RAIRO-Theor. Inf. Appl. 48 (2014) 187–207
DOI: 10.1051/ita/2014003

Available online at:
www.rairo-ita.org

ON THE STATE COMPLEXITY OF SEMI-QUANTUM FINITE AUTOMATA [*], [**]

Shenggen Zheng[1], Jozef Gruska[1] and Daowen Qiu[2]

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.

Mathematics Subject Classification. 81-08, 68Q19, 68Q45.

Keywords and phrases. Quantum computing, quantum finite automata, semi-quantum finite automata, state complexity.

[*] *Work of the first and second authors 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 the first and second authors 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.*

[1] Faculty of Informatics, Masaryk University, Brno 60200, Czech Republic.
`zhengshenggen@gmail.com; gruska@fi.muni.cz`

[2] Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, P.R. China.
`issqdw@mail.sysu.edu.cn`

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 very first attempts to introduce such models, by Moore and Crutchfields [34] as well as Kondacs and Watrous [26] 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 [26]. Therefore it started to be of interest to introduce and explore some "less quantum" variations of 2FA and their power [3,4,10,33,43].

A "hybrid" – quantum/clssical – variations of 2FA, namely, *two-way finite automata with quantum and classical states* (2QCFA), were introduced by Ambainis and Watrous [3]. 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) [3,46,47]. A one-way version of 2QCFA was studied in [45], 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 [42], *e.g.*, in natural language and speech processing, image generation and encoding, *etc.* Early in 1959, Rabin and Scott [37] 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 [40] 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 [23]. 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 [1–9, 13–17, 21, 27–32, 41–46].

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 strings equality problem.

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 [11, 12].

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

Klauck [24] 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[3]. Applying the communication complexity result from [11, 12] to finite automata, for any $n \in \mathbb{Z}^+$, we prove that promise problem $A_{EQ}(n)$ can be solved by an exact 1QCFA with n quantum basis states and $\mathbf{O}(n)$ classical states, whereas the sizes of the corresponding 1DFA are $2^{\mathbf{\Omega}(n)}$.

As the next we will consider state complexity of the language $L(p) = \{a^{kp} \,|\, k \in \mathbb{Z}^+\}$. It is well know that, for any $p \in \mathbb{Z}^+$, each 1DFA and 1NFA accepting $L(p)$ has at least p states. Ambainis and Freivalds [4], 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 ε with $poly\left(\frac{1}{\varepsilon}\right) \cdot \log p$ basis states

[3] Ambainis and Yakaryilmaz showed in [6] that there is a very special case in which the superiority of quantum computation to classical one cannot be bounded.

(where $poly(x)$ is some polynomial in x). This bound was improved to $\mathbf{O}(\frac{\log p}{\varepsilon^3})$ in [8] and to $4\frac{\log 2p}{\varepsilon}$ in [5]. 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 [4]. For the case that p is not a prime, Mereghetti *et al.* [30] showed that the number of states of a 1PFA necessary and sufficient for accepting the language $L(p)$ with isolated cut point is $p_1^{\alpha_1} + p_2^{\alpha_2} + \ldots + p_s^{\alpha_s}$, where $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ is the prime factorization of p. Mereghetti el at. [30] 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) [29]. For the case that p is not prime, the number of states necessary and sufficient for accepting $L(p)$ on 2DFA and 2NFA is $p_1^{\alpha_1} + p_2^{\alpha_2} + \ldots + p_s^{\alpha_s}$ [29], where $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ is the prime factorization of p. Yakaryilmaz and Cem Say [44] showed that there exists a 7-state *one-way finite automaton with restart* (1QFA$^{\circlearrowleft}$) which accepts $L(p)$ with one-sided error ε 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 1QFA$^{\circlearrowleft}$ $\mathcal{M}_1$ with expected running time $t(|w|)$, Yakaryilmaz and Cem Say [44] 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 ε 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 ε 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 $m \in \mathbb{Z}^+$, is extensively studied in literatures as well. For any $m \in \mathbb{Z}^+$ and any finite alphabet Σ, it is obvious that the number of states of a 1DFA for accepting the language $C(m) = \{w \,|\, w \in \Sigma^m\}$ is at least m. Freivalds [15] showed that there is an ε error probability 1PFA accepting $C(m)$ with $\mathbf{O}(\log^2 m)$ states. Ambainis and Freivalds [4] proved that $C(m)$ can be recognized by an MO-1QFA with $\mathbf{O}(\log m)$ quantum basis states. Yakaryilmaz and Cem Say [44] showed that there exists a 7-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}$ which accepts $C(m)$ with one-sided error ε and expected running time $\mathbf{O}(\frac{1}{\varepsilon}2^m|w|)$ which is an exponential of m. The 1QFA$^{\circlearrowleft}$ $\mathcal{M}$ 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 ε in 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 and $|w|$. 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 ε 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.

The paper is structured as follows. In Section 2 some basic concepts and notations are introduced and 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. Finally, Section 6 contains a conclusion and suggestions for further research.

2. Preliminaries

We introduce in this section some basic concepts and also notations concerning quantum information processing and afterwards also the models of 1QCFA and 2QCFA. Concerning more on quantum information processing we refer the reader to [19, 38], and concerning more on classical and quantum automata [19, 20, 22, 35, 39].

2.1. Preliminaries of quantum information processing

According to quantum mechanical principles, to each closed quantum system $\mathcal{S}$, a Hilbert space $\mathcal{H}_\mathcal{S}$ is associated and states of $\mathcal{S}$ correspond to vectors of the norm one of $\mathcal{H}_\mathcal{S}$. In case $\mathcal{H}_\mathcal{S}$ is an n-dimensional vector space then it has a basis (actually infinite many of them) consisting of n mutually orthogonal vectors. We will mostly denote such a basis and its vectors by

$$\{|i\rangle\}_{i=1}^n.$$

In such a case any vector of $\mathcal{H}_\mathcal{S}$ can be uniquely expressed as a superposition

$$|\psi\rangle = \sum_{i=1}^n \alpha_i |i\rangle, \qquad (2.1)$$

where α_i's are complex numbers, called probability amplitudes, that satisfy the following, so-called normalization, condition $\sum_{i=1}^n |\alpha_i|^2 = 1$. If the state $|\psi\rangle$ is measured with respect to the above basis, then the state collapses to one of the states $|i\rangle$ and to a particular state $|i_0\rangle$ with the probability $|\alpha_{i_0}|^2$. i_0 is then the outcome (discrete) received into the classical world.

