let  $\Sigma' = \Sigma \cup \{\$, \#\}$ , where  $\#$  will be used as the left end-marker and  $\$$  as the right end-marker.
4.  $|q_0\rangle \in Q$  is the initial quantum state.
5.  $s_0$  is the initial classical state.
6.  $S_{acc} \subset S$  and  $S_{rej} \subset S$ , where  $S_{acc} \cap S_{rej} = \emptyset$  are sets of the classical accepting and rejecting states, respectively.
7.  $\Theta$  is a quantum transition function

$$\Theta : S \setminus (S_{acc} \cup S_{rej}) \times \Sigma' \rightarrow U(H(Q)) \cup O(H(Q)), \tag{2}$$

where  $U(H(Q))$  and  $O(H(Q))$  are sets of unitary operations and projective measurements on the Hilbert space generated by quantum states from  $Q$ .

8.  $\delta$  is a classical transition function. If the automaton  $\mathcal{A}$  is in the classical state  $s$ , its tape head is scanning a symbol  $\sigma$  and its quantum memory is in the quantum state  $|\psi\rangle$ , then  $\mathcal{A}$  performs quantum and classical transitions as follows.
  - (a) If  $\Theta(s, \sigma) \in U(H(Q))$ , then the unitary operation  $\Theta(s, \sigma)$  is applied on the current state  $|\psi\rangle$  of quantum memory to produce a new quantum state. The automaton performs, in addition, the following classical transition function

$$\delta : S \setminus (S_{acc} \cup S_{rej}) \times \Sigma' \rightarrow S \times \{-1, 0, 1\}. \tag{3}$$

If  $\delta(s, \sigma) = (s', d)$ , then the new classical state of the automaton is  $s'$  and its head moves in the direction  $d$ .

(b) If  $\Theta(s, \sigma) \in O(H(Q))$ , then the measurement operation  $\Theta(s, \sigma)$  is applied on the current state  $|\psi\rangle$ . Suppose the measurement  $\Theta(s, \sigma)$  is specified by operators  $\{P_1, \dots, P_n\}$  and its corresponding classical outcome is from the set  $N_{\Theta(s, \sigma)} = \{1, 2, \dots, n\}$ . The classical transition function  $\delta$  can be then specified as follow

$$\delta : S \setminus (S_{acc} \cup S_{rej}) \times \Sigma' \times N_{\Theta(s, \sigma)} \rightarrow S \times \{-1, 0, 1\}. \tag{4}$$

In such a case, if  $i$  is the classical outcome of the measurement, then the current quantum state  $|\psi\rangle$  is changed to the state  $P_i|\psi\rangle/\|P_i|\psi\rangle\|$ . Moreover, if  $\delta(s, \sigma)(i) = (s', d)$ , then the new classical state of the automaton is  $s'$  and its head moves in the direction  $d$ .

The automaton halts and accepts (rejects) the input when it enters a classical accepting (rejecting) state (from  $S_{acc}(S_{rej})$ ).

The computation of a 2QCFA  $\mathcal{A} = (Q, S, \Sigma, \Theta, \delta, |q_0\rangle, s_0, S_{acc}, S_{rej})$  on an input  $w \in \Sigma^*$  starts with the string  $\$x\$$  on the input tape. At the start, the tape head of the automation is positioned on the left end-marker and the automaton begins the computation in the classical initial state and in the initial quantum state. After that, in each step, if its classical state is  $s$ , its tape head reads a symbol  $\sigma$  and its quantum state is  $|\psi\rangle$ , then the automaton changes its states and makes its head movement following the steps described in the definition.

The computation will end whenever the resulting classical state is in  $S_{acc} \cup S_{rej}$ . Therefore, similarly to the definition of accepting and rejecting probabilities for 2QFA [14], the accepting and rejecting probabilities  $Pr[\mathcal{A} \text{ accepts } w]$  and  $Pr[\mathcal{A} \text{ rejects } w]$  for an input  $w$  are, respectively, the sums of all accepting probabilities and all rejecting probabilities before the end of computation on the input  $w$ .

