ELSEVIER

Theoretical Computer Science 287 (2002) 299–311

Theoretical Computer Science

www.elsevier.com/locate/tcs

Two-way finite automata with quantum and classical states

Andris Ambainis[a,*], John Watrous[b]

[a] Computer Science Division, University of California, Berkeley, CA 94720, USA
[b] Department of Computer Sciences, University of Calgary, Calgary, Alberta, Canada T2N 1N4

Abstract

We introduce 2-way finite automata with quantum and classical states (2qcfa's). This is a variant on the 2-way quantum finite automata (2qfa) model which may be simpler to implement than unrestricted 2qfa's; the internal state of a 2qcfa may include a quantum part that may be in a (mixed) quantum state, but the tape head position is required to be classical.

We show two languages for which 2qcfa's are better than classical 2-way automata. First, 2qcfa's can recognize palindromes, a language that cannot be recognized by 2-way deterministic or probabilistic finite automata. Second, in polynomial time 2qcfa's can recognize $\{a^n b^n | n \in \mathbb{N}\}$, a language that can be recognized classically by a 2-way probabilistic automaton but only in exponential time. © 2002 Elsevier Science B.V. All rights reserved.

1. Introduction

The theory of quantum computing has had some remarkable successes, such as Shor's quantum algorithm for factoring integers in polynomial time [21] and Grover's algorithm for searching an unordered list of size n with just $O(\sqrt{n})$ accesses to the list [11]. However, these algorithms are for general quantum Turing machines or quantum circuits. Today's experimental quantum computers are much less powerful and the biggest quantum computer consists of just 5 quantum bits (qubits). Therefore, it may be interesting to consider more restricted theoretical models of quantum computers. In this paper, we consider the following question: what is the simplest and most restricted model of computation where quantum computers are still more powerful than their classical counterparts? Classically, one of simplest models of computation is a finite

[*] Corresponding author.
E-mail addresses: ambainis@cs.berkeley.edu (A. Ambainis), jwatrous@cpsc.ucalgary.ca (J. Watrous).

0304-3975/02/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0304-3975(02)00138-X

automaton. Quantum finite automata have been recently studied by several authors [2,3,5,15,17].

Two models of quantum finite automata have been considered. The simplest is 1-way quantum finite automata (1qfa's) introduced by Kondacs and Watrous [15] and Moore and Crutchfield [17]. This is very simple model of computation but it is not very powerful; the languages recognized by 1qfa's form a proper subset of the regular languages (languages recognized by 1-way deterministic automata). A more powerful generalization of this model is 1-way qfa's that allow mixed states (defined similarly to quantum circuits with mixed states [1]). Any 1-way dfa can be easily simulated by a 1-way qfa with mixed states. However, all languages recognized by 1-way qfa's with mixed states (with bounded error) are still regular. The second model is 2-way quantum finite automata (2qfa's) [15]. In this model, it is easy to simulate any deterministic automaton and some nonregular languages can be recognized as well. This implies that 2qfa's are strictly more powerful than their classical counterparts. However, this model has another disadvantage: it allows superpositions where the head can be in multiple positions simultaneously. To implement such a machine, we need at least $O(\log n)$ qubits to store the position of the head (where n is the length of the input). It would be nicer to have a model where the size of the quantum part does not depend on the length of the input.

In this paper, we propose 2-way finite automata with quantum and classical states (2qcfa's), an intermediate model between 1qfa's and 2qfa's. This model is both powerful (2qcfa's can trivially simulate any classical automaton and recognize some languages that classical automata cannot) and can be implemented with a quantum part of constant size.

We consider the following two languages: $L_{\mathrm{pal}} = \{x \in \{a,b\}^* \,|\, x = x^R\}$ (the language consisting of all palindromes over the alphabet $\{a,b\}$) and $L_{\mathrm{eq}} = \{a^n b^n \,|\, n \in \mathbb{N}\}$. It has been shown that no probabilistic 2-way finite automaton can recognize L_{pal} with bounded error in any amount of time [7], and that no classical 2-way finite automaton can recognize L_{eq} (or any other nonregular language) with bounded error in polynomial time [6,13]. We prove that there exists an exponential time 2qcfa recognizing L_{pal} with bounded probability of error, and a polynomial time 2qcfa recognizing L_{eq} with bounded probability of error, thereby giving two examples where 2qcfa's are provably more powerful than classical 2pfa's.

It is interesting to note that our 2qcfa's for L_{pal} and L_{eq} require that the quantum part of the machine consist of only a single qubit; in essence, our 2qcfa's use the quantum state of this qubit to represent and process certain information regarding the input. While the extremely high precision required in manipulating this single qubit certainly calls into question the practicalities of these algorithms, it is interesting that such extreme examples of space-efficiency/precision trade-offs exist, particularly in light of existing bounds on the amount of information transmittable and accessible in a single qubit (or finite collection of qubits) [3,12,18].

