Succinctness of two-way probabilistic and quantum finite automata

Abuzer Yakaryilmaz, A. C. Cem Say

Discrete Mathematics and Theoretical Computer Science DMTCS vol. **12:4**, 2010, 19–40

Succinctness of two-way probabilistic and quantum finite automata[†‡]

Abuzer Yakaryılmaz and A.C. Cem Say

Boğaziçi University, Department of Computer Engineering, Bebek 34342 İstanbul, Turkey
{abuzer,say}@boun.edu.tr

received 31st October 2009, accepted 1st June 2010.

We introduce a new model of two-way finite automaton, which is endowed with the capability of resetting the position of the tape head to the left end of the tape in a single move during the computation. Several variants of this model are examined, with the following results: The weakest known model of computation where quantum computers recognize more languages with bounded error than their classical counterparts is identified. We prove that two-way probabilistic and quantum finite automata (2PFAs and 2QFAs) can be considerably more concise than both their one-way versions (1PFAs and 1QFAs), and two-way nondeterministic finite automata (2NFAs). For this purpose, we demonstrate several infinite families of regular languages which can be recognized with some fixed probability greater than $\frac{1}{2}$ by just tuning the transition amplitudes of a 2QFA (and, in one case, a 2PFA) with a constant number of states, whereas the sizes of the corresponding 1PFAs, 1QFAs and 2NFAs grow without bound. We also show that 2QFAs with mixed states can support highly efficient probability amplification.

Keywords: quantum and probabilistic automata, succinctness, probability amplification

1 Introduction

In recent years, the research effort on quantum versions of finite automata has mainly focused on one-way models, with the study of two-way quantum finite automata (2QFAs), which are synonymous with constant space quantum Turing machines, receiving relatively less attention. In their seminal paper, Kondacs and Watrous [KW97] proved that 2QFAs recognize all regular languages with zero error, and the language $L_{eq} = \{a^n b^n \mid n \geq 0\}$ with any desired error bound $\epsilon > 0$, in time $O(\frac{1}{\epsilon}|w|)$, using $O((\frac{1}{\epsilon})^2)$ states, where w is the input string. Since two-way probabilistic finite automata (2PFAs) can decide L_{eq} only in exponential time [Fre81, GW86, KF90, DS92], this established the superiority of 2QFAs over 2PFAs. Paralleling work by Aharonov et al. [AKN98] on quantum circuits with mixed states, Ambainis and Watrous [AW02] introduced an alternative model, the two-way finite automaton with quantum and

[†]A preliminary version of this paper was presented at the AutoMathA Plenary Conference 2009, in Liège, Belgium.

[‡]This work was partially supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) with grant 108142 and the Boğaziçi University Research Fund with grant 08A102.

classical states (2QCFA), which includes a constant-size quantum part which may be in a mixed state, but requires the tape head position to be classical. Yakaryılmaz and Say [YS09a] noted that conventional methods of probability amplification give significantly inefficient results when applied to 2QFAs, and presented methods which can be used to decide L_{eq} with error bound ϵ in as low as $O(|w|)$ steps (i.e. with runtime independent of ϵ), and with as low as $O(\log^2(\frac{1}{\epsilon})\log\log(\frac{1}{\epsilon}))$ states.

In this paper, we introduce a new model of two-way finite automaton, which is endowed with the capability of resetting the position of the tape head to the left end of the tape in a single move during the computation. A restricted quantum version of these machines, called the one–way quantum finite automaton with restart (1QFA$^{\circlearrowleft}$), which can switch only to the initial state during left resets, and cannot perform single-step left or stationary moves, is shown to be the weakest known model of computation where quantum computers recognize more languages with bounded error than their classical counterparts. The classical counterpart of the same version is compared with the standard 2PFA model.

We use this new model in the proofs of several facts about the properties of well-known models of probabilistic and quantum two-way finite automata. As our main result, we demonstrate several infinite families of regular languages which can be recognized with some fixed probability greater than $\frac{1}{2}$ by just tuning the transition amplitudes of a 2QFA (and, in one case, a 2PFA) with a constant number of states, whereas the sizes of the corresponding one-way machines, and two-way nondeterministic finite automata (2NFAs) grow without bound.

The Kondacs-Watrous model of quantum finite automaton (to be called, from now on, KWQFA), which allows measurements of a restricted type, rather than the full set sanctioned by quantum theory, has been proven to be weaker in terms of language recognition power [KW97], probability amplification capability [AF98], and, in some cases at least, succinctness [ANTSV02], than the corresponding classical model, in the one-way case. More general models, such as the 2QCFA, employing mixed states, are able to simulate the corresponding classical probabilistic automata efficiently in both the one-way and two-way settings, and to recognize some languages that 2PFAs cannot [AW02]. We show that 2QFAs with mixed states can support highly efficient probability amplification, surpassing the best known methods for 2KWQFAs recognizing these languages.

The rest of this paper is structured as follows: Section 2 contains the definitions and some basic facts about our new model that will be used throughout the paper. In Section 3, we prove some key lemmata about the relationship between one–way quantum finite automata with and without restart, and examine the class of languages recognized with bounded error by 1QFA$^{\circlearrowleft}$'s. Our main succinctness result is presented in Section 4. In Section 5, we present several algorithms that improve previous results about the efficiency of probability amplification in 2KWQFAs and 2QCFAs. In Section 6, we investigate the computational power of probabilistic finite automata with restart. Section 7 is a conclusion.

2 Preliminaries

Watrous [Wat97] notes that a 2KWQFA algorithm he presents for recognizing a nonregular language is remarkably costly in terms of probability amplification, and states that this problem stems from the fact that 2KWQFAs cannot "reset" themselves during execution to repeatedly carry out the same computation. The 2QCFA model provides one way of solving this problem, by having a classical part, in addition to the quantum register. We present an alternative 2QFA model, employing only quantum states, whose only difference from the 2KWQFA is the existence of an additional "reset move" in its repertory. Section 2.1 contains the definitions of this and the other models that will be examined in the paper. Section 2.2

describes some facts which will make the analyses of the algorithms in later sections easier.

2.1 Definitions

Let Σ be an input alphabet, not containing the end–marker symbols $\mathfrak{c}$ and \$, and let $\Gamma = \Sigma \cup \{\mathfrak{c}, \$\}$ be the tape alphabet.

A *2-way quantum finite automaton with reset* (2QFA$^{\circlearrowleft}$) is a 7-tuple

$$\mathcal{M} = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej}, Q_{reset} = \cup_{q \in Q_{non}} Q_q^{\circlearrowleft}), \tag{1}$$

where

1. $Q = \{q_0, \ldots, q_n\}$ is the finite set of states;
2. δ is the transition function, described below;
3. $q_0 \in Q$ is the initial state;
4. Q_{acc} is the set of accepting states;
5. Q_{rej} is the set of rejecting states;
6. $Q_{non} = Q \setminus (Q_{acc} \cup Q_{rej} \cup Q_{reset})$ is the set of nonhalting and nonresetting states;
7. Q_{reset} is the union of disjoint reset sets, i.e., each $Q_{q \in Q_{non}}^{\circlearrowleft}$ contains reset states that cause the computation to restart with state q, as described below.

We assume that the states in Q_{non} have smaller indices than other members of Q; $q_i \in Q_{non}$ for $0 \leq i < |Q_{non}|$.

The configurations of a 2QFA$^{\circlearrowleft}$ are pairs of the form $(state, head\ position)$. Initially, the head is on the left end-marker $\mathfrak{c}$, and so the machine starts computation in the superposition $|q_0, 0\rangle$.

The transition function of a 2QFA$^{\circlearrowleft}$ working on an input string $w \in \Sigma^*$, (that is, a tape containing $\mathsf{w} = \mathfrak{c}w\$$,) is required to induce a unitary operator U_δ^w on the Hilbert space $\ell_2(Q \times \mathbb{Z}_{|\mathsf{w}|})$, since quantum machines can exist in superpositions of more than one configuration.

In all 2QFA$^{\circlearrowleft}$'s described in this paper, every transition entering the same state involves the tape head moving in the same direction (left, right, or stationary). With this simplification, considering the Hilbert space $\ell_2(Q)$, a syntactically correct 2QFA$^{\circlearrowleft}$ (that is, one where U_δ^w is unitary for every w,) can be specified easily by just providing a unitary operator $\mathsf{U}_\sigma : \ell_2(Q) \to \ell_2(Q)$ for each symbol $\sigma \in \Gamma$. More formally,

$$\delta(q, \sigma, q', d_{q'}) = \langle q' | \mathsf{U}_\sigma | q \rangle \tag{2}$$

is the amplitude with which the machine currently in state q and scanning symbol σ will jump to state q' and move the head in direction $d_{q'}$. Here, $d_{q'} \in \{-1, 0, 1\}$ is the direction of the tape head determined by q'. For the remaining directions, all transitions with target q' have amplitude zero.

Apart from the left reset capability, 2QFA$^{\circlearrowleft}$'s are identical to 2KWQFAs. In the following, we focus on this new capability, and refer the reader to [KW97] for detailed coverage of the technical properties of 2KWQFAs.

In each step of its execution, a 2QFA$^{\circlearrowleft}$ undergoes two linear operations: The first one is a unitary transformation of the current superposition according to δ, and the second one is a measurement. The

observable describing this measurement process is designed so that the outcome of any observation is one of "accept", "reject", "continue without resetting", or "reset with state q", for any $q \in Q_{non}$. Formally, we use the observable $\mathcal{O}$, corresponding to the decomposition

$$E = E_{acc} \oplus E_{rej} \oplus E_{non} \oplus E_{reset-0} \oplus E_{reset-1} \oplus \cdots \oplus E_{reset-(k-1)}, \tag{3}$$

where $k = |Q_{non}|$, and for a given input w,

1. the set of all configurations of the 2QFA$^{\circlearrowleft}$ is $Q \times \mathbb{Z}_{|w|}$;
2. $E = \text{span}\{|c\rangle \mid c \in Q \times \mathbb{Z}_{|w|}\}$;
3. $E_{acc} = \text{span}\{|c\rangle \mid c \in Q_{acc} \times \mathbb{Z}_{|w|}\}$;
4. $E_{rej} = \text{span}\{|c\rangle \mid c \in Q_{rej} \times \mathbb{Z}_{|w|}\}$;
5. $E_{non} = \text{span}\{|c\rangle \mid c \in Q_{non} \times \mathbb{Z}_{|w|}\}$;
6. $E_{reset-i} = \text{span}\{|c\rangle \mid c \in Q^{\circlearrowleft}_{q_i \in Q_{non}} \times \mathbb{Z}_{|w|}\}$ $(0 \leq i \leq k-1)$.