*Remark 2.* 1QCFA are one-way versions of 2QCFA [25]. In this paper, we only use 1QCFA in which a unitary transformation is applied in every step after scanning a symbol and an measurement is performed after scanning the right end-marker. Such model is an measure-once 1QCFA and corresponds to a variant of MO-1QFA.

Three basic modes of language acceptance to be considered here are the following ones: Let  $L \subset \Sigma^*$  and  $0 < \varepsilon < \frac{1}{2}$ . A finite automaton  $\mathcal{A}$  recognizes  $L$  with a *one-sided error* (an *error probability*)  $\varepsilon$  if, for  $w \in \Sigma^*$ , (1)  $\forall w \in L, Pr[\mathcal{A} \text{ accepts } w] = 1 (\geq 1 - \varepsilon)$  and (2)  $\forall w \notin L, Pr[\mathcal{A} \text{ rejects } w] \geq 1 - \varepsilon$ .

Obviously, one-sided error acceptance is stricter than an error probability acceptance.

Language acceptance is a special case of so called promise problem solving. A *promise problem* is a pair  $A = (A_{yes}, A_{no})$ , where  $A_{yes}, A_{no} \subset \Sigma^*$  are disjoint sets. Languages may be viewed as promise problems that obey the additional constraint  $A_{yes} \cup A_{no} = \Sigma^*$ .

A promise problem  $A = (A_{yes}, A_{no})$  is solved by exactly by a 1QCFA  $\mathcal{A}$  if (1)  $\forall w \in A_{yes}, Pr[\mathcal{A} \text{ accepts } w] = 1$  and (2)  $\forall w \in A_{no}, Pr[\mathcal{A} \text{ rejects } w] = 1$ .

### 3 State Succinctness for Promise Problem $A_{EQ}(n)$

**Theorem 3.** *The promise problem  $A_{EQ}(n)$  can be solved exactly by a 1QCFA  $\mathcal{A}(n)$  with  $n$  quantum basis states and  $\mathbf{O}(n)$  classical states, whereas the sizes of the corresponding 1DFA are  $2^{\Omega(n)}$ .*

**A1:** Description of the behavior of  $\mathcal{A}(n)$  when solving the promise problem  $A_{EQ}(n)$ .

1. Read the left end-marker  $\dagger$ , perform  $U_s$  on the initial quantum state  $|1\rangle$ , change its classical state to  $\delta(s_0, \dagger) = s_1$ , and move the tape head one cell to the right.
2. Until the currently scanned symbol  $\sigma$  is not  $\#$ , do the following:
  - 2.1 Apply  $\Theta(s_i, \sigma) = U_{i,\sigma}$  to the current quantum state.
  - 2.2 Change the classical state  $s_i$  to  $s_{i+1}$  and move the tape head one cell to the right.
3. Change the classical state  $s_{n+1}$  to  $s_1$  and move the tape head one cell to the right.
4. While the currently scanned symbol  $\sigma$  is not the right end-marker  $\$, do the following:
 
  - 2.1 Apply  $\Theta(s_i, \sigma) = U_{i,\sigma}$  to the current quantum state.
  - 2.2 Change the classical state  $s_i$  to  $s_{i+1}$  and move the tape head one cell to the right.$
5. When the right end-marker is reached, perform  $U_f$  on the current quantum state, measure the current quantum state with  $M = \{P_i = |i\rangle\langle i|\}_{i=1}^n$ . If the outcome is  $|1\rangle$ , accept the input; otherwise reject the input.