Each evolution step of a finite n dimensional quantum system is specified by a unitary $n \times n$ matrix U and changes any current state $|\phi\rangle$ into the state $U|\phi\rangle$.

To extract some information from a quantum state $|\psi\rangle$ a measurement has to be performed. We will consider here mostly measurements defined by a set $\{P_m\}$ of so-called projective operators/matrices, where indices m refer to the potential classical outcomes of measurements, with the property:

$$P_iP_j = \begin{cases} P_i & i = j, \\ 0 & i \neq j, \end{cases} \tag{2.2}$$

that, in addition, satisfies the following completeness condition

$$\sum_m P_m = I. \tag{2.3}$$

In case a state $|\psi\rangle$ is measured with respect to the set of projective operators $\{P_m\}$, then the classical outcome m is obtained with the probability

$$p(m) = \|P_m|\psi\rangle\|^2, \tag{2.4}$$

and then the state $|\psi\rangle$ "collapses" into the state

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}. \tag{2.5}$$

A projective measurement $\{P_m\}$ is usually specified by an *observable* M, a Hermitian matrix that has a so called spectral decomposition

$$M = \sum_m mP_m, \tag{2.6}$$

where m are mutually different eigenvalues of M and each P_m is a projector into the space of eigenvectors associated to the eigenvalue m.

2.2. Preliminaries on semi-quantum finite automata

2QCFA were introduced by Ambainis and Watrous [3] and explored also by Yakaryilmaz, Qiu, Zheng and others [36,44–48]. 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 2.1. A 2QCFA $\mathcal{A}$ is specified by a 9-tuple

$$\mathcal{A} = (Q, S, \Sigma, \Theta, \delta, |q_0\rangle, s_0, S_{\rm acc}, S_{\rm rej}) \tag{2.7}$$

where:

(1) Q is a finite set of orthonormal quantum basis states.
(2) S is a finite set of classical states.
(3) Σ 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) $S_{\text{acc}} \subset S$ and $S_{\text{rej}} \subset S$, where $S_{\text{acc}} \cap S_{\text{rej}} = \emptyset$ are sets of the classical accepting and rejecting states, respectively.
(7) Θ is a quantum transition function

$$\Theta : S \setminus (S_{\text{acc}} \cup S_{\text{rej}}) \times \Sigma' \to U(H(Q)) \cup O(H(Q)), \tag{2.8}$$

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) δ is a classical transition function. If the automaton $\mathcal{A}$ is in the classical state s, its tape head is scanning a symbol σ 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

$$\delta : S \setminus (S_{\text{acc}} \cup S_{\text{rej}}) \times \Sigma' \to S \times \{-1, 0, 1\}. \tag{2.9}$$

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 $\{P_1, \ldots, P_n\}$ and its corresponding classical outcome is from the set $N_{\Theta(s,\sigma)} = \{1, 2, \ldots, n\}$. The classical transition function δ can be then specified as follow

$$\delta : S \setminus (S_{\text{acc}} \cup S_{\text{rej}}) \times \Sigma' \times N_{\Theta(s,\sigma)} \to S \times \{-1, 0, 1\}. \tag{2.10}$$

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 $S_{\text{acc}}(S_{\text{rej}})$).

The computation of a 2QCFA $\mathcal{A} = (Q, S, \Sigma, \Theta, \delta, |q_0\rangle, s_0, S_{\text{acc}}, S_{\text{rej}})$ 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 σ 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 $S_{\text{acc}} \cup S_{\text{rej}}$. Therefore, similarly to the definition of accepting and rejecting probabilities for 2QFA [26], the accepting and rejecting probabilities $Pr[\mathcal{A}\ accepts\ w]$ and $Pr[\mathcal{A}$ 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 2.2. 1QCFA are one-way versions of 2QCFA [45]. 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 endmarker. 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 $0 < \varepsilon \leq \frac{1}{2}$. A finite automaton $\mathcal{A}$ recognizes L with a *one-sided error* ε if, for $w \in \Sigma^*$,

1. $\forall w \in L$, $Pr[\mathcal{A}$ accepts $w] = 1$, and
2. $\forall w \notin L$, $Pr[\mathcal{A}$ rejects $w] \geq 1 - \varepsilon$.

Let $0 < \varepsilon < \frac{1}{2}$. A finite automaton $\mathcal{A}$ recognizes L with an *error probability* ε if, for $w \in \Sigma^*$,

1. $\forall w \in L$, $Pr[\mathcal{A}$ accepts $w] \geq 1 - \varepsilon$, and
2. $\forall w \notin L$, $Pr[\mathcal{A}$ rejects $w] \geq 1 - \varepsilon$.

Let $0 < \lambda < 1$. A language L is said to be accepted by a finite automation $\mathcal{A}$ with an *isolated cut point* λ if there exists $\delta > 0$, for $w \in \Sigma^*$, such that

1. $\forall w \in L$, $Pr[\mathcal{A}$ accepts $w] \geq \lambda + \delta$, and
2. $\forall w \notin L$, $Pr[\mathcal{A}$ accepts $w] \leq \lambda - \delta$.

Obviously, for $0 < \varepsilon < \frac{1}{2}$, one-sided error acceptance is stricter than an error probability acceptance and the error probability acceptance is stricter than an isolated cut point acceptance.