The probability of each outcome is determined by the amplitudes of the relevant configurations in the present superposition. The contribution of each configuration to this probability is the modulus squared of its amplitude. For instance, the outcome "reset with state q_i" will be measured with probability $\sum_{c \in Q^{\circlearrowleft}_{q_i} \times \mathbb{Z}_{|w|}} |\alpha_c|^2$, where α_c is the amplitude of configuration c. If "accept" or "reject" is measured, the computation halts. If "continue without resetting" is measured, the machine continues running from a superposition of the nonhalting and nonresetting configurations, obtained by normalizing the projection of the superposition before the measurement onto $\text{span}\{|c\rangle | c \in Q_{non} \times \mathbb{Z}_{|w|}\}$. If "reset with state q_i" is measured, the tape head is reset to point to the left end-marker, and the machine continues from the superposition $|q_i, 0\rangle$ in the next step. Note that the decoherence associated with this measurement means that the system allows mixed states.

A 2QFA$^{\circlearrowleft}$ $\mathcal{M}$ is said to recognize a language L with error bounded by ϵ if $\mathcal{M}$'s computation results in "accept" being measured for all members of L with probability at least $1-\epsilon$, and "reject" being measured for all other inputs with probability at least $1-\epsilon$.

A *2-way quantum finite automaton with restart* (2QFA$^{\circlearrowleft}$) is a restricted 2QFA$^{\circlearrowleft}$ in which the "reset moves" can target only the original start state of the machine, that is, in terms of Equation 1, all the $Q^{\circlearrowleft}_q$ of a 2QFA$^{\circlearrowleft}$ are empty, with the exception of $Q^{\circlearrowleft}_{q_0}$, represented as $Q_{restart}$.

The *two-way probabilistic finite automaton* (2PFA) is the classical probabilistic counterpart of 2KWQFAs; see [Fre81, Kaņ91] for the details. A *one-way probabilistic finite automaton* (1PFA) [Rab63] is a 2PFA in which the head moves only to the right in every step. A *rational 1PFA* [Tur69] is a 1PFA where all entries in the transition matrices are rational numbers.

Other variants of two-way automata with reset that will be examined in this paper are

1. A *one-way (Kondacs-Watrous) quantum finite automaton with reset* (1QFA$^{\circlearrowleft}$) is a restricted 2QFA$^{\circlearrowleft}$ which uses neither "move one square to the left" nor "stay put" transitions, and whose tape head is therefore classical,
2. A *one-way (Kondacs-Watrous) quantum finite automaton with restart* (1QFA$^{\circlearrowleft}$) is a 1QFA$^{\circlearrowleft}$ where the reset moves can target only the original start state, and,

3. A *one-way probabilistic finite automaton with restart* (1PFA$^{\circlearrowleft}$) is a 1PFA which has been enhanced with the capability of resetting the tape head to the left end-marker and swapping to the original start state.

A *one-way (Kondacs-Watrous) quantum finite automaton* (1KWQFA) [KW97] is a 2KWQFA which moves its tape head only to the right in every step.

A well-known two-way mixed-state model is the 2QCFA [AW02]. Formally, a *2-way finite automaton with quantum and classical states* (2QCFA) is a 9-tuple

$$\mathcal{M} = (Q, S, \Sigma, \Theta, \delta, q_0, s_0, S_{acc}, S_{rej}), \tag{4}$$

where

1. $Q = \{q_0, \ldots, q_{n_1}\}$ is the finite set of the quantum states;
2. $S = \{s_0, \ldots, s_{n_2}\}$ is the finite set of the classical states;
3. Θ and δ govern the machine's behavior, as described below;
4. $q_0 \in Q$ is the initial quantum state;
5. $s_0 \in S$ is the initial classical state;
6. $S_{acc} \subset S$ is the set of classical accepting states;
7. $S_{rej} \subset S$ is the set of classical rejecting states.

The functions Θ and δ specify the evolution of the quantum and classical parts of $\mathcal{M}$, respectively. Both functions take the currently scanned symbol $\sigma \in \Gamma$ and current classical state $s \in S$ as arguments. $\Theta(s, \sigma)$ is either a unitary transformation, or an orthogonal measurement. In the first case, the new classical state and tape head direction (left, right, or stationary) are determined by δ, depending on s and σ. In the second case, when an orthogonal measurement is applied on the quantum part, δ determines the new classical state and the tape head direction using the result of that measurement, as well as s and σ. The quantum and classical parts are initialized with $|q_0\rangle$ and s_0, respectively, and the tape head starts on the first cell of the tape, on which $\mathbb{c}w\$$ is written for a given input string $w \in \Sigma^*$. During the computation, if an accepting or rejecting state is entered, the machine halts with the relevant response to the input string.

Note that like the 1QFA$^{\circlearrowleft}$, and unlike the 2QFA and the 2QFA$^{\circlearrowleft}$, the tape head position of a 2QCFA is classical, (that is, there are no superpositions with the head in more than one position simultaneously,) meaning that the machine can be implemented using a quantum part of constant size.

2.2 Basic facts

We start by stating some basic facts concerning automata with restart, which will be used in later sections.

A segment of computation which begins with a (re)start, and ends with a halting or restarting configuration will be called a *round*. Clearly, every automaton with restart which makes nontrivial use of its restarting capability will run for infinitely many rounds on some input strings. Throughout this paper, we make the assumption that our two-way automata do not contain infinite loops within a round, that is, the computation restarts or halts with probability 1 in a finite number steps for each round.

Everywhere in this section, $\mathcal{R}$ will stand for a finite state automaton with restart, and $w \in \Sigma^*$ will represent an input string using the alphabet Σ.

Definition 1

- $p_{acc}(\mathcal{R},w)$, $p_{rej}(\mathcal{R},w)$, *and* $p_{restart}(\mathcal{R},w)$ *denote the probabilities that* $\mathcal{R}$ *will accept, reject, or restart, respectively, on input* w*, in the first round.*
- $\mathsf{P_{acc}}(\mathcal{R},w)$ *and* $\mathsf{P_{rej}}(\mathcal{R},w)$ *denote the overall acceptance and rejection probabilities of* w *by* $\mathcal{R}$*, respectively.*

Moreover, $p_{halt}(\mathcal{R},w)=p_{acc}(\mathcal{R},w)+p_{rej}(\mathcal{R},w)$.

Lemma 1

$$\mathsf{P_{acc}}(\mathcal{R},w)=\frac{1}{1+\frac{p_{rej}(\mathcal{R},w)}{p_{acc}(\mathcal{R},w)}};\ \ \mathsf{P_{rej}}(\mathcal{R},\mathsf{w})=\frac{1}{1+\frac{p_{acc}(\mathcal{R},w)}{p_{rej}(\mathcal{R},w)}}. \tag{5}$$

Proof:

$$\begin{aligned}
\mathsf{P_{acc}}(\mathcal{R},w) &= \sum_{i=0}^{\infty}\left(1-p_{acc}(\mathcal{R},w)-p_{rej}(\mathcal{R},w)\right)^i p_{acc}(\mathcal{R},w)\\
&= p_{acc}(\mathcal{R},w)\left(\frac{1}{1-\left(1-p_{acc}(\mathcal{R},w)-p_{rej}(\mathcal{R},w)\right)}\right)\\
&= \frac{p_{acc}(\mathcal{R},w)}{p_{acc}(\mathcal{R},w)+p_{rej}(\mathcal{R},w)}\\
&= \frac{1}{1+\frac{p_{rej}(\mathcal{R},w)}{p_{acc}(\mathcal{R},w)}}.
\end{aligned}$$

$\mathsf{P_{rej}}(\mathcal{R},w)$ is calculated in the same way. □

Lemma 2 *The language* $L\subseteq\Sigma^*$ *is recognized by* $\mathcal{R}$ *with error bound* $\epsilon>0$ *if and only if* $\frac{p_{rej}(\mathcal{R},w)}{p_{acc}(\mathcal{R},w)}\leq\frac{\epsilon}{1-\epsilon}$ *when* $w\in L$*, and* $\frac{p_{acc}(\mathcal{R},w)}{p_{rej}(\mathcal{R},w)}\leq\frac{\epsilon}{1-\epsilon}$ *when* $w\notin L$*. Furthermore, if* $\frac{p_{rej}(\mathcal{R},w)}{p_{acc}(\mathcal{R},w)}$ $(\frac{p_{acc}(\mathcal{R},w)}{p_{rej}(\mathcal{R},w)})$ *is at most* ϵ*, then* $\mathsf{P_{acc}}(\mathcal{R},w)$ $(\mathsf{P_{rej}}(\mathcal{R},w))$ *is at least* $1-\epsilon$*.*

Proof: This follows from Lemma 1, since, for all $p\geq 0$, $\epsilon\in[0,\frac{1}{2})$,

$$\frac{1}{1+p}\geq 1-\epsilon\Leftrightarrow p\leq\frac{\epsilon}{1-\epsilon},\ \text{and} \tag{6}$$

$$p\leq\epsilon\Rightarrow\frac{1}{1+p}\geq 1-\epsilon. \tag{7}$$

□

Lemma 3 *Let* $p=p_{halt}(\mathcal{R},w)$*, and let* $s(w)$ *be the maximum number of steps in any branch of a round of* $\mathcal{R}$ *on* w*. The worst-case expected runtime of* $\mathcal{R}$ *on* w *is*

$$\frac{1}{p}(s(w)). \tag{8}$$

Proof: The worst-case expected running time of $\mathcal{R}$ on w is

$$\sum_{i=0}^{\infty}(i+1)(1-p)^i(p)(s(w)) = (p)(s(w))\frac{1}{p^2} = \frac{1}{p}(s(w)). \tag{9}$$

□

Lemma 4 *Any one-way automaton with restart with expected runtime t can be simulated by a corresponding two-way automaton without restart in expected time no more than $2t$.*

Proof: The program of the two-way machine ($\mathcal{R}_2$) is identical to that of the one-way machine with restart ($\mathcal{R}_1$), except for the fact that each restart move of $\mathcal{R}_1$ is imitated by $\mathcal{R}_2$ by moving the head one square per step all the way to the left end-marker. This causes the runtimes of the i nonhalting rounds in the summation in Equation (9) in Lemma 3 to increase by a factor of 2. □

We will now give a quick review of the technique of probability amplification. Suppose that we are given a machine (with or without reset) $\mathcal{A}$, which recognizes a language L with error bounded by ϵ, and we wish to construct another machine which recognizes L with a much smaller, but still positive, probability of error, say, ϵ'. It is well known[(i)] that one can achieve this by running $\mathcal{A}$ $O(\log(\frac{1}{\epsilon'}))$ times on the same input, and then giving the majority answer as our verdict about the membership of the input string in L.