*Proof.* Let  $x = x_1 \cdots x_n$  and  $y = y_1 \cdots y_n$  with  $x, y \in \{0, 1\}^n$ . Let us consider an MO-1QCFA  $\mathcal{A}(n)$  with  $n$  quantum basis states  $\{|i\rangle : i = 1, 2, \dots, n\}$ .  $\mathcal{A}(n)$  will start in the quantum state  $|1\rangle = (1, 0, \dots, 0)^T$ . We use classical states  $s_i \in S$  ( $1 \leq i \leq n+1$ ) to point out the positions of the tape head that will provide some information for quantum transformations. If the classical state of  $\mathcal{A}(n)$  will be  $s_i$  ( $1 \leq i \leq n$ ) that will mean that the next scanned symbol of the tape head is the  $i$ -th symbol of  $x(y)$  and  $s_{n+1}$  means that the next scanned symbol of the tape head is  $\#(\$)$ . The automaton proceeds as Algorithm **A1**, where

$$U_s|1\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle; \tag{5}$$

$$U_{i,\sigma}|i\rangle = (-1)^\sigma |i\rangle \quad \text{and} \quad U_{i,\sigma}|j\rangle = |j\rangle \quad \text{for } j \neq i; \tag{6}$$

$$U_f\left(\sum_{i=1}^n \alpha_i |i\rangle\right) = \left(\frac{1}{\sqrt{n}} \sum_{i=1}^n \alpha_i\right) |1\rangle + \dots \tag{7}$$

Transformations  $U_s$  and  $U_f$  are unitary, where the first column of  $U_s$  is  $\frac{1}{\sqrt{n}}(1, \dots, 1)^T$  and the first row of  $U_f$  is  $\frac{1}{\sqrt{n}}(1, \dots, 1)$ .

The quantum state after scanning the left end-marker is  $|\psi_1\rangle = U_s|1\rangle = \sum_{i=1}^n \frac{1}{\sqrt{n}} |i\rangle$ , the quantum state after Step 2 is  $|\psi_2\rangle = \sum_{i=1}^n \frac{1}{\sqrt{n}} (-1)^{x_i} |i\rangle$ , and

the quantum state after Step 4 is  $|\psi_3\rangle = \sum_{i=1}^n \frac{1}{\sqrt{n}}(-1)^{x_i+y_i}|i\rangle$ . The quantum state after scanning the right end-marker is therefore

$$|\psi_4\rangle = U_f \left( \sum_{i=1}^n \frac{1}{\sqrt{n}}(-1)^{x_i+y_i}|i\rangle \right) = U_f \frac{1}{\sqrt{n}} \begin{pmatrix} (-1)^{x_1+y_1} \\ (-1)^{x_2+y_2} \\ \vdots \\ (-1)^{x_n+y_n} \end{pmatrix} \tag{8}$$

$$= \begin{pmatrix} \frac{1}{n} \sum_{i=1}^n (-1)^{x_i+y_i} \\ \vdots \\ \vdots \end{pmatrix}. \tag{9}$$

If the input string  $w \in A_{yes}(n)$ , then  $x_i = y_i$  for any  $i$  and  $|\frac{1}{n} \sum_{i=1}^n (-1)^{x_i+y_i}|^2 = 1$ . The amplitude of  $|1\rangle$  is 1, and that means  $|\psi_4\rangle = |1\rangle$ . Therefore the input will be accepted with probability 1 at the measurement in Step 5.

If the input string  $w \in A_{no}(n)$ , then  $H(x, y) = \frac{n}{2}$ . Therefore the probability of getting outcome  $|1\rangle$  in the measurement in Step 5 is  $|\frac{1}{n} \sum_{i=1}^n (-1)^{x_i+y_i}|^2 = 0$ .

The deterministic communication complexity for the promise version of equality problem is at least  $0.007n$  [7]. Therefore, the sizes of the corresponding 1DFA are  $2^{\Omega(n)}$  [15].

## 4 State Succinctness for 2QCFA

State succinctness for 2QCFA was explored by Yakaryilmaz, Zheng and others [24, 26]. In [26], Zheng et al. showed the state succinctness for polynomial time 2QCFA for families of promise problems and for exponential time 2QCFA for a family of languages. In this section, we show the state succinctness for linear time 2QCFA and polynomial time 2QCFA for two families of languages.