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

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is solved by an exact 1QCFA $\mathcal{A}$ if

1. $\forall w \in A_{\text{yes}}$, $Pr[\mathcal{A}$ accepts $w] = 1$, and
2. $\forall w \in A_{\text{no}}$, $Pr[\mathcal{A}$ rejects $w] = 1$.

3. State complexities for strings equality problems

Strings equality problem is a basic problem in communication complexity [25] defined as follows. Let Alice and Bob be the two communicating parties. Alice is given as an input $x \in \{0,1\}^n$ and Bob is given as an input $y \in \{0,1\}^n$. They wish to compute the value of the function $EQ(x,y)$ defined to be 1 if $x = y$ and 0 otherwise.

We use a promise problem to model the promise version of strings equality problem studied in [11, 12]. For the alphabet $\Sigma = \{0,1,\#\}$ and even $n \in \mathbb{Z}^+$, let us consider the promise problem $A_{EQ}(n) = (A_{\text{yes}}(n), A_{\text{no}}(n))$, where $A_{\text{yes}}(n) = \{x\#y \,|\, x = y, x, y \in \{0,1\}^n\}$ and $A_{\text{no}}(n) = \{x\#y \,|\, x \neq y, x, y \in \{0,1\}^n, H(x,y) = \frac{n}{2}\}$.

Theorem 3.1. *The promise problem $A_{EQ}(n)$ can be solved by an exact 1QCFA $\mathcal{A}(n)$ with n quantum basis states and $\mathbf{O}(n)$ classical states, whereas the sizes of the corresponding 1DFA are $2^{\mathbf{\Omega}(n)}$.*

```
1. Read the left end-marker ¢, perform $U_s$ on the initial quantum state $|1\rangle$, change its classical state to $\delta(s_0, ¢) = s_1$, 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.
```

Figure 1. Description of the behavior of $\mathcal{A}(n)$ when solving the promise problem $A_{EQ}(n)$.

Proof.
Let $x = x_1 \dots x_n$ and $y = y_1 \dots y_n$ with $x, y \in \{0,1\}^n$. Let us consider a 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 ith symbol of $x(y)$ and s_{n+1} means that the next scanned symbol of the tape head is #($). The automaton proceeds as shown in Figure 1, where

$$U_s|1\rangle = \tfrac{1}{\sqrt{n}} \textstyle\sum_{i=1}^{n} |i\rangle;$$
$$U_{i,\sigma}|i\rangle = (-1)^{\sigma}|i\rangle \quad \text{and} \quad U_{i,\sigma}|j\rangle = |j\rangle \text{ for } j \neq i;$$
$$U_f(\textstyle\sum_{i=1}^{n} \alpha_i|i\rangle) = \left(\tfrac{1}{\sqrt{n}} \textstyle\sum_{i=1}^{n} \alpha_i\right) |1\rangle + \ldots$$

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

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

$$|\psi_4\rangle = U_f\left(\sum_{i=1}^{n} \frac{1}{\sqrt{n}}(-1)^{x_i+y_i}|i\rangle\right) = U_f\frac{1}{\sqrt{n}}\begin{pmatrix}(-1)^{x_1+y_1}\\(-1)^{x_2+y_2}\\\vdots\\(-1)^{x_n+y_n}\end{pmatrix} \tag{3.1}$$

$$= \begin{pmatrix}\frac{1}{n}\sum_{i=1}^{n}(-1)^{x_i+y_i}\\\vdots\\\vdots\end{pmatrix}. \tag{3.2}$$

If the input string $w \in A_{\text{yes}}(n)$, then $x_i = y_i$ for $1 \leq i \leq n$ 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 $w \in A_{\text{no}}(n)$, 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 strings equality problem is at least $0.007n$ [11,12]. Therefore, the sizes of the corresponding 1DFA are $2^{\mathbf{\Omega}(n)}$ [25]. □

4. State succinctness for 2QCFA

State succinctness for 2QCFA was explored by Yakaryilmaz, Zheng and others [44,46]. In [46], 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.

```
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.
```

FIGURE 2. Description of the behavior of $\mathcal{A}(p,\varepsilon)$ when recognizing the language $L(p)$.

4.1. State succinctness for the language $L(p)$

Theorem 4.1. *For any $p \in \mathbb{Z}^+$ and $0 < \varepsilon \leq \frac{1}{2}$, the language $L(p)$ can be recognized with one-sided error ε by a 2QCFA $\mathcal{A}(p,\varepsilon)$ with 2 quantum basis states and a constant number of classical states (neither depending on p nor on ε) in a linear expected running time $\mathbf{O}(\frac{1}{\varepsilon}p^2 n)$, where n is the length of input.*

Proof.
The main idea of the proof is as follows: we 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 current quantum state. If the resulting quantum state is $|q_1\rangle$, the input string is rejected, otherwise the automaton proceeds as shown in Figure 2, where

$$U_p = \begin{pmatrix} \cos\frac{\pi}{p} & -\sin\frac{\pi}{p} \\ \sin\frac{\pi}{p} & \cos\frac{\pi}{p} \end{pmatrix} \text{ and } U_{p,\varepsilon} = \begin{pmatrix} \frac{1}{\sqrt{p^2/4\varepsilon}} & -\frac{\sqrt{p^2/4\varepsilon-1}}{\sqrt{p^2/4\varepsilon}} \\ \frac{\sqrt{p^2/4\varepsilon-1}}{\sqrt{p^2/4\varepsilon}} & \frac{1}{\sqrt{p^2/4\varepsilon}} \end{pmatrix}. \tag{4.1}$$

Lemma 4.2. *If the input $w \in L(p)$, then the quantum state of $\mathcal{A}(p,\varepsilon)$ after step 2 is one of the quantum states $\pm|q_0\rangle$.*