Suppose that the original machine $\mathcal{A}$ needs to be run $2k+1$ times for the overall procedure to work with the desired correctness probability. Two counters can be used to count the acceptance and rejection responses, and the overall computation accepts (rejects) when the number of recorded acceptances (rejections) reaches $k+1$. To implement these counters in the finite automaton setting, we need to "connect" $(k+1)^2$ copies of $\mathcal{A}$, $\{\mathcal{A}_{i,j} \mid 0 \leq i,j \leq k\}$, where the subscripts indicate the values of the two counters, i.e., the states of $\mathcal{A}_{i,j}$ encode the information that $\mathcal{A}$ has accepted i times and rejected j times in its previous runs. The new machine $\mathcal{M}$ is constructed from the $\mathcal{A}_{i,j}$'s as follows:

- The start state of $\mathcal{M}$ is the start state of $\mathcal{A}_{0,0}$;
- Upon reaching any accept state of $\mathcal{A}_{i,j}$ ($0 \leq i,j < k$), $\mathcal{M}$ moves the head back to the left end-marker and then switches to the start state of $\mathcal{A}_{i+1,j}$;
- Upon reaching any reject states of $\mathcal{A}_{i,j}$ ($0 \leq i,j < k$), $\mathcal{M}$ moves the head back to the left end-marker and then switches to the start state of $\mathcal{A}_{i,j+1}$;
- The accept states of $\mathcal{M}$ are the accept states of $\mathcal{A}_{k,j}$ ($0 \leq j < k$);
- The reject states of $\mathcal{M}$ are the reject states of $\mathcal{A}_{i,k}$ ($0 \leq i < k$).

Lemma 5 *If language $L \subseteq \Sigma^*$ is recognized by $\mathcal{R}$ with a fixed error bound $\epsilon > 0$, then for any positive error bound $\epsilon' < \epsilon$, there exists a finite automaton with reset, $\mathcal{R}'$, recognizing L . Moreover, if $\mathcal{R}$ has n states and its (expected) runtime is $O(s(|w|))$, then $\mathcal{R}'$ has $O(\log^2(\frac{1}{\epsilon'})n)$ states, and its (expected) runtime is $O(\log(\frac{1}{\epsilon'})s(|w|))$, where w is the input string.*

(i) See, for instance, pages 369-370 of [Sip06].

Proof: Follows easily from the above description. □

Finally, we note the following relationship between the computational powers of the 2QCFA and the 1QFA$^{\circlearrowleft}$.

Lemma 6 *For any 1QFA$^{\circlearrowleft}$ $\mathcal{M}_1$ with n states and expected runtime $t(|w|)$, there exists a 2QCFA $\mathcal{M}_2$ with n quantum states, $O(n)$ classical states, and expected runtime $O(t(|w|))$, such that $\mathcal{M}_2$ accepts every input string w with the same probability that $\mathcal{M}_1$ accepts w.*

Proof: We utilize the 2QCFAs ability of making arbitrary orthogonal measurements. Given a 1QFA$^{\circlearrowleft}$ $\mathcal{M}_1$, we construct a 2QCFA $\mathcal{M}_2$ with the same set of quantum states. On each tape square, $\mathcal{M}_2$ first performs the unitary transformation associated with the current symbol by the program of $\mathcal{M}_1$. It then makes a measurement (over the space spanned by the set of quantum states) using an observable $\mathcal{O}'$, which is formed by replacing each subspace of the form $E_{reset-i}$ in the observable $\mathcal{O}$ (Equation 3) of $\mathcal{M}_1$[(ii)] by its subspaces

$$\{E_{reset-i-q_{i_1}} \oplus E_{reset-i-q_{i_2}} \oplus \cdots \oplus E_{reset-i-q_{i_m}}\},$$

where $\{q_{i_1}, q_{i_2}, \ldots, q_{i_m}\} = Q_{q_i}^{\circlearrowleft}$, and $E_{reset-i-q_{i_j}} = \text{span}\{|q_{i_j}\rangle\}$ $(1 \leq j \leq m)$. The outcome associated with $E_{reset-i-q_{i_j}}$ is simply the name of q_{i_j}.

$\mathcal{M}_2$ takes the action specified below according to the result of this observation:

1. "continue without resetting": move the head one square to the right,
2. "accept": accept,
3. "reject": reject,
4. "q_{i_j}": enter a classical state that moves the head left until the left end-marker ¢ is seen, and perform a unitary transformation that transforms the quantum register from state q_{i_j} to q_i.

□

3 Computational power of 1QFA$^{\circlearrowleft}$'s

In this section, we focus on the 1QFA$^{\circlearrowleft}$, which turns out to be the simplest and most restricted known model of quantum computation that is strictly superior in terms of bounded-error language recognition to its classical counterpart.

Our first result shows that 1QFA$^{\circlearrowleft}$'s can simulate any 1PFA$^{\circlearrowleft}$ with small state cost, albeit with great slowdown. Note that no such relation is known between the 2KWQFA and its classical counterpart, the 2PFA, in the bounded error case.

Theorem 1 *Any language $L \subseteq \Sigma^*$ recognized by an n-state 1PFA$^{\circlearrowleft}$ with error bound ϵ can be recognized by a $2n+4$-state 1QFA$^{\circlearrowleft}$ with the same error bound. Moreover, if the expected runtime of the 1PFA$^{\circlearrowleft}$ is $O(s(|w|))$, then the expected runtime of the 1QFA$^{\circlearrowleft}$ is $O(l^{2|w|}s^2(|w|))$ for a constant $l > 1$ depending on n, where w is the input string.*

(ii) Since the head is classical, the observable is redefined to be a decomposition of the space spanned by just the set of states.

Proof: Let $\mathcal{P}$ be an n-state 1PFA$^{\circlearrowleft}$ recognizing L with error bound ϵ. We will construct a $2n+4$-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}$ recognizing the same language with error bound $\epsilon' \leq \epsilon$.

By adding two more states, s_{acc} and s_{rej}, to $\mathcal{P}$, we obtain a new 1PFA$^{\circlearrowleft}$, $\mathcal{P}'$, where the halting of the computation in each round is postponed to the last symbol, \$, on which the overall accepting and rejecting probabilities are summed up into s_{acc} and s_{rej}, respectively. Therefore, for any given input string $w \in \Sigma^*$, the value of s_{acc} and s_{rej} are $p_{acc}(\mathcal{P}, w)$ and $p_{rej}(\mathcal{P}, w)$, respectively, at the end of the first round.

By using the method described in [YS09b, YS10], each stochastic matrix can be converted to a unitary one with twice the size as shown in the template

$$\mathsf{U} = \begin{pmatrix} \frac{1}{l}\left(\mathsf{A} \mid B\right) \\ \hline D \end{pmatrix},$$

where A is the original stochastic matrix; the columns of B, corresponding to newly added states, are filled in to ensure that each row of $(A \mid B)$ is pairwise orthogonal to the others, and has the same length l, which depends only on the dimension of A, and the entries of D are then selected to make U a unitary matrix.

Each transition matrix of $\mathcal{P}'$ can be converted to a $(2n+4) \times (2n+4)$-dimensional unitary matrix according to this template. These are the transition matrices of $\mathcal{M}$. The state set of $\mathcal{M}$ can be specified as follows:

1. The states corresponding to s_{acc} and s_{rej} are the accepting and rejecting states, q_{acc} and q_{rej}, respectively,
2. the states corresponding to the non-halting and non-restarting states of $\mathcal{P}'$ are non-halting and non-restarting states, respectively, and,
3. all remaining states are restarting states.

The initial state of $\mathcal{M}$ is the state corresponding to the initial state of $\mathcal{P}$.

When $\mathcal{M}$ runs on input string $|w|$, the amplitudes of q_{acc} and q_{rej}, the only halting states of $\mathcal{M}$, at the end of the first round are $\left(\frac{1}{l}\right)^{|w|+2} p_{acc}(\mathcal{P}, w)$ and $\left(\frac{1}{l}\right)^{|w|+2} p_{rej}(\mathcal{P}, w)$, respectively. Therefore, when $w \in L$,

$$\frac{p_{rej}(\mathcal{M}, w)}{p_{acc}(\mathcal{M}, w)} = \frac{p^2_{rej}(\mathcal{P}, w)}{p^2_{acc}(\mathcal{P}, w)} \leq \frac{\epsilon^2}{(1-\epsilon)^2},$$

and similarly, when $w \notin L$,

$$\frac{p_{acc}(\mathcal{M}, w)}{p_{rej}(\mathcal{M}, w)} = \frac{p^2_{acc}(\mathcal{P}, w)}{p^2_{rej}(\mathcal{P}, w)} \leq \frac{\epsilon^2}{(1-\epsilon)^2}.$$

By solving the equation

$$\frac{\epsilon'}{1-\epsilon'} = \frac{\epsilon^2}{(1-\epsilon)^2},$$

we obtain

$$\epsilon' = \frac{\epsilon^2}{1-2\epsilon+2\epsilon^2} \leq \epsilon.$$

The expected runtime of $\mathcal{P}$ is

$$\frac{1}{p_{acc}(\mathcal{P},w)+p_{rej}(\mathcal{P},w)} \in O(s(|w|)),$$

and so the expected runtime of $\mathcal{M}$ is

$$(l)^{2|w|+4}\frac{1}{p_{acc}^2(\mathcal{P},w)+p_{rej}^2(\mathcal{P},w)} < 3\,(l)^{2|w|+4}\left(\frac{1}{p_{acc}(\mathcal{P},w)+p_{rej}(\mathcal{P},w)}\right)^2 \in O(l^{2|w|}s^2(|w|)).$$

□

Corollary 1 *1QFA$^{\circlearrowleft}$'s can recognize all regular languages with zero error.*

To establish the strict superiority of 1QFA$^{\circlearrowleft}$'s over 1PFA$^{\circlearrowleft}$'s, we will make use of the following concepts.