### 4.1 State Succinctness for the Language $L(p)$

**Theorem 4.** *For any  $p \in \mathbb{Z}^+$  and  $0 < \varepsilon \leq \frac{1}{2}$ , the language  $L(p)$  can be recognized with one-sided error  $\varepsilon$  by a 2QCFA  $\mathcal{A}(p, \varepsilon)$  with 2 quantum basis states and a constant number of classical states (not depending on  $p$ ) in a linear expected running time  $\mathcal{O}(\frac{1}{\varepsilon}p^2n)$ , where  $n$  is the length of input.*

*Proof.* The main idea of the proof is as follows: Consider a 2QCFA  $\mathcal{A}(p, \varepsilon)$  with 2 orthogonal quantum basis states  $|q_0\rangle$  and  $|q_1\rangle$ .  $\mathcal{A}(p, \varepsilon)$  starts computation in the initial quantum state  $|q_0\rangle$  and with the tape head on the left end-marker. Every time when  $\mathcal{A}(p, \varepsilon)$  reads a symbol ‘a’, the current quantum state is rotated by the angle  $\frac{\pi}{p}$ . When the right end-marker \$ is reached,  $\mathcal{A}(p, \varepsilon)$  measures the



**A2:** Description of the behavior of  $\mathcal{A}(p, \varepsilon)$  when recognizing the language  $L(p)$ . Repeat the following ad infinity:

1. Move the tape head to the right of the left end-marker.
2. Until the scanned symbol is the right end-marker, apply  $U_p$  to the current quantum state and move the head one cell to the right.
- 3 Measure the current quantum state in the basis  $\{|q_0\rangle, |q_1\rangle\}$ .
  - 3.1 If quantum outcome is  $|q_1\rangle$ , reject the input.
  - 3.2 Otherwise apply  $U_{p,\varepsilon}$  to the current quantum state  $|q_0\rangle$ .
- 4 Measure the quantum state in the basis  $\{|q_0\rangle, |q_1\rangle\}$ . If the result is  $|q_0\rangle$ , accept the input; otherwise apply a unitary operation to change the quantum state from  $|q_1\rangle$  to  $|q_0\rangle$  and start a new iteration.

current quantum state. If the resulting quantum state is  $|q_1\rangle$ , the input string is rejected, otherwise the automaton proceeds as Algorithm **A2**, where

$$U_p = \begin{pmatrix} \cos \frac{\pi}{p} & -\sin \frac{\pi}{p} \\ \sin \frac{\pi}{p} & \cos \frac{\pi}{p} \end{pmatrix} \quad \text{and} \quad U_{p,\varepsilon} = \begin{pmatrix} \frac{1}{\sqrt{p^2/4\varepsilon}} & -\frac{\sqrt{p^2/4\varepsilon-1}}{\sqrt{p^2/4\varepsilon}} \\ \frac{\sqrt{p^2/4\varepsilon-1}}{\sqrt{p^2/4\varepsilon}} & \frac{1}{\sqrt{p^2/4\varepsilon}} \end{pmatrix}. \quad (10)$$

See Section 4.1 in [27] for a detail proof. (Similar unitary matrixes of  $U_p$  and proof methods can be found in[3, 4, 17, 24].)

**Theorem 5.** *For any integer  $p$ , any polynomial expected running time 2PFA recognizing  $L(p)$  with error probability  $\varepsilon < \frac{1}{2}$  has at least  $\sqrt[3]{(\log p)/b}$  states, where  $b$  is a constant.*

In order to prove this theorem, we need

**Lemma 6 ([8]).** *For every  $\varepsilon < 1/2$ ,  $a > 0$  and  $d > 0$ , there exists a constant  $b > 0$  such that, for any integer  $c$ , if a language  $L$  is recognized with an error probability  $\varepsilon$  by a  $c$ -state 2PFA within time  $an^d$ , where  $n = |w|$  is the length of input, then  $L$  is recognized by some DFA with at most  $c^{bc^2}$  states.*