The remainder of this paper has the following organization. In Section 2 we give a definition of 2-way finite automata with quantum and classical states. In Section 3 we describe a 2qcfa for L_{pal} and in Section 4 we give a 2qcfa for L_{eq}. We conclude with Section 5, which includes mention of various open questions relating to this paper.

2. Definitions

In this section we give our definition for 2-way finite automata with quantum and classical states. Informally, we may describe a 2qcfa as a classical 2-way finite automaton that has access to a fixed-size quantum register, upon which it may perform quantum transformations and measurements. The transformations and measurements are determined by local descriptions of the classical portion of the machine, and the results of the measurements may determine the manner in which the classical part of the machine evolves.

Before giving a more formal definition of our model, we recall a few basic facts regarding quantum computing. For a more detailed overview of quantum computing, we refer the reader to [4,14,19,20]. Let Q be a finite set. A *superposition* of elements in Q is a norm 1 vector in a Hilbert space $\mathscr{H}$ of dimension $|Q|$, where each element $q \in Q$ is identified with an elementary unit vector denoted by $|q\rangle$. Any superposition may therefore be written in the form $\sum_{q \in Q} \alpha_q |q\rangle$, where each α_q is a complex number and we have $\sum_{q \in Q} |\alpha_q|^2 = 1$. In general, we denote superpositions as $|\phi\rangle$, $|\psi\rangle$, etc., even when symbols ϕ, ψ, etc., are not used alone. A unitary operator on $\mathscr{H}$ is any invertible linear operator that preserves length (equivalently U is unitary if $U^{-1} = U^{\dagger}$, where $U^{\dagger}$ denotes the adjoint of U). When we say that we apply the *unitary transformation* described by U to a system in a given superposition $|\psi\rangle$, we mean that the superposition of this system is changed according to the mapping $|\psi\rangle \mapsto U|\psi\rangle$. A set of operators $\{P_j\}$ on $\mathscr{H}$ specify an *orthogonal measurement* (also called a *von Neumann measurement*) if $P_j = P_j^{\dagger}$ and $P_j^2 = P_j$ for all j, $P_j P_k = 0$ for $j \neq k$, and $\sum_j P_j = I$. If a superposition $|\psi\rangle$ is measured (or observed) via a measurement described by a collection $\{P_j\}$, the following happens: (i) the result of the measurement is j with probability $\|P_j|\psi\rangle\|^2$ for each j, and (ii) the superposition of the system is changed to $(1/\|P_j|\psi\rangle\|)P_j|\psi\rangle$ for whichever j was the result of the measurement.

Now we may define 2qcfa's more precisely. A two-way finite automaton with quantum and classical states is specified by a 9-tuple

$$M = (Q, S, \Sigma, \Theta, \delta, q_0, s_0, S_{\mathrm{acc}}, S_{\mathrm{rej}}),$$

where Q and S are finite state sets (quantum states and classical states, respectively), Σ is a finite alphabet, Θ and δ are functions described below that specify the behavior of M, $q_0 \in Q$ is the initial quantum state, $s_0 \in S$ is the initial classical state, and $S_{\mathrm{acc}}, S_{\mathrm{rej}} \subseteq S$ are the sets of (classical) accepting states and rejecting states, respectively. We let $\Gamma = \Sigma \cup \{¢, \$\}$ be the tape alphabet of M, where $¢ \notin \Sigma$ is called the left end-marker and $\$ \notin \Sigma$ is called the right end-marker.

The function Θ specifies the evolution of the quantum portion of the internal state: for each pair $(s, \sigma) \in S \backslash (S_{\mathrm{acc}} \cup S_{\mathrm{rej}}) \times \Gamma$, $\Theta(s, \sigma)$ is an action to be performed on the quantum portion of the internal state of M. Each action $\Theta(s, \sigma)$ corresponds to either a unitary transformation or an orthogonal measurement.

The function δ specifies the evolution of the classical part of M (i.e., the classical part of the internal state and the tape head). In case $\Theta(s, \sigma)$ is a unitary transformation, $\delta(s, \sigma)$ is an element of $S \times \{-1, 0, 1\}$ specifying a new classical state and a movement of the tape head. In case $\Theta(s,\sigma)$ is a measurement, $\delta(s,\sigma)$ is a mapping from the set of possible results of the measurement to $S \times \{-1,0,1\}$ (again specifying a new classical state and a tape head movement, this time one such pair for each outcome of the observation). It is assumed that δ is defined so that the tape head never moves left when scanning the left end-marker ¢, and never moves right when scanning the right end-marker \$.

On a given input x, a 2qcfa M is to operate as follows. Initially, the classical part of M's internal state is in state s_0, the quantum part of the internal state is in superposition $|q_0\rangle$, and the tape head of M is scanning the tape square indexed by 0. The tape squares indexed by $1,\ldots,|x|=n$ contain $x_1,\ldots,x_n$, while the squares indexed by 0 and $n+1$ contain end-markers ¢ and \$, respectively. On each step, the quantum part of the internal state is first changed according to $\Theta(s,\sigma)$, where s is the current classical internal state and σ is the currently scanned tape symbol, and then the classical internal state and tape head position are changed according to $\delta(s,\sigma)$ (along with the particular result obtained from $\Theta(s,\sigma)$ in case $\Theta(s,\sigma)$ is a measurement).