An automaton $\mathcal{M}$ is said to recognize a language L with *positive one-sided unbounded error* if every input string $w \in L$ is accepted by $\mathcal{M}$ with nonzero probability, and every $w \notin L$ is rejected by $\mathcal{M}$ with probability 1. An automaton $\mathcal{M}$ is said to recognize a language L with *negative one-sided unbounded error* if every input string $w \in L$ is accepted by $\mathcal{M}$ with probability 1, and every $w \notin L$ is rejected by $\mathcal{M}$ with nonzero probability. In the cases described in the previous two sentences, if L is also recognized with bounded error by $\mathcal{M}$, it is said to be recognized with positive (respectively, negative) one-sided bounded error.

For an automaton $\mathcal{M}$ recognizing a language L, we define the *gap function*, $g_{\mathcal{M}} : N \rightarrow [0,1]$, such that $g_{\mathcal{M}}(n)$ is the difference between the minimum acceptance probability of a member of L with length at most n and the maximum acceptance probability of a non-member of L with length at most n[(iii)].

Lemma 7 *If a language L is recognized by a 1KWQFA $\mathcal{M}$ with positive (negative) one-sided unbounded error such that $g_{\mathcal{M}}(n) \geq c^{-n}$ for some $c > 1$, then for all $\epsilon \in (0, \frac{1}{2})$, L is recognized by some 1QFA$^{\circlearrowleft}$ having three more states than $\mathcal{M}$ with positive (negative) one-sided error ϵ in expected time $O(\frac{1}{\epsilon}c^{|w|}|w|)$.*

Proof: We consider the case of positive one-sided error. The adaptation to the other case is trivial. $\mathcal{M}$ is converted into a 1QFA$^{\circlearrowleft}$ $\mathcal{M}'_\epsilon$ as follows. $\mathcal{M}'_\epsilon$ starts by branching to two equiprobable paths, $\mathtt{path}_1$ and $\mathtt{path}_2$, at the beginning of the computation. $\mathtt{path}_1$ imitates the computation of $\mathcal{M}$, except that all reject states that appear in its subpaths are replaced by restart states. Regardless of the form of the input, $\mathtt{path}_2$ moves right with amplitude $\frac{1}{\sqrt{c}}$, (and so restarts the computation with the remaining probability,) on every input symbol. When it arrives at the right end-marker, $\mathtt{path}_2$ rejects with amplitude $\sqrt{\epsilon}$, and restarts the computation with amplitude $\sqrt{1-\epsilon}$.

When $w \notin L$,

$$p_{acc}(\mathcal{M}'_\epsilon, w) = 0, \text{ and } p_{rej}(\mathcal{M}'_\epsilon, w) = \frac{\epsilon}{2c^{|w|}},$$

and so the input is rejected with probability 1. When $w \in L$,

$$p_{acc}(\mathcal{M}'_\epsilon, w) \geq \frac{1}{2c^{|w|}}, \text{ and } p_{rej}(\mathcal{M}'_\epsilon, w) = \frac{\epsilon}{2c^{|w|}},$$

[(iii)] The definition of $g_{\mathcal{M}}$ is due to Bertoni and Carpentieri [BC01], who call it the "error function."

and so the input is accepted with error bound $\epsilon > 0$ due to Lemma 2, since

$$\frac{p_{rej}(\mathcal{M}'_\epsilon, w)}{p_{acc}(\mathcal{M}'_\epsilon, w)} \leq \epsilon.$$

Since $p_{halt}(\mathcal{M}'_\epsilon, w)$ is always greater than $\frac{\epsilon}{2c^{|w|}}$, the expected runtime of $\mathcal{M}'_\epsilon$ is $O(\frac{1}{\epsilon}c^{|w|}|w|)$. □

Lemma 8 *If a language L is recognized by a 1KWQFA $\mathcal{M}$ with positive (negative) one-sided bounded error such that $g_{\mathcal{M}}(n) \geq c^{-1}$ for some $c > 1$, then for all $\epsilon \in (0, \frac{1}{2})$, L is recognized by some 1QFA$^{\circlearrowleft}$ having three more states than $\mathcal{M}$ with positive (negative) one-sided error ϵ in expected time $O(\frac{1}{\epsilon}c|w|)$.*

Proof: The construction is almost identical to that in Lemma 7, except that $\mathtt{path}_2$ rejects with amplitude $\sqrt{\epsilon}$, and restarts the computation with amplitude $\sqrt{1-\epsilon}$ immediately on the left end-marker, thereby causing every input to be rejected with the constant probability $\frac{\epsilon}{2c}$. Hence, the expected runtime of $\mathcal{M}'_\epsilon$ turns out to be $O(\frac{1}{\epsilon}c|w|)$. □

Lemma 7 is a useful step towards an eventual characterization of the class of languages that are recognized with one-sided bounded error by 1QFA$^{\circlearrowleft}$'s, since full classical characterizations are known [YS] for the classes of languages recognized by one-sided unbounded error by several 1QFA models, including the 1KWQFA.

A language L is said to belong to the class $\mathrm{S}^{=}_{rat}$ [Tur69, Mac93] if there exists a rational 1PFA that accepts all and only the members of L with probability $\frac{1}{2}$.

Theorem 2 *For every language $L \in \mathrm{S}^{=}_{rat}$, there exists a number n such that for all error bounds $\epsilon > 0$, there exist n-state 1QFA$^{\circlearrowleft}$'s that recognize L and $\overline{L}$ with one-sided error bounded by ϵ.*

Proof: For a language L in $\mathrm{S}^{=}_{rat}$, let $\mathcal{P}$ be the rational 1PFA associated by L as described above. Turakainen [Tur69] showed that there exists a constant $b > 1$ such that for any string $w \notin L$, the probability that $\mathcal{P}$ accepts w cannot be in the interval $(\frac{1}{2} - b^{-|w|}, \frac{1}{2} + b^{-|w|})$. By using the method described in [YS], we can convert $\mathcal{P}$ to a 1KWQFA $\mathcal{M}$ recognizing $\overline{L}$ with one-sided unbounded error, so that $\mathcal{M}$ accepts any $w \in \overline{L}$ with probability greater than $c^{-|w|}$, for a constant $c > b$. We can conclude with Lemma 7. □

$\mathrm{S}^{=}_{rat}$ contains many well-known languages, such as L_{eq}, $L_{pal} = \{w \mid w = w^R\}$, $L_{twin} = \{wcw \mid w \in \{a,b\}^*\}$, $L_{mult} = \{x\#y\#z \mid x, y, z \text{ are natural numbers in binary notation and } x \times y = z\}$, $L_{square} = \{a^n b^{n^2} \mid n > 0\}$, $L_{power} = \{a^n b^{2^n}\}$, the word problem for finitely generated free groups, and all *polynomial languages*, [Tur82] defined as

$$\{a_1^{n_1} \cdots a_k^{n_k} b_1^{p_1(n_1,\ldots,n_k)} \cdots b_r^{p_r(n_1,\ldots,n_k)} \mid p_i(n_1,\ldots,n_k) \geq 0\},$$

where $a_1, \ldots, a_k, b_1, \ldots, b_r$ are distinct symbols, and each p_i is a polynomial with integer coefficients. Note that Theorem 2 and Lemma 6 answer a question posed by Ambainis and Watrous [AW02] about whether L_{square} and L_{power} can be recognized with bounded error by 2QCFAs affirmatively.

Corollary 2 *The class of languages recognized by 1QFA$^{\circlearrowleft}$'s with bounded error properly contains the class of languages recognized by 1PFA$^{\circlearrowleft}$'s.*

Proof: This follows from Theorems 1 and 2, Lemma 4, and the fact [DS92, FK94] that L_{pal} cannot be recognized with bounded error by 2PFAs. □

Since general 1QFAs [Pas00, Hir08, YS10] are known to be equivalent in language recognition power to 1PFAs, one has to consider a two-way model to demonstrate the superiority of quantum computers over classical ones. The 2QCFA is known [AW02] to be superior to its classical counterpart, the 2PFA, also by virtue of L_{pal}. Recall that, by Lemma 6, 2QCFAs can simulate 1QFA$^{\circlearrowleft}$'s easily, and we do not know of a simulation in the other direction.

4 Conciseness of 2QFAs with mixed states and 2PFAs

In this section, we demonstrate several infinite families of regular languages which can be recognized with some fixed probability greater than $\frac{1}{2}$ by just tuning the transition amplitudes of a 1QFA$^{\circlearrowleft}$ with a constant number of states, whereas the sizes of the corresponding 1QFAs, 1PFAs, and 2NFAs grow without bound. One of our constructions can be adapted easily to show that 1PFA$^{\circlearrowleft}$'s, (and, equivalently, 2PFAs), also possess the same advantage over those machines.

Definition 2 *For an alphabet Σ containing symbols a and b, and $m \in \mathbb{Z}^+$, the family of languages A_m is defined as*

$$A_m = \{ua \mid u \in \Sigma^*, |u| \leq m\}.$$

Note that Ambainis et al. [ANTSV02] report that any Nayak one-way quantum finite automaton[(iv)] that recognizes A_m with some fixed probability greater than $\frac{1}{2}$ has $2^{\Omega(m)}$ states.