*Proof.* Assume that a  $c$ -state 2PFA  $\mathcal{A}(p)$  recognizes  $L(p)$  with an error probability  $\varepsilon < 1/2$  and also within a polynomial expected running time. According to Lemma 6, there exists a 1DFA that recognizes  $L(p)$  with  $c^{bc^2}$  states, where  $b > 0$  is a constant. As we know, any DFA recognizing  $L(p)$  has at least  $p$  states. Therefore,

$$c^{bc^2} \geq p \Rightarrow bc^2 \log c \geq \log p \Rightarrow c^3 > (\log p)/b \Rightarrow c > \sqrt[3]{(\log p)/b}. \quad (11)$$

### 4.2 State Succinctness for the Language $C(m)$

**Theorem 7.** *For any  $m \in \mathbf{Z}^+$  and  $0 < \varepsilon \leq \frac{1}{2}$ , the language  $C(m)$  can be recognized with one-sided error  $\varepsilon$  by a 2QCFA  $\mathcal{A}(m, \varepsilon)$  with 2 quantum basis states and a constant number of classical states (not depending on  $m$ ) in a polynomial expected running time  $\mathbf{O}(\frac{1}{\varepsilon}m^2n^4)$ , where  $n$  is the length of input.*

**A3:** Description of the behavior of  $\mathcal{A}(m, \varepsilon)$  when recognizing the language  $C(m)$ . Repeat the following ad infinity:

1. Move the tape head to the left end-marker, read the end-marker  $\dagger$ , apply  $U_{\dagger}$  on  $|q_0\rangle$ , and move the tape head one cell to the right.
2. Until the scanned symbol is the right end-marker, apply  $U_{\alpha}$  to the current quantum state and move the tape head one cell to the right.
- 3.0 When the right end-marker is reached, measure the quantum state in the basis  $\{|q_0\rangle, |q_1\rangle\}$ .
  - 3.1 If quantum outcome is  $|q_1\rangle$ , reject the input.
  - 3.2 Otherwise repeat the following subroutine two times:
    - 3.2.1 Move the tape head to the first symbol right to the left end-marker.
    - 3.2.2 Until the currently read symbol is one of the end-markers simulate a coin-flip and move the head right (left) if the outcome of the coin-flip is “head” (“tail”).
4. If the above process ends both times at the right end-marker, apply  $U_{m, \varepsilon}$  to the current quantum state and measure the quantum state in the basis  $\{|q_0\rangle, |q_1\rangle\}$ . If the result is  $|q_0\rangle$ , accept the input; otherwise apply a unitary operation to change the quantum state from  $|q_1\rangle$  to  $|q_0\rangle$  and start a new iteration.

*Proof.* The main idea of the proof is as follows: Consider a 2QCFA  $\mathcal{A}(m, \varepsilon)$  with 2 orthogonal quantum basis states  $|q_0\rangle$  and  $|q_1\rangle$ .  $\mathcal{A}(m, \varepsilon)$  starts computation with the initial quantum state  $|q_0\rangle$ . When  $\mathcal{A}(m, \varepsilon)$  reads the left end-marker  $\dagger$ , the current quantum state will be rotated by the angle  $-\sqrt{2}m\pi$  and every time when  $\mathcal{A}(m, \varepsilon)$  reads a new symbol  $\sigma \in \Sigma$ , the state is rotated by the angle  $\alpha = \sqrt{2}\pi$  (notice that  $\sqrt{2}m\pi = m\alpha$ ). When the right end-marker  $\$$  is reached,  $\mathcal{A}(m, \varepsilon)$  measures the current quantum state with projectors  $\{|q_0\rangle\langle q_0|, |q_1\rangle\langle q_1|\}$ . If the resulting quantum state is  $|q_1\rangle$ , the input string  $w$  is rejected, otherwise, the automaton proceeds as Algorithm **A3**, where

$$U_{\dagger} = \begin{pmatrix} \cos m\sqrt{2}\pi & \sin m\sqrt{2}\pi \\ -\sin m\sqrt{2}\pi & \cos m\sqrt{2}\pi \end{pmatrix}, \quad U_{\alpha} = \begin{pmatrix} \cos \sqrt{2}\pi & -\sin \sqrt{2}\pi \\ \sin \sqrt{2}\pi & \cos \sqrt{2}\pi \end{pmatrix}, \quad (12)$$

$$U_{m, \varepsilon} = \begin{pmatrix} \frac{1}{\sqrt{2m^2/\varepsilon}} & -\frac{\sqrt{2m^2/\varepsilon-1}}{\sqrt{2m^2/\varepsilon}} \\ \frac{\sqrt{2m^2/\varepsilon-1}}{\sqrt{2m^2/\varepsilon}} & \frac{1}{\sqrt{2m^2/\varepsilon}} \end{pmatrix}. \quad (13)$$

See Section 4.2 in [27] for a detail proof. (A similar proof method can be found in [2].)