Since the results obtained from each measurement $\Theta(s,\sigma)$ are probabilistic, the transitions among the classical parts of a given 2qcfa may be probabilistic as well. For each input x, we may define a probability $p_{\mathrm{acc}}(x)$ that a given 2qcfa M eventually enters a classical accepting state, and a probability $p_{\mathrm{rej}}(x)$ that M eventually enters a rejecting state. A given computation is assumed to halt when either an accepting or rejecting classical state is reached, so the above events are mutually exclusive. We say that a given machine M recognizes a language $L \subseteq \Sigma^*$ with one-sided error ε if for all $x \in \Sigma^*$ we have $p_{\mathrm{acc}}(x)+p_{\mathrm{rej}}(x)=1$, $p_{\mathrm{acc}}(x)=1$ if $x \in L$, and $p_{\mathrm{rej}}(x) \geqslant 1-\varepsilon$ if $x \notin L$. Other notions of recognition such as two-sided error, zero error, etc., may be defined analogously, but we will only consider one-sided error in this paper.

A natural extension of our model is to allow POVM-type measurements (see [20], for instance) rather than orthogonal measurements. In fact, this does not change the power of the model since POVM-type measurements may be simulated by orthogonal measurements and unitary operators on (possibly) larger quantum systems. It may be the case that one may reduce the number of states required for various tasks using POVMs, although it is questionable whether this has any physical significance.

3. Recognizing palindromes

In this section we prove that 2qcfa's can recognize palindromes with any fixed error bound $\varepsilon > 0$, which is an impossible task for classical probabilistic 2-way finite automata. We first define a 2qcfa for this language that uses a quantum register having three orthogonal states, since this is easier to describe than the two orthogonal state (i.e., single qubit) case. Once we have this, it is simple to modify the 2qcfa so that it requires a single qubit register, due to the fact that the three orthogonal state machine uses only real amplitudes, along with the fact that there is a natural mapping from the unit sphere in real three-dimensional Euclidean space to the unit sphere in a two-dimensional complex Hilbert space.

Theorem 1. *For any $\varepsilon > 0$ there exists a* 2qcfa *M operating as follows. For any input $x \in \{a, b\}^*$, if x is a palindrome then M accepts x with certainty, and if x is not a palindrome then M accepts x with probability at most ε and rejects x otherwise.*

In order to prove Theorem 1, we consider the 3×3 integer matrices A and B, defined as follows:

$$A = \begin{pmatrix} 4 & 3 & 0 \\ -3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & 4 \end{pmatrix}. \tag{1}$$

Also define a function $f : \mathbb{Z}^3 \to \mathbb{Z}$ as

$$f(u) = 4u[1] + 3u[2] + 3u[3]$$

for each $u \in \mathbb{Z}^3$, and define a set $K \subseteq \mathbb{Z}^3$ as

$$K = \{u \in \mathbb{Z}^3\colon\ u[1] \not\equiv 0 \pmod 5,\ \ f(u) \not\equiv 0 \pmod 5 \\ \text{and } u[2] \cdot u[3] \equiv 0 \pmod 5\}.$$

Lemma 2. *If $u \in K$, then $Au \in K$ and $Bu \in K$.*

Proof. We show that $u \in K$ implies $Au \in K$; the proof for $Bu \in K$ is similar. Write $u = (a, b, c)^{\mathrm{T}}$, so that $Au = (4a + 3b, -3a + 4b, 5c)^{\mathrm{T}}$. We immediately see $(Au)[2] \cdot (Au)[3] \equiv 0 \pmod 5$, so it remains to show $(Au)[1] \not\equiv 0 \pmod 5$ and $f(Au) \not\equiv 0 \pmod 5$. Since $u \in K$, we have

$$a \not\equiv 0 \pmod 5, \tag{2}$$

$$f(u) = 4a + 3b + 3c \not\equiv 0 \pmod 5 \tag{3}$$

and either $b \equiv 0 \pmod 5$ or $c \equiv 0 \pmod 5$.

Suppose first that $b \equiv 0 \pmod 5$. Then we have $(Au)[1] \equiv 4a \pmod 5$ and

$$f(Au) = 4(4a + 3b) + 3(-3a + 4b) + 3(5c) \equiv 2a \pmod 5.$$

Thus $(Au)[1] \not\equiv 0 \pmod 5$ and $f(Au) \not\equiv 0 \pmod 5$ by (2).