Proof.
If $w \in L(p)$, then $|w| = n = kp$, where $k \in \mathbb{Z}^+$. Starting with the state $|q_0\rangle$, $\mathcal{A}(p,\varepsilon)$ changes its quantum state to $|q\rangle = (U_p)^n|q_0\rangle$ after step 2, where

$$|q\rangle = (U_p)^n|q_0\rangle = \begin{pmatrix} \cos\frac{\pi}{p} & -\sin\frac{\pi}{p} \\ \sin\frac{\pi}{p} & \cos\frac{\pi}{p} \end{pmatrix}^n |q_0\rangle = \begin{pmatrix} \cos\frac{n\pi}{p} & -\sin\frac{n\pi}{p} \\ \sin\frac{n\pi}{p} & \cos\frac{n\pi}{p} \end{pmatrix} |q_0\rangle \tag{4.2}$$

$$= \begin{pmatrix} \cos k\pi & -\sin k\pi \\ \sin k\pi & \cos k\pi \end{pmatrix} |q_0\rangle = \pm |q_0\rangle. \tag{4.3}$$

□

Lemma 4.3. *If the input $w \notin L(p)$, then $\mathcal{A}(p, \varepsilon)$ rejects w after step 3 with a probability at least $4/p^2$.*

Proof.
Suppose $n = |w| = kp + i$, where $k \in \mathbb{Z}^+$ and $i \in \{1, 2, \ldots, p-1\}$. The quantum state of $\mathcal{A}(p, \varepsilon)$ after step 2 will be

$$|q\rangle = (U_p)^n |q_0\rangle = \begin{pmatrix} \cos\frac{\pi}{p} & -\sin\frac{\pi}{p} \\ \sin\frac{\pi}{p} & \cos\frac{\pi}{p} \end{pmatrix}^n |q_0\rangle = \begin{pmatrix} \cos\frac{n\pi}{p} & -\sin\frac{n\pi}{p} \\ \sin\frac{n\pi}{p} & \cos\frac{n\pi}{p} \end{pmatrix} |q_0\rangle \tag{4.4}$$

$$= \begin{pmatrix} \cos\frac{i\pi}{p} & -\sin\frac{i\pi}{p} \\ \sin\frac{i\pi}{p} & \cos\frac{i\pi}{p} \end{pmatrix} |q_0\rangle = \cos\frac{i\pi}{p}|q_0\rangle + \sin\frac{i\pi}{p}|q_1\rangle. \tag{4.5}$$

The probability of observing $|q_1\rangle$ is $\sin^2\frac{i\pi}{p}$ in step 3.

Let $f(x) = \sin(x\pi) - 2x$. We have $f''(x) = -\pi^2 \sin(x\pi) \le 0$ when $x \in [0, 1/2]$. Therefore, $f(x)$ is concave in the interval $[0, 1/2]$, and $f(0) = f(1/2) = 0$. So, for any $x \in [0, 1/2]$, $f(x) \ge 0$, that is $\sin(x\pi) \ge 2x$. Therefore,

$$\sin^2\frac{i\pi}{p} \ge \sin^2\frac{\pi}{p} \ge \left(\frac{2}{p}\right)^2 = \frac{4}{p^2}. \tag{4.6}$$

□

Lemma 4.4. *If the input $w \in L(p)$, then $\mathcal{A}(p, \varepsilon)$ accepts w after step 4 with the probability $\frac{4\varepsilon}{p^2}$. If the input $w \notin L(p)$, then $\mathcal{A}(p, \varepsilon)$ accepts w after step 4 with a probability less than $\frac{4\varepsilon}{p^2}$.*

Proof.
If $w \in L(p)$, then the quantum state of $\mathcal{A}(p, \varepsilon)$ after step 2 will be $|q_0\rangle$, according to Lemma 4.2. After step 3 the quantum state will be

$$|q\rangle = U_{p,\varepsilon}|q_0\rangle = \begin{pmatrix} \frac{1}{\sqrt{p^2/4\varepsilon}} & -\frac{\sqrt{p^2/4\varepsilon - 1}}{\sqrt{p^2/4\varepsilon}} \\ \frac{\sqrt{p^2/4\varepsilon - 1}}{\sqrt{p^2/4\varepsilon}} & \frac{1}{\sqrt{p^2/4\varepsilon}} \end{pmatrix} |q_0\rangle = \frac{1}{\sqrt{p^2/4\varepsilon}}|q_0\rangle + \frac{\sqrt{p^2/4\varepsilon - 1}}{\sqrt{p^2/4\varepsilon}}|q_1\rangle. \tag{4.7}$$

Therefore, after the measurement in step 4, the input is accepted with the probability $\frac{4\varepsilon}{p^2}$.

If $w \notin L(p)$, then the probability that the quantum state of $\mathcal{A}(p, \varepsilon)$ after step 2 is $|q_0\rangle$ is less than 1. Therefore, $\mathcal{A}(p, \varepsilon)$ accepts w after step 4 with a probability less than $\frac{4\varepsilon}{p^2}$. □

In step 4, if $\mathcal{A}(p,\varepsilon)$ accepts the input string, then $\mathcal{A}(p,\varepsilon)$ halts. Otherwise, the resulting quantum state of the measurement is $|q_1\rangle$ and an application of the operation $|q_0\rangle\langle q_1|$ results in state $|q_0\rangle$ in which then $\mathcal{A}(p,\varepsilon)$ starts a new iteration.