Theorem 3 *A_m is recognized by a 6-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_{m,\epsilon}$ for any error bound $\epsilon > 0$. Moreover, the expected runtime of $\mathcal{M}_{m,\epsilon}$ on input w is $O(\left(\frac{1}{\epsilon}\right)^{2m}|w|)$.*

Proof: Let $\mathcal{M}_{m,\epsilon} = \{Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej}, Q_{restart}\}$ be a 1QFA$^{\circlearrowleft}$ with $Q_{non} = \{q_0, q_1\}$, $Q_{acc} = \{A\}$, $Q_{rej} = \{R\}$, $Q_{restart} = \{I_1, I_2\}$. $\mathcal{M}_{m,\epsilon}$ contains the transitions

$$\begin{aligned}
\mathsf{U}_{¢}|q_0\rangle &= \epsilon|q_1\rangle + \epsilon^{\frac{2m+5}{2}}|R\rangle + \sqrt{1-\epsilon^2-\epsilon^{2m+5}}|I_1\rangle \\
\mathsf{U}_{a}|q_0\rangle &= \epsilon|q_0\rangle + \sqrt{\frac{1}{2}-\epsilon^2}|I_1\rangle + \frac{1}{\sqrt{2}}|I_2\rangle \\
\mathsf{U}_{a}|q_1\rangle &= \epsilon|q_0\rangle + \sqrt{\frac{1}{2}-\epsilon^2}|I_1\rangle - \frac{1}{\sqrt{2}}|I_2\rangle \\
\mathsf{U}_{\Sigma\setminus\{a\}}|q_0\rangle &= \epsilon|q_1\rangle + \sqrt{\frac{1}{2}-\epsilon^2}|I_1\rangle + \frac{1}{\sqrt{2}}|I_2\rangle \\
\mathsf{U}_{\Sigma\setminus\{a\}}|q_1\rangle &= \epsilon|q_1\rangle + \sqrt{\frac{1}{2}-\epsilon^2}|I_1\rangle - \frac{1}{\sqrt{2}}|I_2\rangle \\
\mathsf{U}_{\$}|q_0\rangle &= |A\rangle \\
\mathsf{U}_{\$}|q_1\rangle &= |R\rangle
\end{aligned}$$

[(iv)] This is a 1QFA model of intermediate power, subsuming the 1KWQFA, but strictly weaker than the most general models ([Pas00, Hir08, YS10]) which recognize any regular language with at most the same state cost as the corresponding DFA.

and the transitions not mentioned above can be completed easily, by extending each U_σ to be unitary.

On the left end-marker, $\mathcal{M}_{m,\epsilon}$ rejects with probability ϵ^{2m+5}, goes on to scan the input string with amplitude ϵ, and restarts immediately with the remaining probability. States q_0 and q_1 implement the check for the regular expression $\Sigma^* a$, but the machine restarts with probability $1-\epsilon^2$ on all input symbols during this check.

If $w = u\sigma'$ for $u \in \Sigma^*$, and $\sigma' \neq a$, the input is rejected with probability 1, since $p_{acc}(\mathcal{M}_{m,\epsilon}, w) = 0$.

If $w = ua$ for $u \in \Sigma^*$,

$$p_{acc}(\mathcal{M}_{m,\epsilon}, w) = \epsilon^{2|w|+2}, \;\; p_{rej}(\mathcal{M}_{m,\epsilon}, w) = \epsilon^{2m+5}.$$

Hence, if $w \in A_m$,

$$p_{acc}(\mathcal{M}_{m,\epsilon}, w) \geq \epsilon^{2m+4},$$

and if $w \notin A_m$,

$$p_{acc}(\mathcal{M}_{m,\epsilon}, w) \leq \epsilon^{2m+6}.$$

In both cases, the corresponding ratio $\frac{p_{rej}(\mathcal{M}_{m,\epsilon},w)}{p_{acc}(\mathcal{M}_{m,\epsilon},w)}$ or $\frac{p_{acc}(\mathcal{M}_{m,\epsilon},w)}{p_{rej}(\mathcal{M}_{m,\epsilon},w)}$ is not greater than ϵ. Thus, by Lemma 2, we conclude that $\mathcal{M}_{m,\epsilon}$ recognizes A_m with error bounded by ϵ. Since $p_{halt}(\mathcal{M}_{m,\epsilon}, w)$ is always greater than ϵ^{2m+5}, the expected runtime of $\mathcal{M}_{m,\epsilon}$ is $O(\left(\frac{1}{\epsilon}\right)^{2m}|w|)$. □

By a theorem of Rabin [Rab63], for any fixed error bound, if a language L is recognized with bounded error by a 1PFA with n states, then there exists a deterministic finite automaton (DFA) that recognizes L with $2^{O(n)}$ states. Parallelly, Freivalds et al. [FOM09] note that one-way quantum finite automata with mixed states are no more than superexponentially more concise than DFAs. These facts can be used to conclude that a collection of 1PFAs (or 1QFAs) with a fixed common number of states that recognize an infinite family of languages with a fixed common error bound less than $\frac{1}{2}$, *à la* the two-way quantum automata of Theorem 3, cannot exist, since that would imply the existence of a similar family of DFAs of fixed size. By the same reasoning, the existence of such families of 2NFAs can also be overruled.

The reader should note that there exists a bounded-error 1PFA$^{\circlearrowleft}$ (and therefore, a 2PFA[(v)],) for A_m, which one can obtain simply by replacing each transition amplitude of 1QFA$^{\circlearrowleft}$ $\mathcal{M}_{m,\epsilon}$ defined in Theorem 3 by the square of its modulus. This establishes the fact that 2PFAs also possess the succinctness advantage discussed above over 1PFAs, 1QFAs and 2NFAs.

We proceed to present two more examples.

Definition 3 *For $m \in \mathbb{Z}^+$, the language family $B_m \subseteq \{a\}^*$ is defined as*

$$B_m = \{a^i \mid i \mod (m) \equiv 0\}.$$

Theorem 4 *For any error bound $\epsilon > 0$, there exists a 7-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_{m,\epsilon}$ which accepts any $w \in B_m$ with certainty, and rejects any $w \notin B_m$ with probability at least $1-\epsilon$. Moreover, the expected runtime of $\mathcal{M}_{m,\epsilon}$ on w is $O\left(\frac{1}{\epsilon}\sin^{-2}(\frac{\pi}{m})|w|\right)$.*

Proof: We will construct a 4-state 1KWQFA recognizing $\overline{B_m}$ with positive one-sided unbounded error, as described in [AF98]. Let $\mathcal{M}_m = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ be 1KWQFA with $Q_{non} = \{q_0, q_1\}$,

[(v)] See Section 6 for an examination of the relationship between the computational powers of the 1PFA$^{\circlearrowleft}$ and the 2PFA.

$Q_{acc} = \{A\}$, $Q_{rej} = \{R\}$. $\mathcal{M}_m$ contains the transitions

$$\begin{aligned}
\mathsf{U}_{¢}|q_0\rangle &= |q_0\rangle \\
\mathsf{U}_a|q_0\rangle &= \cos(\frac{\pi}{m})|q_0\rangle + \sin(\frac{\pi}{m})|q_1\rangle \\
\mathsf{U}_a|q_1\rangle &= -\sin(\frac{\pi}{m})|q_0\rangle + \cos(\frac{\pi}{m})|q_1\rangle \\
\mathsf{U}_\$|q_0\rangle &= |R\rangle \\
\mathsf{U}_\$|q_1\rangle &= |A\rangle,
\end{aligned}$$

and the transition amplitudes not listed above are filled in to satisfy unitarity. $\mathcal{M}_m$ begins computation at the $|q_0\rangle$-axis, and performs a rotation by angle $\frac{\pi}{m}$ in the $|q_0\rangle$-$|q_1\rangle$ plane for each a it reads. Therefore, the value of the gap function, $g_{\mathcal{M}_m}$, is not less than $\sin^2(\frac{\pi}{m})$ for $|w| > 0$. By Lemma 8, there exists a 7-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_{m,\epsilon}$ recognizing $\overline{B_m}$ with positive one-sided bounded error and whose expected runtime is $O\left(\frac{1}{\epsilon}\sin^{-2}(\frac{\pi}{m})|w|\right)$. By swapping the accepting and rejecting states of $\mathcal{M}_{m,\epsilon}$, we can get the desired machine. □

Definition 4 *For an alphabet Σ, and $m \in \mathbb{Z}^+$, the language family C_m is defined as*

$$C_m = \{w \in \Sigma^* \mid |w| = m\}.$$

Theorem 5 *For any error bound $\epsilon > 0$, there exists a 7-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_{m,\epsilon}$ which accepts any $w \in C_m$ with certainty, and rejects any $w \notin C_m$ with probability at least $1-\epsilon$. Moreover, the expected runtime of $\mathcal{M}_{m,\epsilon}$ on w is $O(\frac{1}{\epsilon}2^m|w|)$.*

Proof: We will contruct a 4-state 1KWQFA recognizing $\overline{C_m}$ with positive one-sided unbounded error. Let $\mathcal{M}_m = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ be 1KWQFA with $Q_{non} = \{q_0, q_1\}$, $Q_{acc} = \{A\}$, $Q_{rej} = \{R\}$. $\mathcal{M}_m$ contains the transitions

$$\begin{aligned}
\mathsf{U}_{¢}|q_0\rangle &= \frac{1}{\sqrt{2}}|q_0\rangle + \left(\frac{1}{\sqrt{2}}\right)^{m+1}|q_1\rangle + \sqrt{\frac{1}{2} - \left(\frac{1}{2}\right)^{m+1}}|R\rangle \\
\mathsf{U}_{\sigma\in\Sigma}|q_0\rangle &= \frac{1}{\sqrt{2}}|q_0\rangle + \frac{1}{\sqrt{2}}|R\rangle \\
\mathsf{U}_{\sigma\in\Sigma}|q_1\rangle &= |q_1\rangle \\
\mathsf{U}_\$|q_0\rangle &= \frac{1}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|R\rangle \\
\mathsf{U}_\$|q_1\rangle &= -\frac{1}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|R\rangle
\end{aligned}$$

with the amplitudes of the transitions not mentioned above filled in to ensure unitarity.