Now suppose $c \equiv 0 \pmod 5$. Then

$$\begin{aligned}(Au)[1] &= 4a + 3b \\ &\equiv 4a + 3b + 3c \pmod 5 \\ &\equiv f(u) \pmod 5\end{aligned}$$

and

$$\begin{aligned} f(Au) &= 4(4a+3b)+3(-3a+4b)+3(5c) \\ &\equiv 2a+4b \pmod 5 \\ &\equiv 3(4a+3b+3c) \pmod 5 \\ &\equiv 3f(u) \pmod 5, \end{aligned}$$

so that $(Au)[1] \not\equiv 0 \pmod 5$ and $f(Au) \not\equiv 0 \pmod 5$ by (3), which completes the proof. □

Lemma 3. *Let $u \in \mathbb{Z}^3$ satisfy $u = Av = Bw$ for $v, w \in \mathbb{Z}^3$. Then $u \notin K$.*

Proof. Assume $u = Av = Bw$ for $u, v, w \in \mathbb{Z}^3$, so that $A^{-1}u, B^{-1}u \in \mathbb{Z}^3$. Since $(B^{-1}u)[2] \in \mathbb{Z}$ we conclude $u[2] \equiv 0 \pmod 5$, and since $(A^{-1}u)[1] \in \mathbb{Z}$ we conclude $4u[1] - 3u[2] \equiv 0 \pmod{25}$. Together these congruences imply $u[1] \equiv 0 \pmod 5$, and hence $u \notin K$. □

Lemma 4. *Let*

$$u = Y_1^{-1} \cdots Y_n^{-1} X_n \cdots X_1 (1,0,0)^{\mathrm{T}},$$

where $X_j, Y_j \in \{A, B\}$. If $X_j = Y_j$ for $1 \leqslant j \leqslant n$, then $u[2]^2 + u[3]^2 = 0$. Otherwise, $u[2]^2 + u[3]^2 > 25^{-n}$.

Proof. If $X_j = Y_j$ for $1 \leqslant j \leqslant n$, then we clearly have $u = (1,0,0)^{\mathrm{T}}$, and thus $u[2]^2 + u[3]^2 = 0$.

Next suppose there exists j such that $X_j \neq Y_j$. Note that $\|u\| = 1$, since $5^{-1}X_j$ and $5Y_j^{-1}$ are unitary for each j, and further note that $25^n u$ is integer valued. To prove the lemma it therefore suffices to prove $u \neq \pm(1,0,0)^{\mathrm{T}}$, since $|u[1]| < 1$ implies $|u[1]| \leqslant 1 - 25^{-n}$, and therefore

$$u[2]^2 + u[3]^2 = 1 - u[1]^2 \geqslant 1 - (1 - 25^{-n})^2 > 25^{-n}.$$

Let k be the largest index such that $X_k \neq Y_k$, and without loss of generality suppose $X_k = A$, $Y_k = B$. Write $v = X_{k-1} \cdots X_1 (1,0,0)^{\mathrm{T}}$ and $w = Y_{k-1} \cdots Y_1 (1,0,0)^{\mathrm{T}}$. Since $(1,0,0)^{\mathrm{T}} \in K$, we must have $Av, Bw \in K$ by Lemma 2. By Lemma 3 this implies $Av \neq Bw$, since $Av = Bw$ contradicts the fact that $Av, Bw \in K$. Since $X_j = Y_j$ for $j > k$, we therefore have $Y_n \cdots Y_1 (1,0,0)^{\mathrm{T}} \neq X_n \cdots X_1 (1,0,0)^{\mathrm{T}}$ and thus $u = Y_1^{-1} \cdots Y_n^{-1} X_n \cdots X_1 (1,0,0)^{\mathrm{T}} \neq (1,0,0)^{\mathrm{T}}$. By similar reasoning, $u \neq (-1,0,0)^{\mathrm{T}}$ since $(-1,0,0)^{\mathrm{T}} \in K$ and hence $Y_n \cdots Y_1 (-1,0,0)^{\mathrm{T}} \neq X_n \cdots X_1 (1,0,0)^{\mathrm{T}}$. □

Proof of Theorem 1. Define U_a and U_b to be unitary operators as follows:

$$U_a|q_0\rangle = \tfrac{4}{5}|q_0\rangle - \tfrac{3}{5}|q_1\rangle, \quad U_b|q_0\rangle = \tfrac{4}{5}|q_0\rangle - \tfrac{3}{5}|q_2\rangle,$$

```
Repeat ad infinitum:
  Move the tape head to the first input symbol and set the quantum state to $|q_0\rangle$.
  While the currently scanned symbol is not \$, do the following: (I)
    Perform $U_\sigma$ on the quantum state, for $\sigma$ denoting the currently scanned symbol.
    Move the tape head one square to the right.
  Move the tape head left until the ¢ symbol is reached.
  Move the tape head one square to the right.
  While the currently scanned symbol is not \$, do the following: (II)
    Perform $U_\sigma^{-1}$ on the quantum state, for $\sigma$ denoting the currently scanned symbol.
    Move the tape head one square to the right.
  Measure the quantum state: if the result is not $q_0$ then reject.
  Set $b = 0$.
  While the currently scanned symbol is not ¢, do the following: (III)
    Simulate $k$ coin-flips. Set $b = 1$ in case all results are not "heads".
    Move the tape head one square to the left.
  If $b = 0$, accept.
```

Fig. 1. A 2qcfa for palindromes.

$$U_a|q_1\rangle = \tfrac{3}{5}|q_0\rangle + \tfrac{4}{5}|q_1\rangle, \quad U_b|q_1\rangle = |q_1\rangle,$$

$$U_a|q_2\rangle = |q_2\rangle, \quad U_b|q_2\rangle = \tfrac{3}{5}|q_0\rangle + \tfrac{4}{5}|q_2\rangle$$

and define M to be a 2qcfa as described in Fig. 1. The parameter k will be specified below according to the error bound ε.