If $w \in L(p)$, then according to Lemma 4.4, the probability of accepting the input in one iteration is

$$P_a = \frac{4\varepsilon}{p^2} \tag{4.8}$$

and the probability of rejecting the input in one iteration is

$$P_r = 0. \tag{4.9}$$

If the whole process is repeated ad infinitum, then the accepting probability is

$$Pr[\mathcal{A}(p,\varepsilon) \text{ accepts } w] = \sum_{i\geq 0}(1-P_a)^i(1-P_r)^i P_a = \sum_{i\geq 0}(1-P_a)^i P_a = \frac{P_a}{P_a} = 1. \tag{4.10}$$

If $w \notin L(p)$, then according to Lemmas 4.3 and 4.4, the probability of accepting the input in one iteration is

$$P_a < \frac{4\varepsilon}{p^2} \tag{4.11}$$

and the probability of rejecting the input in one iteration is

$$P_r > \frac{4}{p^2}\cdot \tag{4.12}$$

If the whole process is repeated indefinitely, then the probability that $\mathcal{A}(p,\varepsilon)$ rejects the input w is

$$Pr[\mathcal{A}(p,\varepsilon) \text{ rejects } w] = \sum_{i\geq 0}(1-P_a)^i(1-P_r)^i P_r = \frac{P_r}{P_a+P_r-P_aP_r} > \frac{P_r}{P_a+P_r} \tag{4.13}$$

$$> \frac{\frac{4}{p^2}}{\frac{4\varepsilon}{p^2}+\frac{4}{p^2}} = \frac{1}{\varepsilon+1} > 1-\varepsilon. \tag{4.14}$$

Time analysis: Steps 1 to 4 take time $\mathbf{O}(n)$. The halting probability is in both cases $\boldsymbol{\Omega}\left(\frac{\varepsilon}{p^2}\right)$, so the expected number of repetitions of the above process is, in both cases, $\mathbf{O}(\frac{p^2}{\varepsilon})$. Hence the expected running time of $\mathcal{A}(p,\varepsilon)$ is $\mathbf{O}(\frac{1}{\varepsilon}p^2 n)$. □

The most important work in designing an automaton is to design its transition function. Similar unitary matrixes of U_p (the quantum transition function after scanning a symbol of input) and proof methods in the previous Theorem can be found in [4, 5, 8, 30, 44]. The state complexity for $L(P)$ is relative to the error probability ε in [4, 5, 8, 30]. But in this paper the state complexity for $L(P)$ is not relative to the error probability ε, since we use a special matrix $U_{p,\varepsilon}$, which is never used in other papers.

Theorem 4.5. *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 4.6 [14]**.** *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 ε 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 4.6, there exits 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,

$$c^{bc^2} \geq p \Rightarrow bc^2 \log c \geq \log p \Rightarrow c^3 > (\log p)/b \Rightarrow c > \sqrt[3]{(\log p)/b}. \tag{4.15}$$

□

4.2. State succinctness for the language $C(m)$

Theorem 4.7. *For any $m \in \mathbb{Z}^+$ and $0 < \varepsilon \leq \frac{1}{2}$, the language $C(m)$ can be recognized with one-sided error ε by a 2QCFA $\mathcal{A}(m, \varepsilon)$ with 2 quantum basis states and a constant number of classical states (neither depending on m nor on ε) in a polynomial expected running time $\mathbf{O}(\frac{1}{\varepsilon}m^2n^4)$, where n is the length of input.*

Proof.
The main idea of the proof is as follows: we 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 ¢, 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 shown in Figure 3, where

$$U_{¢} = \begin{pmatrix} \cos m\sqrt{2}\pi & \sin m\sqrt{2}\pi \\ -\sin m\sqrt{2}\pi & \cos m\sqrt{2}\pi \end{pmatrix}, \; U_\alpha = \begin{pmatrix} \cos\sqrt{2}\pi & -\sin\sqrt{2}\pi \\ \sin\sqrt{2}\pi & \cos\sqrt{2}\pi \end{pmatrix}, \tag{4.16}$$

$$U_{m,\varepsilon} = \begin{pmatrix} \frac{1}{\sqrt{2m^2/\varepsilon}} & -\frac{\sqrt{2m^2/\varepsilon-1}}{\sqrt{2m^2/\varepsilon}} \\ \frac{\sqrt{2m^2/\varepsilon-1}}{\sqrt{2m^2/\varepsilon}} & \frac{1}{\sqrt{2m^2/\varepsilon}} \end{pmatrix}. \tag{4.17}$$

```
Repeat the following ad infinity:

  1.  Move the tape head to the left end-marker, read the end-marker ¢, apply $U_{¢}$
      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.
```

FIGURE 3. Description of the behavior of $\mathcal{A}(m,\varepsilon)$ when recognizing the language L_m.

Lemma 4.8. *If the input $w \in C(m)$, then the quantum state of the above automaton $\mathcal{A}(m,\varepsilon)$, after step 2, is $|q_0\rangle$.*

Proof.
For $w \in C(m)$, we have $|w| = m$. Starting with the state $|q_0\rangle$, $\mathcal{A}(m,\varepsilon)$ changes its quantum state after processing the whole input after step 2 to

$$|q\rangle = (U_\alpha)^m U_{¢}|q_0\rangle = \begin{pmatrix} \cos\sqrt{2}\pi & -\sin\sqrt{2}\pi \\ \sin\sqrt{2}\pi & \cos\sqrt{2}\pi \end{pmatrix}^m \begin{pmatrix} \cos m\sqrt{2}\pi & \sin m\sqrt{2}\pi \\ -\sin m\sqrt{2}\pi & \cos m\sqrt{2}\pi \end{pmatrix} |q_0\rangle \tag{4.18}$$

$$= \begin{pmatrix} \cos m\sqrt{2}\pi & -\sin m\sqrt{2}\pi \\ \sin m\sqrt{2}\pi & \cos m\sqrt{2}\pi \end{pmatrix} \begin{pmatrix} \cos m\sqrt{2}\pi & \sin m\sqrt{2}\pi \\ -\sin m\sqrt{2}\pi & \cos m\sqrt{2}\pi \end{pmatrix} |q_0\rangle \tag{4.19}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} |q_0\rangle = |q_0\rangle. \tag{4.20}$$

□

Lemma 4.9 [46]**.** *If the input $w \notin C(m)$, then $\mathcal{A}(p,\varepsilon)$ rejects w after step 3.1 with a probability at least $1/(2(m-n)^2+1)$.*

Lemma 4.10 [46]**.** *A coin flipping can be simulated by a 2QCFA using two basis states $|q_0\rangle$ and $|q_1\rangle$.*