$\mathcal{M}_m$ encodes the length of the input string in the amplitude of state q_0, which equals $\left(\frac{1}{\sqrt{2}}\right)^{|w|+1}$ just before the processing of the right end-marker. The desired length m is “hardwired” into the amplitudes of

q_1. For a given input string $w \in \Sigma^*$, if $w \in C_m$, then the amplitudes of states q_0 and q_1 are equal, and the quantum Fourier transform (QFT) [KW97] performed on the right end-marker sets the amplitude of A to 0. Therefore, w is rejected with certainty. If $w \in \overline{C_m}$, then the accepting probability is equal to

$$\left(\left(\frac{1}{\sqrt{2}}\right)^{|w|+2} - \left(\frac{1}{\sqrt{2}}\right)^{m+2}\right)^2,$$

and it is minimized when $|w| = m+1$, which gives us the inequality

$$g_{\mathcal{M}_m}(w) > \left(\frac{1}{2}\right)^{m+6}.$$

By Lemma 8, there exists a 7-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_{m,\epsilon}$ recognizing $\overline{C_m}$ with positive one-sided bounded error and whose expected runtime is $O\left(\frac{1}{\epsilon}2^m|w|\right)$. By swapping the accepting and rejecting states of $\mathcal{M}_{m,\epsilon}$, we can get the desired machine. □

Note that, unlike what we had with Theorem 3, the QFAs of Theorems 4 and 5 cannot be converted so easily to 2PFAs. In fact, we can prove that there exist no 2PFA families of fixed size which recognize B_m and C_m with fixed one-sided error less than $\frac{1}{2}$, like those QFAs: Assume that such a 2PFA family exists. Switch the accept and reject states to obtain a family for the complements of the languages. The 2PFAs thus obtained operate with cutpoint 0. Obtain an equivalent 2NFA with the same number of states by converting all transitions with nonzero weight to nondeterministic transitions. But there are only finitely many 2NFAs of this size, meaning that they cannot recognize our infinite family of languages.

5 Efficient Probability Amplification

Many automaton descriptions in this paper, and elsewhere in the theory of probabilistic and quantum automata, describe not a single algorithm, but a general template which one can use for building a machine M_ϵ that operates with a desired error bound ϵ. The dependences of the runtime and number of states of M_ϵ on $\frac{1}{\epsilon}$ are measures of the complexity of the probability amplification process involved in the construction method used. Viewed as such, the constructions described in the theorems in Section 4 are maximally efficient in terms of the state cost, with no dependence on the error bound. In this section, we present improvements over previous results about the efficiency of probability amplification in 2QFAs.

5.1 Improved algorithms for L_{eq}

In classical computation, one only needs to sequence $O(\log(\frac{1}{\epsilon}))$ identical copies of a given probabilistic automaton with one sided error $p < 1$ to run on the same input in order to obtain a machine with error bound ϵ. Yakaryılmaz and Say [YS09a] noted that this method of probability amplification does not yield efficient results for 2KWQFAs; the number of machine copies required to reduce the error to ϵ can be as high as $(\frac{1}{\epsilon})^2$. The most succinct 2KWQFAs for L_{eq} produced by alternative methods developed in [YS09a] have $O(\log^2(\frac{1}{\epsilon})\log\log(\frac{1}{\epsilon}))$ states, and runtime linear in the size of the input w. In Appendix Appendix A, we present a construction which yields (exponential time) 1QFA$^{\circlearrowleft}$'s that recognize L_{eq} within any desired error bound ϵ, with no dependence of the state set size on ϵ. Ambainis and Watrous [AW02] present a method which can be used to build 2QCFAs that recognize L_{eq} also with constant state set size,

where the "tuning" of the automaton for a particular error bound is achieved by setting some transition amplitudes appropriately, and the expected runtime of those machines is $O(|w|^4)$. We now show that the 2QFA$^{\circlearrowleft}$ formalism allows more efficient probability amplification.

Theorem 6 *There exists a constant n, such that, for any $\epsilon > 0$, an n-state 2QFA$^{\circlearrowleft}$ which recognizes L_{eq} with one-sided error bound ϵ within $O(\frac{1}{\epsilon}|w|)$ expected runtime can be constructed, where w is the input string.*

Proof: We start with Kondacs and Watrous' original 2KWQFA [KW97] M_N, which recognizes L_{eq} with one-sided error $\frac{1}{N}$, for any integer $N > 1$. After a deterministic test for membership of a^*b^*, M_N branches to N computational paths, each of which perform a QFT at the end of the computation. Set $N = 2$. M_2 accepts all members of L_{eq} with probability 1. Non-members of L_{eq} are rejected with probability at least $\frac{1}{2}$. We convert M_2 to a 2QFA$^{\circlearrowleft}$ $\mathcal{M}'_\epsilon$ by changing the target states of the QFT as follows:

$$\mathsf{path}_1 \rightarrow \frac{1}{\sqrt{2}}|\text{Reject}\rangle + \sqrt{\frac{\epsilon}{2}}|\text{Accept}\rangle + \sqrt{\frac{1-\epsilon}{2}}|\text{Restart}\rangle$$

$$\mathsf{path}_2 \rightarrow -\frac{1}{\sqrt{2}}|\text{Reject}\rangle + \sqrt{\frac{\epsilon}{2}}|\text{Accept}\rangle + \sqrt{\frac{1-\epsilon}{2}}|\text{Restart}\rangle$$

where the amplitude of each path is $\frac{1}{\sqrt{2}}$. For a given input $w \in \Sigma^*$,

1. if w is not of the form a^*b^*, then $p_{rej}(\mathcal{M}'_\epsilon, w) = 1$;
2. if w is of the form a^*b^* and $w \notin L$, then $p_{rej}(\mathcal{M}'_\epsilon, w) = \frac{1}{2}$, and $p_{acc}(\mathcal{M}'_\epsilon, w) = \frac{\epsilon}{2}$;
3. if $w \in L$, then $p_{rej}(\mathcal{M}'_\epsilon, w) = 0$ and $p_{acc}(\mathcal{M}'_\epsilon, w) = \epsilon$.

It is easily seen that the error is one-sided. Since $\frac{p_{acc}(\mathcal{M}'_\epsilon, w)}{p_{rej}(\mathcal{M}'_\epsilon, w)} = \epsilon$, we can conclude with Lemma 2. Moreover, the minimum halting probability occurs in the third case above, and so the expected runtime of $\mathcal{M}'_\epsilon$ is $O(\frac{1}{\epsilon}|w|)$. □

Theorem 7 *For any $\epsilon \in (0, \frac{1}{2})$, there exists a 2QFA$^{\curvearrowright}$ with $O(\log(\frac{1}{\epsilon}))$ states that recognizes L_{eq} with one-sided error bound ϵ in $O(\log(\frac{1}{\epsilon})|w|)$ steps, where w is the input string.*

Proof: Let M_2 be the 2KWQFA recognizing L_{eq} with one-sided error bound $\frac{1}{2}$ mentioned in the proof of Theorem 6. Then, a 2QFA$^{\curvearrowright}$ that is constructed by sequentially connecting $O(\log(\frac{1}{\epsilon}))$ copies of M_2, so that the input is accepted only if it is accepted by all the copies, and rejected otherwise, can recognize L_{eq} with one-sided error bound ϵ. □

5.2 An improved algorithm for L_{pal}

Ambainis and Watrous [AW02] present a 2QCFA construction which decides L_{pal} in expected time $O(\left(\frac{1}{\epsilon}\right)^{|w|}|w|)$ with error bounded by $\epsilon > 0$, where w is the input string. (Watrous [Wat98] describes a 2KWQFA which accepts all members of the complement of L_{pal} with probability 1, and fails to halt for all palindromes; it is not known if 2KWQFAs can recognize this language by halting for all inputs.) We will now present a 1QFA$^{\circlearrowleft}$ construction, which, by Lemma 6, can be adapted to yield 2QCFAs with the

Paths	$\mathsf{U}_{¢}, \mathsf{U}_a$	U_b
	$\mathsf{U}_{¢}\|q_0\rangle = \frac{1}{\sqrt{2}}\|p_1\rangle + \frac{1}{\sqrt{2}}\|q_1\rangle$	
path_1	$\mathsf{U}_a\|p_1\rangle = \sqrt{\frac{2}{3}}\|p_1\rangle - \frac{1}{\sqrt{3}}\|R_1\rangle$	$\mathsf{U}_b\|p_1\rangle = \frac{1}{\sqrt{6}}\|p_1\rangle + \frac{1}{\sqrt{6}}\|p_2\rangle + \frac{1}{\sqrt{3}}\|R_1\rangle + \frac{1}{\sqrt{3}}\|R_2\rangle$
	$\mathsf{U}_a\|p_2\rangle = \frac{1}{\sqrt{6}}\|p_1\rangle + \frac{1}{\sqrt{6}}\|p_2\rangle + \frac{1}{\sqrt{3}}\|R_1\rangle + \frac{1}{\sqrt{3}}\|R_2\rangle$	$\mathsf{U}_b\|p_2\rangle = \sqrt{\frac{2}{3}}\|p_2\rangle - \frac{1}{\sqrt{3}}\|R_1\rangle$
path_2	$\mathsf{U}_a\|q_1\rangle = \frac{1}{\sqrt{6}}\|q_1\rangle + \frac{1}{\sqrt{6}}\|q_3\rangle - \frac{1}{\sqrt{3}}\|R_3\rangle + \frac{1}{\sqrt{3}}\|R_4\rangle$	$\mathsf{U}_b\|q_1\rangle = \frac{1}{\sqrt{6}}\|q_1\rangle + \frac{1}{\sqrt{6}}\|q_2\rangle - \frac{1}{\sqrt{3}}\|R_3\rangle + \frac{1}{\sqrt{3}}\|R_4\rangle$
	$\mathsf{U}_a\|q_2\rangle = \sqrt{\frac{2}{3}}\|q_2\rangle + \frac{1}{\sqrt{3}}\|R_5\rangle$	$\mathsf{U}_b\|q_2\rangle = \sqrt{\frac{2}{3}}\|q_2\rangle + \frac{1}{\sqrt{3}}\|R_3\rangle$
	$\mathsf{U}_a\|q_3\rangle = \sqrt{\frac{2}{3}}\|q_3\rangle + \frac{1}{\sqrt{3}}\|R_3\rangle$	$\mathsf{U}_b\|q_3\rangle = \sqrt{\frac{2}{3}}\|q_3\rangle + \frac{1}{\sqrt{3}}\|R_5\rangle$
	$\mathsf{U}_{\$}$	
path_1	$\mathsf{U}_{\$}\|p_1\rangle = \|R_1\rangle$	
	$\mathsf{U}_{\$}\|p_2\rangle = \frac{1}{\sqrt{2}}\|A\rangle + \frac{1}{\sqrt{2}}\|R_2\rangle$	
path_2	$\mathsf{U}_{\$}\|q_1\rangle = \|R_3\rangle$	
	$\mathsf{U}_{\$}\|q_2\rangle = -\frac{1}{\sqrt{2}}\|A\rangle + \frac{1}{\sqrt{2}}\|R_2\rangle$	
	$\mathsf{U}_{\$}\|q_3\rangle = \|R_4\rangle$	

Fig. 1: Specification of the transition function of $\mathcal{M}$

same complexity, which reduces the dependence of the Ambainis-Watrous method on the desired error bound considerably.