The action of M on input $x = x_1 x_2 \cdots x_n$ is as follows. The machine starts with its quantum state in superposition $|q_0\rangle$. As while-loop (I) is executed, the tape head moves over each input symbol and performs either the transformation U_a or U_b on the quantum state (depending on whether the symbol scanned is a or b). Letting X_j denote the matrix A or B, as defined in (1), depending on whether x_j is a or b, we see that the superposition of the quantum state of M after performing loop (I) is

$$\alpha_0|q_0\rangle + \alpha_1|q_1\rangle + \alpha_2|q_2\rangle$$

for $(\alpha_0, \alpha_1, \alpha_2)^{\mathrm{T}} = 5^{-n} X_n \cdots X_1 (1,0,0)^{\mathrm{T}}$. At this point, the tape head is moved back to the first input symbol and while-loop (II) is performed. A process similar to while-loop (I) is performed (except the inverses of U_a and U_b are applied instead of U_a and U_b), yielding superposition

$$\beta_0|q_0\rangle + \beta_1|q_1\rangle + \beta_2|q_2\rangle$$

for $(\beta_0, \beta_1, \beta_2)^{\mathrm{T}} = X_n^{-1} \cdots X_1^{-1} X_n \cdots X_1 (1,0,0)^{\mathrm{T}}$. Now the quantum state is measured: M rejects with probability $p_{\mathrm{rej}} = \beta_1^2 + \beta_2^2$, and otherwise the quantum state collapses to $|q_0\rangle$ with probability β_0^2. By Lemma 4 we conclude $p_{\mathrm{rej}} = 0$ in case x is a palindrome, and $p_{\mathrm{rej}} > 25^{-n}$ otherwise. Finally, M sets the variable b (stored in its classical internal state) to 0, executes while-loop (III), and accepts if the while-loop terminates with b still set to 0; it may be checked that this happens with probability $p_{\mathrm{acc}} = 2^{-k(n+1)}$.

This sequence of steps is repeated indefinitely, causing M to eventually reject with probability

$$\sum_{j\geqslant 0}(1-p_{\mathrm{acc}})^j(1-p_{\mathrm{rej}})^j p_{\mathrm{rej}} = \frac{p_{\mathrm{rej}}}{p_{\mathrm{acc}}+p_{\mathrm{rej}}-p_{\mathrm{acc}}p_{\mathrm{rej}}}$$

and accept with probability

$$\sum_{j\geqslant 0}(1-p_{\mathrm{acc}})^j(1-p_{\mathrm{rej}})^{j+1} p_{\mathrm{acc}} = \frac{p_{\mathrm{acc}}-p_{\mathrm{acc}}p_{\mathrm{rej}}}{p_{\mathrm{acc}}+p_{\mathrm{rej}}-p_{\mathrm{acc}}p_{\mathrm{rej}}}.$$

These probabilities clearly sum to 1, and the probability of acceptance is therefore 1 in case x is a palindrome. Letting $k\geqslant \max\{\log 25, -\log\varepsilon\}$, we see that if x is not a palindrome, then M rejects with probability at least $1-\varepsilon$, which completes the proof. □

We now outline how this 2qcfa may be modified so that a only single qubit is used. Define a mapping Φ from the unit sphere in $\mathbb{R}^3$ to the unit sphere in $\mathbb{C}^2$ as follows:

$$\begin{aligned}&\Phi(\cos\phi|q_0\rangle + \sin\phi\sin\psi|q_1\rangle + \sin\phi\cos\psi|q_2\rangle)\\ &\quad = \mathrm{e}^{-\mathrm{i}\psi/2}\cos\frac{\phi}{2}\,|0\rangle + \mathrm{e}^{\mathrm{i}\psi/2}\sin\frac{\phi}{2}|1\rangle\end{aligned}$$

and define

$$\begin{aligned}&\hat{U}_a|0\rangle = \cos\frac{\theta}{2}\,|0\rangle - \mathrm{i}\sin\frac{\theta}{2}|1\rangle, \quad \hat{U}_b|0\rangle = \cos\frac{\theta}{2}\,|0\rangle + \sin\frac{\theta}{2}|1\rangle,\\ &\hat{U}_a|1\rangle = -\mathrm{i}\sin\frac{\theta}{2}\,|0\rangle + \cos\frac{\theta}{2}|1\rangle, \quad \hat{U}_b|1\rangle = -\sin\frac{\theta}{2}\,|0\rangle + \cos\frac{\theta}{2}|1\rangle\end{aligned}$$