Lemma 4.11. *Suppose that the length of input $|w| = n$. If $w \in C(m)$, then $\mathcal{A}(m,\varepsilon)$ accepts w after step 4 with the probability $\frac{\varepsilon}{2m^2(n+1)^2}$. If $w \notin C(m)$, then $\mathcal{A}(m,\varepsilon)$ accepts w, after step 4, with a probability less than $\frac{\varepsilon}{2m^2(n+1)^2}$.*

Proof.
If $w \in C(m)$, then the quantum state of $\mathcal{A}(m, \varepsilon)$ after step 2 will be $|q_0\rangle$, according to Lemma 4.8. In step 3.2 two random walks start at cell 1 and stop at cell 0 (with the left end-marker ¢) or at the cell $n+1$ (with the right end-marker \$). It is known, from the Markov chains theory, that the probability of reaching cell $n+1$ is $\frac{1}{n+1}$ (see Chapt. 14.2 in [18]). Therefore, the probability that the quantum state of $\mathcal{A}(m, \varepsilon)$ is $|q_0\rangle$ after step 3.2 will be $\frac{1}{(n+1)^2}$.

The quantum state of $\mathcal{A}(m, \varepsilon)$ after step 4 will therefore be

$$|q\rangle = U_{m,\varepsilon}|q_0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2m^2/\varepsilon}} & -\frac{\sqrt{2m^2/\varepsilon-1}}{\sqrt{2m^2/\varepsilon}} \\ \frac{\sqrt{2m^2/\varepsilon-1}}{\sqrt{2m^2/\varepsilon}} & \frac{1}{\sqrt{2m^2/\varepsilon}} \end{pmatrix} |q_0\rangle \tag{4.21}$$

$$= \frac{1}{\sqrt{2m^2/\varepsilon}}|q_0\rangle + \frac{\sqrt{2m^2/\varepsilon - 1}}{\sqrt{2m^2/\varepsilon}}|q_1\rangle. \tag{4.22}$$

The input is therefore accepted after the measurement in step 4 with the probability $\frac{\varepsilon}{2m^2(n+1)^2}$.

If $w \notin C(m)$, then the probability that after step 2 the quantum state of $\mathcal{A}(m, \varepsilon)$ is $|q_0\rangle$ is less than 1. Therefore, $\mathcal{A}(m, \varepsilon)$ accepts w, after step 4, with a probability less than $\frac{\varepsilon}{2m^2(n+1)^2}$. □

In step 4, if $\mathcal{A}(m, \varepsilon)$ accepts the input string, then $\mathcal{A}(m, \varepsilon)$ halts. Otherwise, the resulting quantum state after the measurement is $|q_1\rangle$ and an application of the operator $|q_0\rangle\langle q_1|$ results in state $|q_0\rangle$ in which then $\mathcal{A}(m, \varepsilon)$ starts a new iteration.

Suppose that the length of input w is n. If $w \in C(m)$, then according to Lemma 4.11, the probability of accepting the input in one iteration is

$$P_a = \frac{\varepsilon}{2m^2(n+1)^2} = \frac{\varepsilon}{2m^2(m+1)^2} \tag{4.23}$$

and the probability of rejecting the input in one iteration is

$$P_r = 0. \tag{4.24}$$

If the whole process is repeated for infinity, the accepting probability is

$$Pr[\mathcal{A}(m, \varepsilon) \text{ accepts } w] = \sum_{i \geq 0}(1 - P_a)^i(1 - P_r)^i P_a = \sum_{i \geq 0}(1 - P_a)^i P_a = \frac{P_a}{P_a} = 1. \tag{4.25}$$

If $w \notin C(m)$, then according to Lemmas 4.9 and 4.11, the probability of accepting the input in one iteration is

$$P_a < \frac{\varepsilon}{2m^2(n+1)^2} \tag{4.26}$$

and the probability of rejecting the input in one iteration is

$$P_r > \frac{1}{2(m-n)^2+1}. \tag{4.27}$$

If the whole process is repeated indefinitely, then the probability that $\mathcal{A}(p,\varepsilon)$ rejects the input w is

$$\begin{aligned} Pr[\mathcal{A}(p,\varepsilon) \text{ rejects } w] &= \sum_{i\geq 0}(1-P_a)^i(1-P_r)^i P_r \\ &= \frac{P_r}{P_a+P_r-P_aP_r} > \frac{P_r}{P_a+P_r} \\ &> \frac{\frac{1}{2(m-n)^2+1}}{\frac{\varepsilon}{2m^2(n+1)^2}+\frac{1}{2(m-n)^2+1}} \qquad (4.28) \\ &= \frac{1}{\frac{(2(m-n)^2+1)\varepsilon}{2m^2(n+1)^2}+1} > \frac{1}{\varepsilon+1} > 1-\varepsilon. \qquad (4.29) \end{aligned}$$

In the above inequality we have used the fact that $0 < \frac{2(m-n)^2+1}{2m^2(n+1)^2} < 1$ for any $m > 0$ and $n > 0$.

Time analysis: The expected running time of steps 1 to 4 is $\mathbf{O}(n^2)$ time. The halting probability is in both cases $\mathbf{\Omega}\left(\frac{\varepsilon}{m^2n^2}\right)$, and therefore the expected number of repetitions of the above process is, in both cases, $\mathbf{O}(\frac{m^2n^2}{\varepsilon})$. Hence the expected running time of $\mathcal{A}(m,\varepsilon)$ is $\mathbf{O}(\frac{1}{\varepsilon}m^2n^4)$. □

The matrices (quantum transition function) used in the previous Theorem are modifications of the ones used in [3]. Similar proof methods can be found in [3, 46, 47].