Theorem 8 *For any $\epsilon > 0$, there exists a 15-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_\epsilon$ which accepts any $w \in L_{pal}$ with certainty, and rejects any $w \notin L_{pal}$ with probability at least $1 - \epsilon$. Moreover, the expected runtime of $\mathcal{M}_\epsilon$ on w is $O(\frac{1}{\epsilon}3^{|w|}|w|)$.*

Proof: We will first construct a modified version of the 1KWQFA algorithm of Lāce et al. [LSDF09] for recognizing the nonpalindrome language. The idea behind the construction is that we encode both the input string and its reverse into the amplitudes of two of the states of the machine, and then perform a substraction between these amplitudes using the QFT [LSDF09]. If the input is not a palindrome, the two amplitudes do not cancel each other completely, and the nonzero difference is transferred to an accept state. Otherwise, the accepting probability will be zero.

Let $\mathcal{M} = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ be 1KWQFA with $Q_{non} = \{p_1, p_2, q_0, q_1, q_2, q_3\}$, $Q_{acc} = \{A\}$, $Q_{rej} = \{R_i \mid 1 \leq i \leq 5\}$. The transition function of $\mathcal{M}$ is shown in Figure 1. As before, we assume that the transitions not specified in the figure are filled in to ensure that the U_σ are unitary. path_2 and path_1 encode the input string and its reverse [Rab63, Paz71] into the amplitudes of states q_2 and p_2, respectively. If the input is $w = w_1 w_2 \cdots w_l$, then the values of these amplitudes just before the transition associated with the right end-marker in the first round are as follows:

- State p_2 has amplitude $\frac{1}{\sqrt{2}}\left(\sqrt{\frac{2}{3}}\right)^{|w|}(0.w_l w_{l-1} \cdots w_1)_2$, and
- state q_2 has amplitude $\frac{1}{\sqrt{2}}\left(\sqrt{\frac{2}{3}}\right)^{|w|}(0.w_1 w_2 \cdots w_l)_2$.

The factor of $\sqrt{\frac{2}{3}}$ is due to the "loss" of amplitude necessitated by the fact that the originally non-unitary encoding matrices of [Rab63, Paz71] have to be "embedded" in a unitary matrix [YS09b, YS10]. Note that the symbols a and b are encoded by 0 and 1, respectively.

If $w \in L_{pal}$, the acceptance probability is zero. If $w \in \overline{L_{pal}}$, the acceptance probability is minimized by strings which are almost palindromes, except for a single defect in the middle, that is, when $|w| = 2k$ for $k \in \mathbb{Z}^+$, $w_i = w_{2k-i+1}$, where $1 \leq i \leq k-1$, and $w_k \neq w_{k+1}$, so,

$$g_{\mathcal{M}}(w) \geq \frac{1}{8}\left(\frac{1}{3}\right)^{|w|}.$$

By Lemma 7, there exists a 15-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_\epsilon$ recognizing $\overline{L_{pal}}$ with positive one-sided bounded error, whose expected runtime is $O(\frac{1}{\epsilon}3^{|w|}|w|)$. By swapping accepting and rejecting states of $\mathcal{M}_m$, we can get the desired machine. □

Note that the technique used in the proof above can be extended easily to handle bigger input alphabets by using the matrices defined on Page 169 of [Paz71], and the method of simulating stochastic matrices by unitary matrices described in [YS09b, YS10].

6 1PFA$^{\circlearrowleft}$ vs. 2PFA

It is interesting to examine the power of the restart move in classical computation as well. Any 1PFA$^{\circlearrowleft}$ which runs in expected t steps can be simulated by a 2PFA which runs in expected $2t$ steps (see Lemma 4). We ask in this section whether the restart move can substitute the "left" and "stationary" moves of a 2PFA without loss of computational power. Since every polynomial-time 2PFA recognizes a regular language, which can of course be recognized by using only "right" moves, we focus on the best-known example of a nonregular language that can be recognized by an exponential-time 2PFA.

Theorem 9 *There exists a natural number k, such that for any $\epsilon > 0$, there exists a k-state 1PFA$^{\circlearrowleft}$ $\mathcal{P}_\epsilon$ recognizing language L_{eq} with error bound ϵ and expected runtime $O((\frac{2}{\epsilon^2})^{|w|}|w|)$, where w is the input string.*

Proof: We will construct the 1PFA$^{\circlearrowleft}$ $\mathcal{P}_\epsilon$ as follows: Let $x = \frac{\epsilon^2}{2}$. The computation splits into three paths called path_1, path_2, and path_3 with equal probabilities on symbol $\not\in$. All three paths, while performing their main tasks, parallelly check whether the input is of the form a^*b^*, if not, all paths simply reject. The main tasks of the paths are as follows:

- path_1 moves on with probability x and restarts with probability $1-x$ when reading symbols a and b. After reading the right end-marker \$, it accepts with probability with 1.
- path_2 moves on with probability x^2 and restarts with probability $1-x^2$ when reading symbol a. On b's, it continues with the "syntax" check. After reading the \$, it rejects with probability $\frac{\epsilon}{2}$ and restarts with probability $1-\frac{\epsilon}{2}$.
- path_3 is similar to path_2, except that the transitions of symbols a and b are interchanged.

If the input is of the form $a^m b^n$, then the accept and reject probabilities of the first round are calculated as

$$p_{acc}(\mathcal{P}_\epsilon, w) = \frac{1}{3}x^{m+n}, \text{ and } p_{rej}(\mathcal{P}_\epsilon, w) = \frac{\epsilon}{6}\left(x^{2m} + x^{2n}\right).$$

If $m = n$, then

$$\frac{p_{rej}(\mathcal{P}_\epsilon, w)}{p_{acc}(\mathcal{P}_\epsilon, w)} = \epsilon.$$

If $m \neq n$ (assume without loss of generality that $m = n + d$ for some $d \in \mathbb{Z}^+$) , then

$$\frac{p_{acc}(\mathcal{P}_\epsilon, w)}{p_{rej}(\mathcal{P}_\epsilon, w)} = \frac{2}{\epsilon}\frac{x^{2n+d}}{x^{2n+2d} + x^{2n}} = \frac{2}{\epsilon}\frac{x^d}{x^{2d} + 1} < \frac{2}{\epsilon}x^d \leq \frac{2}{\epsilon}x$$

By replacing $x = \dfrac{\epsilon^2}{2}$, we can get

$$\frac{p_{acc}(\mathcal{P}_\epsilon, w)}{p_{rej}(\mathcal{P}_\epsilon, w)} < \epsilon.$$

By using Lemma 2, we can conclude that $\mathcal{P}_\epsilon$ recognizes L_{eq} with error bound ϵ.

Since $p_{halt}(\mathcal{P}_\epsilon, w)$ is always greater than $\frac{1}{3}x^{|w|}$, the expected runtime of the algorithm is $O((\frac{2}{\epsilon^2})^{|w|}|w|)$, where w is the input string. □

7 Concluding remarks

By a theorem of Dwork and Stockmeyer [DS90], for every $\epsilon < \frac{1}{2}$, if L is recognized by a $O(n)$–time 2PFA with c states within error probability ϵ, then L is also recognized by a DFA with c^{bc^2} states, where the number b depends on ϵ and the constant hidden in the big-O. The two-way machines of Section 4 can be seen to have such factors that grow with m in the expressions for their time complexities; this is how the machines described in that section achieve their huge superiority in terms of the state cost over the other models that they are compared with.

It is known [YS09b, YS10, FYS10] that 2KWQFAs can recognize some nonstochastic languages (i.e. those which cannot be recognized by 2PFAs) in the unbounded error setting. On the other hand, we conjecture that 2QFAs with classical head position, such as the 2QCFA, cannot recognize any nonstochastic language. Therefore, it is an interesting question whether 2QFA$^{\circlearrowleft}$'s (or possibly an even more general 2QFA model allowing head superposition) can recognize any nonstochastic language with bounded error or not.

Some other open questions related to this work are:

1. Can 1QFA$^{\circlearrowleft}$'s simulate 2QCFAs?
2. Are 1PFA$^{\circlearrowleft}$'s (with just "restart" and "right" moves) equivalent in power to 2PFAs in the bounded-error setting, as hinted by Section 6?
3. Does there exist an analogue of the Dwork-Stockmeyer theorem mentioned above for two-way quantum finite automata?

Acknowledgements

We are grateful to Andris Ambainis and John Watrous for their helpful comments on earlier versions of this paper. We also thank Rūsiņš Freivalds for kindly providing us a copy of reference [LSDF09].

References

[AF98] Andris Ambainis and Rūsiņš Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *FOCS'98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 332–341, Palo Alto, California, 1998.

[AKN98] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, New York, NY, USA, 1998. ACM.

[ANTSV02] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

[AW02] Andris Ambainis and John Watrous. Two–way finite automata with quantum and classical states. *Theoretical Computer Science*, 287(1):299–311, 2002.

[BC01] Alberto Bertoni and Marco Carpentieri. Regular languages accepted by quantum automata. *Information and Computation*, 165(2):174–182, 2001.

[DS90] Cynthia Dwork and Larry Stockmeyer. A time complexity gap for two-way probabilistic finite-state automata. *SIAM Journal on Computing*, 19(6):1011–1123, 1990.

[DS92] Cynthia Dwork and Larry Stockmeyer. Finite state verifiers I: The power of interaction. *Journal of the ACM*, 39(4):800–828, 1992.

[FK94] Rūsiņš Freivalds and Marek Karpinski. Lower space bounds for randomized computation. In *ICALP'94: Proceedings of the 21st International Colloquium on Automata, Languages and Programming*, pages 580–592, London, UK, 1994. Springer-Verlag.