*Remark 8.* Using the above theorem and the intersection property of languages recognized by 2QCFA [20], it is easy to improve the result from [26] related to the promise problem<sup>2</sup>  $A^{eq}(m)$  to a language  $L^{eq}(m) = \{a^m b^m\} = L^{eq} \cap C(2m)$ , where the language  $L^{eq} = \{a^n b^n \mid n \in \mathbf{N}\}$ . Therefore, the open problem from [26] is solved.

<sup>2</sup> See page 102 in [26].

It is obvious that the number of states of a 1DFA to accept the language  $C(m)$  is at least  $m$ . Using a similar proof as of Theorem 5, we get:

**Theorem 9.** *For any integer  $m$ , any polynomial expected running time 2PFA recognizing  $C(m)$  with error probability  $\varepsilon < \frac{1}{2}$  has at least  $\sqrt[3]{(\log m)/b}$  states, where  $b$  is a constant.*

The sizes of 1PFA and 1QFA recognizing languages  $L(p)$  or  $C(m)$  with an error  $\varepsilon$  depend on the error  $\varepsilon$  in most of the papers. For example, in [4], the size of MO-1QFA accepting  $L(p)$  with one-sided error  $\varepsilon$  is  $4 \frac{\log 2p}{\varepsilon}$ . If  $\varepsilon < \frac{4}{p}$ , the state complexity advantage of MO-1QFA disappears. However, in our model, the sizes of 2QCFA do not depend on the error  $\varepsilon$ , which means that 2QCFA have state advantage for any  $\varepsilon > 0$ .

## 5 A Trade-Off Property of 1QCFA

Quantum resources are expensive and hard to deal with. One can expect to have only very limited number of qubits in current quantum system. In some cases, one cannot expect to have enough qubits to solve a given problem (or to recognize a given language). It is therefore interesting to find out whether there are some trade-off between needed quantum and classical resources. We prove in the following that it is so in some cases. Namely, we prove that there exist trade-offs in case 1QCFA are used to accept the language  $L(p)$ .

**Theorem 10.** *For any integer  $p > 0$  with prime factorization  $p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$  ( $s > 1$ ), for any partition  $I_1, I_2$  of  $\{1, \dots, s\}$ , and for  $q_1 = \prod_{i \in I_1} p_i^{\alpha_i}$  and  $q_2 = \prod_{i \in I_2} p_i^{\alpha_i}$ , the language  $L(p)$  can be recognized with one-sided error  $\varepsilon$  by a 1QCFA  $A(q_1, q_2, \varepsilon)$  with  $\mathbf{O}(\log q_1) = \mathbf{O}(\sum_{i \in I_1} \alpha_i \log p_i)$  quantum basis states and  $\mathbf{O}(q_2) = \mathbf{O}(\prod_{i \in I_2} p_i^{\alpha_i})$  classical states.*

*Proof.* See Section 5 in [27] for a detail proof.

