Characterizations of 1-Way Quantum Finite Automata

Alex Brodsky
Department of Computer Science
University of British Columbia
abrodsky@cs.ubc.ca

Nicholas Pippenger
Department of Computer Science
University of British Columbia
nicholas@cs.ubc.ca

October 30, 2000

Abstract

The 2-way quantum finite automaton introduced by Kondacs and Watrous[KW97] can accept non-regular languages with bounded error in polynomial time. If we restrict the head of the automaton to moving classically and to moving only in one direction, the acceptance power of this 1-way quantum finite automaton is reduced to a proper subset of the regular languages.

In this paper we study two different models of 1-way quantum finite automata. The first model, termed measure-once quantum finite automata, was introduced by Moore and Crutchfield[MC00], and the second model, termed measure-many quantum finite automata, was introduced by Kondacs and Watrous[KW97].

We characterize the measure-once model when it is restricted to accepting with bounded error and show that, without that restriction, it can solve the word problem over the free group. We also show that it can be simulated by a probabilistic finite automaton and describe an algorithm that determines if two measure-once automata are equivalent.

We prove several closure properties of the classes of languages accepted by measure-many automata, including inverse homomorphisms, and provide a new necessary condition for a language to be accepted by the measure-many model with bounded error. Finally, we show that piecewise testable sets can be accepted with bounded error by a measure-many quantum finite automaton, in the process introducing new construction techniques for quantum automata.

1 Introduction

In 1997 Kondacs and Watrous[KW97] showed that a 2-way quantum finite automaton (2QFA) could accept the language $L = a^n b^n$ in linear time with bounded error. The ability of the reading head to be in a superposition of locations rather than in a single location at any time during the computation gives the 2QFA its power. Even if we restrict the head of a 2-way quantum finite automaton from moving left, we can still construct a 2QFA that can accept the language $L' = \{x \in \{a,b\}^* \mid |x|_a = |x|_b\}$ in linear time with bounded error. However, if we restrict the head of a 2QFA to moving right on each transition, we get the 1-way quantum finite automaton of Kondacs and Watrous[KW97], which, when accepting with bounded error, can only accept a proper subset of the regular languages.

If the reading head is classical then quantum mechanical evolution hinders language acceptance; restricting the set of languages accepted by 1-way quantum finite automata with bounded error to a proper subset of the regular languages[KW97].

During its computation, a 1-way QFA performs measurements on its configuration. Since the acceptance capability of a 1-way QFA depends on the measurements that the QFA may perform during the computation, we investigate two models of 1-way QFAs that differ only in the type of measurement that they perform during the computation.

The first model, termed measure-once quantum finite automata (MO-QFAs), is similar to the one introduced by Moore and Crutchfield[MC00]. The second model, termed measure-many quantum finite automata (MM-QFAs), is similar to the one introduced by Kondacs and Watrous[KW97], and is more complex than the MO-QFA. The main difference between the two models is that a measure-once automaton performs one measurement at the end of its computation, while a measure-many automaton performs a measurement after every transition. This makes the measure-many model more powerful than the measure-once model, where the power of a model refers to the acceptance capability of the corresponding automata.

First, we present results dealing with MO-QFAs. We show that the class of languages accepted by MO-QFAs with bounded error is exactly the class of group languages. Consequently, this class of languages accepted by MO-QFAs is closed under inverse homomorphisms, word quotients, and boolean operations. We show that MO-QFAs that do not accept with bounded error can accept non-regular languages and, in particular, can solve the word problem over the free group. We also describe an algorithm that determines if two MO-QFAs are equivalent and prove that probabilistic finite automata (PFAs) can simulate MO-QFAs.

Second, we shift our focus to MM-QFAs. We show that the classes of languages accepted by these automata are closed under complement, inverse homomorphisms, and word quotients. We prove by example that the class of languages accepted by MM-QFAs with bounded error is not closed under homomorphisms, and prove a necessary condition for membership within this class. We also relate the sufficiency of this condition to the question of whether the class is closed under boolean operations. Finally, we show, by construction, that MM-QFAs can accept piecewise testable sets with bounded error and introduce novel concepts for constructing MM-QFAs.

The rest of the paper is organized in the following way: Section 2 contains the definitions of the quantum automata and background information, Section 3 discusses measure-once quantum finite automata, Section 4 discusses measure-many quantum finite automata, and Section 5 summarizes.

2 Definitions and Background

2.1 Definition of MO-QFA

A measure-once quantum finite automaton is defined by a 5-tuple

$$M = (Q, \Sigma, \delta, q_0, F)$$

where Q is a finite set of states, Σ is a finite input alphabet with an end-marker symbol \$, δ is the transition function

$$\delta : Q \times \Sigma \times Q \to \mathbb{C}$$

that represents the probability density amplitude that flows from state q to state q' upon reading symbol σ, the state q_0 is the initial configuration of the system, and F is the set of accepting states. For all states $q_1, q_2 \in Q$ and symbols $\sigma \in \Sigma$ the function δ must be unitary, thus satisfying the condition

$$\sum_{q' \in Q} \overline{\delta(q_1, \sigma, q')} \delta(q_2, \sigma, q') = \begin{cases} 1 & q_1 = q_2 \\ 0 & q_1 \neq q_2 \end{cases} . \tag{1}$$

We assume that all input is terminated by the end-marker \$; this is the last symbol read before the computation terminates. At the end of a computation M measures its configuration; if it is in an accepting state then it accepts, otherwise it rejects. This definition is equivalent to that of the QFA defined by Moore and Crutchfield[MC00].