for $\theta = \tan^{-1}(4/3)$. It may be verified that the following relations hold:

$$\begin{aligned}&\hat{U}_a\Phi(\alpha_0|q_0\rangle + \alpha_1|q_1\rangle + \alpha_2|q_2\rangle) = \mathrm{e}^{\mathrm{i}\phi}\Phi(U_a(\alpha_0|q_0\rangle + \alpha_1|q_1\rangle + \alpha_2|q_2\rangle)),\\ &\hat{U}_b\Phi(\alpha_0|q_0\rangle + \alpha_1|q_1\rangle + \alpha_2|q_2\rangle) = \mathrm{e}^{\mathrm{i}\phi}\Phi(U_b(\alpha_0|q_0\rangle + \alpha_1|q_1\rangle + \alpha_2|q_2\rangle)),\end{aligned}$$

where $\mathrm{e}^{\mathrm{i}\phi}$ represents a phase factor (possibly depending on α_0, α_1, and α_2) that will not affect the operation of the machine. The proof of this claim follows from a much more general relationship between rigid rotations in three dimensions and unitary transformations in two dimensions; see, for instance, [16] for further discussion. (See also Section 2.3.2 in [20].) Note here that we have exchanged the x and z coordinates from the mappings described in these references in order to allow the observations to function correctly. Clearly, we have that an observation of the state $\Phi(|q_0\rangle)$ (in the $\{|0\rangle,|1\rangle\}$ basis) yields $|0\rangle$ with probability 1, and an observation of $\Phi(\alpha_0|q_0\rangle + \alpha_1|q_1\rangle + \alpha_2|q_2\rangle)$ yields $|1\rangle$ with probability at least $(1-\sqrt{1-\delta})/2\geqslant\delta/4$ in case $\alpha_1^2+\alpha_2^2\geqslant\delta$. Thus, by substituting transformation $\hat{U}_a$ for U_a, $\hat{U}_b$ for U_b, adjusting k as necessary, and letting

$|0\rangle$ be the initial state of the quantum register in the machine constructed above, we obtain a 2qcfa for palindromes that uses a single qubit.

4. Recognizing $a^n b^n$

The second language that we consider is $\{a^n b^n \,|\, n \in \mathbb{N}\}$. It is nonregular but can be recognized by a 2-way probabilistic finite automaton [9]. However, any 2-way probabilistic automaton recognizing it runs in exponential expected time [10]. (More generally, a similar result is true for 2-way probabilistic automata recognizing any nonregular language [6,13].)

In the quantum world, this language can be recognized by a 2qfa [15]. However, this 2qfa uses superpositions where the head of the qfa is in different places for different components of the superposition and, therefore, cannot be implemented with a quantum part of finite size. In this paper, we show that this language can be also recognized by a 2qcfa in polynomial time.

Theorem 5. *For any $\varepsilon > 0$, there is a 2qcfa M that accepts any $x \in \{a^n b^n \,|\, n \in \mathbb{N}\}$ with certainty, rejects $x \notin \{a^n b^n \,|\, n \in \mathbb{N}\}$ with probability at least $1 - \varepsilon$ and halts in expected time $\mathrm{O}(m^4)$ where m is the length of the word x.*

Proof. The main idea is as follows:

We consider a qcfa M with 2 quantum states $|q_0\rangle$ and $|q_1\rangle$. M starts in the state $|q_0\rangle$. Every time when M reads a, the state is rotated by angle $\alpha = \sqrt{2}\pi$ and every time when M reads b, the state is rotated by $-\alpha$. When the end of the word is reached, M measures the state. If it is $|q_1\rangle$, the word is rejected. Otherwise, the whole process is repeated.

If the number of a's is equal to the number of b's, rotations cancel one another and the final state is q_0. Otherwise, the final state is different from q_0 because $\sqrt{2}$ is irrational. Moreover, the amplitude of q_1 in the final state is sufficiently large.[1] Therefore, repeating the above process $\mathrm{O}(n^2)$ times guarantees getting q_1 at least once (and rejecting the input) with a high probability.

We also need that M halts on inputs $x \in \{a^n b^n \,|\, n \in \mathbb{N}\}$ (instead of repeating the above process forever). To achieve this, we periodically execute a subroutine that accepts with a small probability c/n^2. If the word is not in language, this does not have much influence because this probability is much smaller than the probability of getting q_1 in one run. The resulting automaton is described in Fig. 2.

Next, we show that this automaton recognizes $\{a^n b^n \,|\, n \in \mathbb{N}\}$. It is enough to consider its action on words of form $a^n b^{n'}$ (because all other words are rejected by it at the very beginning). We start with two lemmas that bound the probabilities of accepting after loop (I) and rejecting after loop (II).