## References

1. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and quantum automata. *Journal of the ACM* 49(4), 496–511 (2002)
2. Ambainis, A., Watrous, J.: Two-way finite automata with quantum and classical states. *Theoretical Computer Science* 287, 299–311 (2002)
3. Ambainis, A., Freivalds, R.: One-way quantum finite automata: strengths, weaknesses and generalizations. In: *Proceedings of the 39th FOCS*, pp. 332–341 (1998)
4. Ambainis, A., Nahimovs, N.: Improved constructions of quantum automata. *Theoretical Computer Science* 410, 1916–1922 (2009)
5. Ambainis, A., Yakaryilmaz, A.: Superiority of exact quantum automata for promise problems. *Information Processing Letters* 112(7), 289–291 (2012)
6. Bertoni, A., Mereghetti, C., Palano, B.: Some formal tools for analyzing quantum automata. *Theoretical Computer Science* 356, 14–25 (2006)
7. Buhrman, H., Cleve, R., Massar, S., de Wolf, R.: Nonlocality and Communication Complexity. *Rev. Mod. Phys.* 82, 665–698 (2010)

8. Dwork, C., Stockmeyer, L.: A time-complexity gap for two-way probabilistic finite state automata. *SIAM J. Comput.* 19, 1011–1023 (1990)
9. Freivalds, R.: On the growth of the number of states in result of determinization of probabilistic finite automata. *Automatic Control and Computer Sciences* 3, 39–42 (1982)
10. Gruska, J.: Descriptive complexity issues in quantum computing. *J. Automata, Languages Combin.* 5(3), 191–218 (2000)
11. Hopcroft, J.E., Ullman, J.D.: *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, New York (1979)
12. Kiraz, G.A.: Compressed Storage of Sparse Finite-State Transducers. In: Boldt, O., Jürgensen, H. (eds.) *WIA 1999. LNCS*, vol. 2214, pp. 109–121. Springer, Heidelberg (2001)
13. Klauck, H.: On quantum and probabilistic communication: Las Vegas and one-way protocols. In: *Proceedings of the 32th STOC*, pp. 644–651 (2000)
14. Kondacs, A., Watrous, J.: On the power of quantum finite state automata. In: *Proceedings of the 38th FOCS*, pp. 66–75 (1997)
15. Kushilevitz, E.: Communication Complexity. *Advances in Computers* 44, 331–360 (1997)
16. Mereghetti, C., Pighizzini, G.: Two-way automata simulations and unary languages. *J. Autom. Lang. Comb.* 5, 287–300 (2000)
17. Mereghetti, C., Palano, B., Pighizzini, G.: Note on the Succinctness of Deterministic, Nondeterministic, Probabilistic and Quantum Finite Automata. *RAIRO-Inf. Theor. Appl.* 35, 477–490 (2001)
18. Moore, C., Crutchfield, J.P.: Quantum automata and quantum grammars. *Theoretical Computer Science* 237, 275–306 (2000)
19. Paz, A.: *Introduction to Probabilistic Automata*. Academic Press, New York (1971)
20. Qiu, D.: Some Observations on Two-Way Finite Automata with Quantum and Classical States. In: Huang, D.-S., Wunsch II, D.C., Levine, D.S., Jo, K.-H. (eds.) *ICIC 2008. LNCS*, vol. 5226, pp. 1–8. Springer, Heidelberg (2008)
21. Rabin, M.O., Scott, D.: Finite automata and their decision problems. *IBM J. Research and Development* 3(2), 115–125 (1959)
22. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
23. Salomaa, A.: On the reducibility of events represented in automata. In: *Annales Academiae Scientiarum Fennicae*, volume Series A of I. *Mathematica* 353 (1964)
24. Yakaryilmaz, A., Cem Say, A.C.: Succinctness of two-way probabilistic and quantum finite automata. *Discrete Mathematics and Theoretical Computer Science* 12(4), 19–40 (2010)
25. Zheng, S.G., Qiu, D.W., Li, L.Z., Gruska, J.: One-way finite automata with quantum and classical states. In: Bordihn, H., Kutrib, M., Truthe, B. (eds.) *Languages Alive. LNCS*, vol. 7300, pp. 273–290. Springer, Heidelberg (2012)
26. Zheng, S.G., Qiu, D.W., Gruska, J., Li, L.Z., Mateus, P.: State succinctness of two-way finite automata with quantum and classical states. *Theoretical Computer Science* 499, 98–112 (2013)
27. Zheng, S.G., Gruska, J., Qiu, D.W.: On the state complexity of semi-quantum finite automata. *arXiv:1307.2499* (2013)