[FOM09] Rūsiņš Freivalds, Māris Ozols, and Laura Mančinska. Improved constructions of mixed state quantum automata. *Theoretical Computer Science*, 410(20):1923–1931, 2009.

[Fre81] Rūsiņš Freivalds. Probabilistic two-way machines. In *Proceedings of the International Symposium on Mathematical Foundations of Computer Science*, pages 33–45, 1981.

[FYS10] Rūsiņš Freivalds, Abuzer Yakaryılmaz, and A. C. Cem Say. A new family of nonstochastic languages. *Information Processing Letters*, 110(10):410–413, 2010.

[GW86] Albert G. Greenberg and Alan Weiss. A lower bound for probabilistic algorithms for finite state machines. *Journal of Computer and System Sciences*, 33(1):88–105, 1986.

[Hir08] Mika Hirvensalo. Various aspects of finite quantum automata. In *DLT'08: Proceedings of the 12th international conference on Developments in Language Theory*, pages 21–33. Springer-Verlag, 2008.

[Kaņ91] Jānis Kaņeps. Stochasticity of the languages acceptable by two-way finite probabilistic automata. *Discrete Mathematics and Applications*, 1:405–421, 1991.

[KF90] Jānis Kaņeps and Rūsiņš Freivalds. Minimal nontrivial space complexity of probabilistic one-way Turing machines. In *Proceedings on Mathematical Foundations of Computer Science*, volume 452 of *Lecture Notes in Computer Science*, pages 355–361, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[KW97] Attila Kondacs and John Watrous. On the power of quantum finite state automata. In *FOCS'97: Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 66–75, 1997.

[LSDF09] Lelde Lāce, Oksana Scegulnaja-Dubrovska, and Rūsiņš Freivalds. Languages recognizable by quantum finite automata with cut-point 0. In *SOFSEM'09: Proceedings of the 35th International Conference on Current Trends in Theory and Practice of Computer Science*, volume 2, pages 35–46, 2009.

[Mac93] Ioan Macarie. Closure properties of stochastic languages. Technical Report 441, University of Rochester, 1993.

[Pas00] Kathrin Paschen. Quantum finite automata using ancilla qubits. Technical report, University of Karlsruhe, 2000. Available at http://digbib.ubka.uni-karlsruhe.de/volltexte/1452000.

[Paz71] Azaria Paz. *Introduction to Probabilistic Automata*. Academic Press, New York, 1971.

[Rab63] Michael O. Rabin. Probabilistic automata. *Information and Control*, 6:230–243, 1963.

[Sip06] Michael Sipser. *Introduction to the Theory of Computation, 2nd edition*. Thomson Course Technology, United States of America, 2006.

[Tur69] Paavo Turakainen. On languages representable in rational probabilistic automata. *Annales Academiae Scientiarum Fennicae, Ser.A*, (439):4–10, 1969.

[Tur82] Paavo Turakainen. *Discrete Mathematics*, volume 7 of *Banach Center Publications*, chapter Rational stochastic automata in formal language theory, pages 31–44. PWN-Polish Scientific Publishers, Warsaw, 1982.

[Wat97] John Watrous. On the power of 2-way quantum finite state automata. Technical Report CS-TR-1997-1350, University of Wisconsin, 1997. (Also available at citeseer.ist.psu.edu/article/watrous97power.html).

[Wat98] John Watrous. *Space-bounded quantum computation*. PhD thesis, University of Wisconsin - Madison, USA, 1998.

[YS] Abuzer Yakaryılmaz and A. C. Cem Say. Languages recognized by nondeterministic quantum finite automata. *Quantum Information and Computation*. (To Appear) (Also available at arXiv:0902.2081).

[YS09a] Abuzer Yakaryılmaz and A. C. Cem Say. Efficient probability amplification in two-way quantum finite automata. *Theoretical Computer Science*, 410(20):1932–1941, 2009.

[YS09b] Abuzer Yakaryılmaz and A. C. Cem Say. Languages recognized with unbounded error by quantum finite automata. In *CSR'09: Proceedings of the Fourth International Computer Science Symposium in Russia*, volume 5675 of *Lecture Notes in Computer Science*, pages 356–367, 2009.

[YS10] Abuzer Yakaryılmaz and A. C. Cem Say. Unbounded-error quantum computation with small space bounds. in preparation, 2010.

Appendix A A 1QFA$^{\circlearrowleft}$ algorithm for L_{eq}

Theorem 10 *For any $\epsilon > 0$, there exists a 15-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_\epsilon$, which accepts any $w \in L_{eq}$ with certainty, and rejects any $w \notin L_{eq}$ with probability at least $1-\epsilon$. Moreover, the expected runtime of $\mathcal{M}_\epsilon$ on w is $O(\frac{1}{\epsilon}(2\sqrt{2})^{|w|}|w|)$.*

Proof: We will contruct a 12-state 1KWQFA recognizing $\overline{L_{eq}}$ with positive one-sided unbounded error. Let $\mathcal{M} = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ be 1KWQFA with $Q_{non} = \{p_0, p_1, p_2, q_0, q_1, q_2\}$, $Q_{acc} = \{A_1, A_2, A_3\}, Q_{rej} = \{R_1, R_2, R_3\}$. The transition function of $\mathcal{M}$ is shown in Figure 2. As before, we

Paths	$\mathsf{U}_{¢}, \mathsf{U}_a$	U_b	$\mathsf{U}_\$$
	$\mathsf{U}_{¢}\|q_0\rangle = \frac{1}{\sqrt{2}}\|p_0\rangle + \frac{1}{\sqrt{2}}\|q_0\rangle$		
path_1	$\mathsf{U}_a\|p_0\rangle = \frac{1}{2}\|p_1\rangle + \frac{1}{2}\|R_1\rangle + \frac{1}{\sqrt{2}}\|R_2\rangle$	$\mathsf{U}_b\|p_0\rangle = \|A_1\rangle$	$\mathsf{U}_\$\|p_0\rangle = \|R_1\rangle$
	$\mathsf{U}_a\|p_1\rangle = \frac{1}{2}\|p_1\rangle + \frac{1}{2}\|R_1\rangle - \frac{1}{\sqrt{2}}\|R_2\rangle$	$\mathsf{U}_b\|p_1\rangle = \frac{1}{\sqrt{2}}\|p_2\rangle + \frac{1}{\sqrt{2}}\|R_1\rangle$	$\mathsf{U}_\$\|p_1\rangle = \|A_1\rangle$
	$\mathsf{U}_a\|p_2\rangle = \|A_1\rangle$	$\mathsf{U}_b\|p_2\rangle = \frac{1}{\sqrt{2}}\|p_2\rangle - \frac{1}{\sqrt{2}}\|R_1\rangle$	$\mathsf{U}_\$\|p_2\rangle = \frac{1}{\sqrt{2}}\|R_2\rangle + \frac{1}{\sqrt{2}}\|A_2\rangle$
path_2	$\mathsf{U}_a\|q_0\rangle = \frac{1}{\sqrt{2}}\|q_1\rangle + \frac{1}{\sqrt{2}}\|R_3\rangle$	$\mathsf{U}_b\|q_0\rangle = \|A_2\rangle$	$\mathsf{U}_\$\|q_0\rangle = \|R_3\rangle$
	$\mathsf{U}_a\|q_1\rangle = \frac{1}{\sqrt{2}}\|q_1\rangle - \frac{1}{\sqrt{2}}\|R_3\rangle$	$\mathsf{U}_b\|q_1\rangle = \frac{1}{2}\|q_2\rangle + \frac{1}{2}\|R_2\rangle + \frac{1}{\sqrt{2}}\|R_3\rangle$	$\mathsf{U}_\$\|q_1\rangle = \|A_3\rangle$
	$\mathsf{U}_a\|q_2\rangle = \|A_2\rangle$	$\mathsf{U}_b\|q_2\rangle = \frac{1}{2}\|q_2\rangle + \frac{1}{2}\|R_2\rangle - \frac{1}{\sqrt{2}}\|R_3\rangle$	$\mathsf{U}_\$\|q_2\rangle = \frac{1}{\sqrt{2}}\|R_2\rangle - \frac{1}{\sqrt{2}}\|A_2\rangle$

Fig. 2: Specification of the transition function of $\mathcal{M}$

assume that the transitions not specified in the figure are filled in to ensure that the U_σ are unitary. As seen in the figure, $\mathcal{M}$ branches to two paths on the left end-marker. Both paths reject immediately if the input $w \in \{a,b\}^*$ is the empty string, and accept with nonzero probability, say α, if it is of the form $(\{a,b\}^* \setminus a^*b^*) \cup a^+ \cup b^+$. Otherwise, $w = a^m b^n$ $(m,n > 0)$, and the amplitudes of the paths just before the transition associated with the right end-marker in the first round are as follows:

- State p_2 has amplitude $\frac{1}{\sqrt{2}}(\frac{1}{2})^m(\frac{1}{\sqrt{2}})^n$,
- state q_2 has amplitude $\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}})^m(\frac{1}{2})^n$.

If $m = n$, then the accepting probability is zero. If $m \neq n$ (assume without loss of generality that $m = n + d$ for some $d \in \mathbb{Z}^+$), then the accepting probability is equal to

$$\left(\frac{1}{2}\right)^{m+n+1}\left(\left(\frac{1}{\sqrt{2}}\right)^m - \left(\frac{1}{\sqrt{2}}\right)^n\right)^2 = \underbrace{\left(\frac{1}{2}\right)^{m+2n+1}}_{>\left(\frac{1}{2}\right)^{\frac{3|w|}{2}+1}} \underbrace{\left(1 - \left(\frac{1}{\sqrt{2}}\right)^{d-2} + \left(\frac{1}{2}\right)^d\right)}_{>\frac{1}{16}}$$

Since α is always greater than this value,

$$g_{\mathcal{M}}(|w|) > \left(\frac{1}{2}\right)^{\frac{3|w|}{2}+5},$$

for $|w| > 0$. By Lemma 7, there exists a 15-state 1QFA$^{\circlearrowleft}$ $\mathcal{M}_\epsilon$ recognizing $\overline{L_{eq}}$ with positive one-sided bounded error and whose expected runtime is $O(\frac{1}{\epsilon}(2\sqrt{2})^{|w|}|w|)$. By swapping accepting and rejecting states of $\mathcal{M}_m$, we can get the desired machine. □