[1] This relies on a property of $\sqrt{2}$ and is not true for an arbitrary irrational number instead of $\sqrt{2}$.

```
Check (classically) whether the input is of form $a^*b^*$. If not, reject.
Otherwise, repeat ad infinitum:
  Move the tape head to the first input symbol and set the quantum state to $|q_0\rangle$.
  While the currently scanned symbol is not $, do the following:      (I)
    If the currently scanned symbol is $a$, perform $U_\alpha$ on the quantum state.
    If the currently scanned symbol is $b$, perform $U_{-\alpha}$ on the quantum state.
    Move the tape head one square to the right.
  Measure the quantum state. If the result is not $q_0$, reject.
  Two times repeat:              (II)
    Move the tape head to the first input symbol
    Move the tape head one square to the right.
    While the currently scanned symbol is not ¢ or $, do the following:     (III)
      Simulate a coin flip. If the result is "heads", move right. Otherwise, move left.
  If both times the process ends at the right end-marker $, do:
    Simulate $k$ coin-flips. If all results are not "heads", accept.
```

Fig. 2. A 2qcfa for a^nb^n.

Lemma 6. *If the input is* $x=a^nb^{n'}$ *and* $n'\neq n$, M *rejects after loop* (*I*) *with probability at least* $1/2(n-n')^2$.

Proof. In this case, the state $|q_0\rangle$ gets rotated by $\sqrt{2}(n-n')\pi$. The superposition after rotating $|q_0\rangle$ by $\sqrt{2}(n-n')\pi$ is

$$\cos(\sqrt{2}(n-n')\pi)|q_0\rangle+\sin(\sqrt{2}(n-n')\pi)|q_1\rangle.$$

The probability of observing $|q_1\rangle$ is $\sin^2(\sqrt{2}(n-n')\pi)$. We bound this probability from below.

Let k be the closest integer to $\sqrt{2}(n-n')$. Assume that $\sqrt{2}(n-n')>k$. (The other case is symmetric.) Then, $k\leqslant\sqrt{2(n-n')^2-1}$ (because k^2 is integer and $2(n-n')^2-1$ is the largest integer that is smaller than $(\sqrt{2}(n-n'))^2$). We have

$$\begin{aligned}
&(\sqrt{2}(n-n')-\sqrt{2(n-n')^2-1})(\sqrt{2}(n-n')+\sqrt{2(n-n')^2-1})\\
&\quad=2(n-n')^2-2(n-n')^2+1=1,\\
&\sqrt{2}(n-n')-k\geqslant\sqrt{2}(n-n')-\sqrt{2(n-n')^2-1}\\
&\quad=\frac{1}{\sqrt{2}(n-n')+\sqrt{2(n-n')^2-1}}>\frac{1}{2\sqrt{2}(n-n')}.
\end{aligned}$$

We have $0<\sqrt{2}(n-n')-k<1/2$ (because k is the closest integer). For any $x\in[0,1/2]$, $\sin(x\pi)\geqslant 2x$ (because this is true for $x=0$ and $1/2$ and sin is concave in this interval). Therefore,

$$\sin^2(\sqrt{2}(n-n')\pi) = \sin^2((\sqrt{2}(n-n')-k)\pi) \geqslant 4(\sqrt{2}(n-n')-k)^2$$

$$\geqslant 4\left(\frac{1}{2\sqrt{2}(n-n')}\right)^2 = \frac{1}{2(n-n')^2}. \qquad \square$$

Lemma 7. *Each execution of* (*II*) *leads to acceptance with probability* $1/2^k(n+n'+1)^2$.

Proof. Each loop (III) is just a random walk starting at location 1 (the first symbol of $a^nb^{n'}$) and ending either at location 0 (the left end-marker ¢) or at location $n+n'+1$ (the right end-marker \$). It is a standard result in probability theory (see [8, Chapter 14.2]) that the probability of reaching the location $n+n'+1$ is exactly $1/(n+n'+1)$. Repeating it twice and flipping k coins afterwards gives the probability $1/2^k(n+n'+1)^2$. □

We select $k = 1 + \lceil \log \varepsilon \rceil$. If $x = a^nb^n$, then the loop (I) always returns $|q_0\rangle$ to $|q_0\rangle$ and M never rejects. The probability of M accepting after cn^2 executions of (II) is

$$1 - \left(1 - \frac{1}{2^k(n+n'+1)^2}\right)^{cn^2}$$

and this can be made arbitrarily close to 1 by selecting an appropriate constant c.