Remark 4.12. Using the above theorem and the intersection property of languages recognized by 2QCFA [36], it is easy to improve the result from [46] related to the promise problem[4] $A^{eq}(m)$ to a language $L^{eq}(m) = \{a^m b^m\} = L^{eq} \cap C(2m)$, where the language $L^{eq} = \{a^n b^n \mid n \in \mathbb{N}\}$. Therefore, the open problem from [46] is solved.

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 4.5, we get:

Theorem 4.13. *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 ε depend on the error ε in most of the papers. For example, in [5], the size of MO-1QFA accepting $L(p)$ with one-sided error ε is $4\frac{\log 2p}{\varepsilon}$. If $\varepsilon < \frac{4}{p}$, the state

[4] See page 102 in [46].

complexity advantage of MO-1QFA disappears. However, in our model, the sizes of 2QCFA do not depend on the error ε, 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 5.1. *For any integer $p \in \mathbb{Z}^+$ 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 one-sided error ε 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.
Obviously, $\gcd(q_1, q_2) = 1$ and therefore $L(p) = L(q_1) \cap L(q_2)$. According to [5], the language $L(q_1)$ can be recognized with one-sided error ε by an MO-1QFA with $4\frac{\log 2q_1}{\varepsilon}$ quantum basis states. It is well known that the language $L(q_2)$ can be recognized by a q_2-state 1DFA. A q_1-state MO-1QFA can be simulated by a 1QCFA with q_1 quantum basis states and 3 classical states [45]. A q_2-state 1DFA can be simulated by 1QCFA with 1 quantum state and $q_2 + 1$ classical states [45]. Now we have to use the following lemma

Lemma 5.2 [45]**.** *Let a language L_1 be recognized with one-sided error ε_1 by a 1QCFA $\mathcal{A}_1$ with q_1 quantum basis states and c_1 classical states. Let a language L_2 be recognized with one-sided error ε_2 by a 1QCFA $\mathcal{A}_2$ with q_2 quantum basis states and c_2 classical states. Then the language $L_1 \cap L_2$ can be recognized with one-sided error $\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2$ by a 1QCFA $\mathcal{A}$ with $q_1 q_2$ quantum basis states and $c_1 c_2$ classical states.*

According to Lemma 5.2, the language $L(p) = L(q_1) \cap L(q_2)$ can be recognized with one-sided error ε 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. □

6. Concluding remarks

We have explored the state complexity of 1QCFA for a family of promise problems. For any $n \in \mathbb{Z}^+$, we have proved that the promise problem $A_{EQ}(n)$, modeling the strings equality problem of length n with restriction, can be solved by an exact 1QCFA $\mathcal{A}(n)$ with $2n$ quantum basis states and $\mathbf{O}(n)$ classical states, whereas the sizes of the corresponding 1DFA are $2^{\mathbf{\Omega}(n)}$. Afterwards, we have shown state succinctness results of 2QCFA for two basic and extensively studied families of regular languages. Namely, $L(p)$ and $C(m)$. We have proved that 2QCFA can be remarkably more concise than their corresponding classical counterparts and we have also solved one open problem from [46]. At last, we have proved that there exist various trade-offs for 1QCFA, which respect to the numbers of quantum and classical states needed for the family of languages $L(p)$.

Some possible problems for future work are:

(1) It has been proved [24] that exact 1QCFA have not state complexity advantage over 1DFA in recognizing a language. How about exact 2QCFA *vs.* 2DFA?
(2) It would be interesting to find out more trade-off properties of 1QCFA or 2QCFA.

Acknowledgements. The first author would like to thank Matej Pivoluska for stimulating discussions. We would also like to thank to the referee for careful reading our paper and various suggestions.

References

[1] A. Ambainis, A. Nayak, A. Ta-Shma and U. Vazirani, Dense quantum coding and quantum automata. *J. ACM* **49** (2002) 496–511.

[2] A. Ambainis, The complexity of probabilistic versus deterministic finite automata, *Proc. of the International Symposium on Algorithms and Computation (ISAAC96). Lect. Notes Comput. Sci.* **1178** (1996) 233–239.

[3] A. Ambainis and J. Watrous, Two-way finite automata with quantum and classical states. *Theoret. Comput. Sci.* **287** (2002) 299–311.

[4] A. Ambainis and R. Freivalds, One-way quantum finite automata: strengths, weaknesses and generalizations, in: *Proc. of the 39th Annual Symposium on Foundations of Computer Science.* IEEE Computer Society Press, Palo Alfo, California, USA (1998) 332–341.

[5] A. Ambainis and N. Nahimovs, Improved constructions of quantum automata. *Theoret. Comput. Sci.* **410** (2009) 1916–1922.

[6] A. Ambainis and A. Yakaryilmaz, Superiority of exact quantum automata for promise problems. *Inform. Process. Lett.* **112** (2012) 289–291.

[7] A. Bertoni, C. Mereghetti and B. Palano, Small size quantum automata recognizing some regular languages. *Theoret. Comput. Sci.* **340** (2005) 394–407.

[8] A. Bertoni, C. Mereghetti and b. Palano. Some formal tools for analyzing quantum automata. *Theoret. Comput. Sci.* **356** (2006) 14–25.

[9] J.C. Birget, State-complexity of finite-state devices, state compressibility and incompressibility. *Math. Systems Theory* **26** (1993) 237–269.

[10] A. Brodsky and N. Pippenger, Characterizations of 1-way quantum finite automata. *SIAM J. Comput.* **31** (2002) 1456–1478.

[11] H. Buhrman, R. Cleve and A. Wigderson, Quantum vs. classical communication and computation. *Proc. of 30th Annual ACM Symposium Theory Computing* (1998) 63–68.

[12] H. Buhrman, R. Cleve, S. Massar and R. de Wolf, Nonlocality and Communication Complexity. *Rev. Mod. Phys.* **82** (2010) 665–698

[13] M. Chrobak, Finite Automata and Unary Languages. *Theoret. Comput. Sci.* **47** (1986) 149–158.