On the other hand, if $x = a^nb^{n'}$ and $n \neq n'$, M rejects after (I) with probability $p_{\rm rej} > 1/2(n-n')^2$ and accepts after (II) with probability $p_{\rm acc}1/2^k(n+n'+1)^2 \leqslant \varepsilon/2(n+n'+1)^2$. If this is repeated indefinitely, the probability of rejecting is

$$\sum_{k\geqslant 0}(1-p_{\rm acc})^k(1-p_{\rm rej})^k p_{\rm rej} = \frac{p_{\rm rej}}{p_{\rm acc}+p_{\rm rej}-p_{\rm acc}p_{\rm rej}}$$

$$> \frac{p_{\rm rej}}{p_{\rm acc}+p_{\rm rej}} > \frac{1/2}{1/2+\varepsilon/2} = \frac{1}{1+\varepsilon} > 1-\varepsilon.$$

In both cases, the expected number of iterations of (I) and (II) before M accepts or rejects is $O((n+n')^2)$ (because, in every iteration, M accepts or rejects with probability at least $c/(n+n')^2$). Loop (I) takes $O(n+n')$ time and each random walk in (II) takes $O((n+n')^2)$ time. Hence, the expected running time of M is at most $O((n+n')^4)$. □

5. Conclusion

In this paper, we have introduced 2-way finite automata with quantum and classical states, and given two examples of languages for which 2qcfa's outperform classical probabilistic 2-way finite automata: $L_{\rm pal} = \{x \in \{a,b\}^* \mid x = x^R\}$ and $L_{\rm eq} = \{a^nb^n \mid n \in \mathbb{N}\}$. It is natural to ask what other languages can be recognized by 2qcfa's. For instance, can any of the following languages be recognized by 2qcfa's?

$$L_{\text{middle}} = \{xay \,|\, x, y \in \{a,b\}^*, |x| = |y|\}.$$

$$L_{\text{balanced}} = \{x \in \{(,)\}^* \,|\, \text{parentheses in } x \text{ are balanced}\}.$$

$$L_{\text{square}} = \{a^n b^{n^2} \,|\, n \in \mathbb{N}\}.$$

$$L_{\text{power}} = \{a^n b^{2^n} \,|\, n \in \mathbb{N}\}.$$

If so, can any of these languages be recognized by polynomial time 2qcfa's?

References

[1] D. Aharonov, A. Kitaev, N. Nisan, Quantum circuits with mixed states, in: Proc. 30th Annu. ACM Symp. on Theory of Computing, Dallas, Texas, 1998, pp. 20–30.

[2] A. Ambainis, R. Freivalds, 1-way quantum finite automata: strengths, weaknesses and generalizations, in: Proc. 39th Annu. Symp. on Foundations of Computer Science, Palo Alfo, California, 1998, pp. 332–341.

[3] A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in: Proc. 31st Annu. ACM Symp. on Theory of Computing, Atlanta, Georgia, 1999, pp. 376–383.

[4] A. Berthiaume, Quantum computation, in: L. Hemaspaandra, A. Selman (Eds.), Complexity Theory Retrospective, Vol. II, Springer, Berlin, 1997, pp. 23–50.

[5] A. Brodsky, N. Pippenger, Characterizations of 1-way quantum finite automata, Los Alamos Preprint Archive, quant-ph/9903014, 1999.

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

[7] C. Dwork, L. Stockmeyer, Finite state verifiers I: the power of interaction, J. ACM 39 (4) (1992) 800–828.

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

[9] R. Freivalds, Probabilistic two-way machines, in: Proc. Internat. Symp. on Mathematical Foundations of Computer Science, Strbske Pleso, Lecture Notes in Computer Science, Vol. 188, Springer, Berlin, 1981, pp. 33–45.

[10] A. Greenberg, A. Weiss, A lower bound for probabilistic algorithms for finite state machines, J. Comput. System Sci. 33 (1) (1986) 88–105.

[11] L. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th Annu. ACM Symp. on Theory of Computing, Philadelphia, Pennsylvania, 1996, pp. 212–219.

[12] A. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Problemy Peredachi Informatsii 9 (3) (1973) 3–11, Prob. Inform. Transmission 9 (1973) (in English).

[13] J. Kaņeps, R. Freivalds, Running time to recognize nonregular languages by 2-way probabilistic automata, in: Proc. 18th Internat. Colloq. on Automata, Languages and Programming, Gosen, Lecture Notes in Computer Science, Vol. 510, Springer, Berlin, 1991, pp. 174–185.

[14] A. Kitaev, Quantum computations: algorithms and error correction, Russian Math. Surveys 52 (6) (1997) 1191–1249.

[15] A. Kondacs, J. Watrous, On the power of quantum finite state automata, in: Proc. 38th Annu. Symp. on Foundations of Computer Science, Miami, Florida, 1997, pp. 66–75.

[16] J. Mathews, R. Walker, Mathematical Methods of Physics, 2nd Edition, Benjamin, New York, 1970.

[17] C. Moore, J. Crutchfield, Quantum automata and quantum grammars, Theoret. Comput. Sci. 237 (2) (2000) 275–306; Los Alamos Preprint Archive, quant-ph/9707031, 1997.

[18] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in: Proc. 40th Annu. Symp. on Foundations of Computer Science, 1999, pp. 369–377; Los Alamos Preprint Archive, quant-ph/9904093, 1999.

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

[20] J. Preskill, Quantum information and computation, Lecture Notes for Physics, Vol. 229, California Institute of Technology, 1998; Available at http://theory.caltech.edu/people/preskill/ph229.

[21] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (5) (1997) 1484–1509.