[14] C. Dwork and L. Stockmeyer, A time-complexity gap for two-way probabilistic finite state automata. *SIAM J. Comput.* **19** (1990) 1011–1023.

[15] R. Freivalds, On the growth of the number of states in result of determinization of probabilistic finite automata. *Automatic Control Comput. Sci.* **3** (1982) 39–42.

[16] R. Freivalds, Non-constructive methods for finite probabilistic automata. *Int. J. Found. Comput. Sci.* **19** (2008) 565–580.

[17] R. Freivalds, M. Ozols and L. Mancinska, Improved constructions of mixed state quantum automata. *Theoret. Comput. Sci.* **410** (2009) 1923–1931.

[18] W. Feller, An Introduction to Probability Theory and its Applications, vol. I. Wiley, New York, 1967.

[19] J. Gruska, Quantum Computing. McGraw-Hill, London (1999).

[20] J. Gruska, Descriptional complexity issues in quantum computing. *J. Automata Languages Combinatorics* **5** (2000) 191–218.

[21] J. Gruska, D.W. Qiu, and S.G. Zheng, Communication complexity of promise problems and their applications to finite automata, `arXiv:1309.7739` (2013).

[22] J.E. Hopcroft and J.D. Ullman, Introduction to Automata Theory, Languages, and Computation. Addision-Wesley, New York, 1979.

[23] G.A. Kiraz, Compressed Storage of Sparse Finite-State Transducers, *Proc. of CIAA*, vol. 2214 of *Lect. Notes Comput. Sci.* (2001) 109–121.

[24] H. Klauck, On quantum and probabilistic communication: Las Vegas and one-way protocols. *Proc. of the 32th STOC* (2000) 644–651.

[25] E. Kushilevitz, Communication Complexity. *Adv. Comput.* **44** (1997) 331–360.

[26] A. Kondacs and J. Watrous, On the power of quantum finite state automata, in *Proc. of 38th IEEE Annal. Sympos. Found. of Comput. Sci.* (1997) 66–75.

[27] F. Le Gall, Exponential separation of quantum and classical online space complexity, in *Proc. of SPAA'06* (2006) 67–73.

[28] G. Liu, C. Martin-Vide, A. Salomaa and S. Yu, State complexity of basic operations combined with reversal, *Inf. Comput.* **206** (2008) 1178–186.

[29] C. Mereghetti and G. Pighizzini, Two-way automata simulations and unary languages. *J. Automata, Languages and Combinatorics* **5** (2000) 287–300.

[30] C. Mereghetti, B. Palano and G. Pighizzini, Note on the Succinctness of Deterministic, Nondeterministic, Probabilistic and Quantum Finite Automata. *RAIRO: ITA* **35** (2001) 477–490.

[31] C. Mereghetti and B. Palano, On the size of one-way quantum finite automata with periodic behaviors. *RAIRO: ITA* **36** (2002) 277–291.

[32] M. Milani and G. Pighizzini, Tight bounds on the simulation of unary probabilistic automata by deterministic automata, *J. Automata, Languages and Combinatorics* **6** (2001) 481–492.

[33] P. Mateusa, D.W. Qiu and L.Z. Li, On the complexity of minimizing probabilistic and quantum automata. *Inform. Comput.* **218** (2012) 36–53.

[34] C. Moore and J. P. Crutchfield, Quantum automata and quantum grammars. *Theoret. Comput. Sci.* **237** (2000) 275–306.

[35] A. Paz, Introduction to Probabilistic Automata. Academic Press, New York (1971).

[36] D. W. Qiu, Some Observations on Two-Way Finite Automata with Quantum and Classical States, *ICIC 2008*. In vol. 5226 of *Lect. Notes Comput. Sci.* (2008) 1–8.

[37] M. O. Rabin and D. Scott, Finite automata and their decision problems. *IBM J. Research Devel.* **3** (1959) 115–125.

[38] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 2000.

[39] D. W. Qiu, L.Z. Li, P. Mateus and J. Gruska, Quantum finite automata, *CRC Handbook of Finite State Based Models and Applications*. Edited by J.C. Wang. CRC Press (2012) 113–144.

[40] A. Salomaa, On the reducibility of events represented in automata. In *Annales Academiae Scientiarum Fennicae. Volume Series A of I. Math.* (1964) 353.

[41] S. Yu, Q. Zhuang and K. Salomaa The state complexity of some basic operations on regular languages. *Theoret. Comput. Sci.* **125** (1994) 315–328.

[42] S. Yu, State Complexity: Recent Results and Open Problems. *Fundamenta Informaticae* **64** (2005) 471–480.

[43] A. Yakaryilmaz and A.C. Cem Say, Unbounded-error quantum computation with small space bounds, *Inform. Comput.* **209** (2011) 873–892.

[44] A. Yakaryilmaz and A.C. Cem Say, Succinctness of two-way probabilistic and quantum finite automata. *Discrete Math. Theoret. Comput. Sci.* **12** (2010) 19–40.

[45] S.G. Zheng, D.W. Qiu, L.Z. Li and J. Gruska, One-way finite automata with quantum and classical states, vol 7300 of *Lect. Notes Comput. Sci.* Edited by H. Bordihn, M. Kutrib, and B. Truthe (2012) 273–290.

[46] S.G. Zheng, D.W. Qiu, J. Gruska, L.Z. Li and P. Mateus, State succinctness of two-way finite automata with quantum and classical states, *Theoret. Comput. Sci.* **499** (2013) 98–112.

[47] S.G. Zheng, D.W. Qiu and L.Z. Li, Some languages recognized by two-way finite automata with quantum and classical states. *Int. J. Foundation Comput. Sci.* **23** (2012) 1117–1129.

[48] S.G. Zheng, J. Gruska and D.W. Qiu. Power of the interactive proof systems with verifiers modeled by semi-quantum two-way finite automata. `arXiv:1304.3876` (2013).

Communicated by C. Choffrut.
Received June 20, 2013. Accepted January 27, 2014.