The configuration of M is a linear superposition of states and is represented by an n-dimensional complex unit vector, where $n = |Q|$. This vector is denoted by

$$|\Psi\rangle = \sum_{i=1}^{n} \alpha_i |q_i\rangle$$

where $\{|q_i\rangle\}$ is the set orthonormal basis vectors corresponding to the states of M. The coefficient α_i is the probability density amplitude of M being in state q_i. Since $|\Psi\rangle$ is a unit vector, it follows that $\sum_{i=1}^{n} |\alpha_i|^2 = 1$.

The transition function δ is represented by a set of unitary matrices $\{U_\sigma\}_{\sigma \in \Sigma}$ where U_σ represents the unitary transitions of M upon reading symbol σ. If M is in configuration $|\Psi\rangle$ and reads symbol σ then the new configuration of M is denoted by

$$|\Psi'\rangle = U_\sigma |\Psi\rangle = \sum_{q_i, q_j \in Q} \alpha_i \delta(q_i, \sigma, q_j) |q_j\rangle.$$

Measurement is represented by a diagonal zero-one projection matrix P where $P_{ii} = [q_i \in F]$. The probability of M accepting string x is defined by

$$p_M(x) = \langle \Psi_x | P | \Psi_x \rangle = \| P |\Psi_x\rangle \|^2$$

where $|\Psi_x\rangle = U(x)|q_0\rangle = U_{x_n} U_{x_{n-1}} \ldots U_{x_1} |q_0\rangle$.

2.2 Definition of MM-QFA

A measure-many quantum finite automaton is defined by a 6-tuple

$$M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$$

where Q is a finite set of states, Σ is a finite input alphabet with an end-marker symbol \$, δ is a unitary transition function of the same form as for an MO-QFA, and the state q_0 is the initial configuration of M. The set Q is partitioned into three subsets: Q_{acc} is the set of halting accepting states, Q_{rej} is the set of halting rejecting states, and Q_{non} is the set of non-halting states.

The operation of an MM-QFA is similar to that of an MO-QFA except that after every transition M measures its configuration with respect to the three subspaces that correspond to the three subsets Q_{non}, Q_{acc}, and Q_{rej}: $E_{non} = Span(\{|q\rangle \mid q \in Q_{non}\})$, $E_{acc} = Span(\{|q\rangle \mid q \in Q_{acc}\})$, and $E_{rej} = Span(\{|q\rangle \mid q \in Q_{rej}\})$. If the configuration of M is in E_{non} then the computation continues; if the configuration is in E_{acc} then M accepts, otherwise it rejects. After every measurement the superposition collapses into the measured subspace and is renormalized.

Just like MO-QFAs, the configuration of an MM-QFA is represented by a complex n-dimensional vector, the transition function is represented by unitary matrices, and measurement is represented by diagonal zero-one projection matrices that project the vector onto the respective subspaces.

The definition of an MM-QFA is almost identical to the definition by Kondacs and Watrous in[KW97]. The only difference is that we only require one end-marker at the end of the tape, rather than two end-markers, at the start and end of the tape; this does not affect the acceptance power of the automaton; see Appendix A for further details.

Since M can have a non-zero probability of halting part-way through the computation, it is useful to keep track of the cumulative accepting and rejecting probabilities. Therefore, in some cases we use the representation, of Kondacs and Watrous[KW97] that represents the state of M as a triple $(|\Psi\rangle, p_{acc}, p_{rej})$, where p_{acc} and p_{rej} are the cumulative probabilities of accepting and rejecting. The evolution of M on reading symbol σ is denoted by

$$(P_{non}|\Psi'\rangle,\ p_{acc} + \|P_{acc}|\Psi'\rangle\|^2,\ p_{rej} + \|P_{rej}|\Psi'\rangle\|^2)$$

where $|\Psi'\rangle = U_\sigma|\Psi\rangle$, and P_{acc}, P_{rej}, and P_{non} are the diagonal zero-one projection matrices that project the configuration onto the non-halting, accepting and rejecting subspaces.

2.3 Language Acceptance

A QFA M is said to accept a language L with cut-point λ if for all $x \in L$ the probability of M accepting x is greater than λ and for all $x \notin L$ the probability of M accepting x is at most λ. A QFA M accepts L with bounded error if there exists an $\epsilon > 0$ such that for all $x \in L$ the probability of M accepting x is greater than $\lambda + \epsilon$ and for all $x \notin L$ the probability of M accepting x is less than $\lambda - \epsilon$. We call ϵ the margin.

We partition the languages accepted by QFAs into several natural classes. Let the class $\mathbf{RMO}_\epsilon$ be the set of languages accepted by an MO-QFA with margin of at least ϵ. Let the restricted class of languages, $\mathbf{RMO} = \cup_{\epsilon>0}\mathbf{RMO}_\epsilon$, be the set of languages accepted by an MO-QFA with bounded error, and let the unrestricted class of languages, $\mathbf{UMO} = \mathbf{RMO}_0$, be the set of languages accepted by an MO-QFA with unbounded error. We define the languages classes $\mathbf{RMM}_\epsilon$, $\mathbf{RMM}$ and $\mathbf{UMM}$ accepted by an MM-QFA in a similar fashion.

Since the cut-point of a QFA can be arbitrarily raised or lowered, we could without loss of generality fix the cut-point to be $\frac{1}{2}$. However, for the purposes of presentation we use the general cut-point definition stated above.

2.4 Reversible Finite Automata

Unitary operations are reversible, thus QFAs bear strong resemblance to various variants of reversible finite automata. A group finite automaton (GFA) is a deterministic finite automata (DFA) $M = (Q, \Sigma, \delta, q_0, F)$ with the restriction that for every state $q \in Q$ and every input symbol $\sigma \in \Sigma$ there exists exactly one state $q' \in Q$ such that $\delta(q', \sigma) = q$, i.e. δ is a complete one-to-one function and the automaton derived from M by reversing all transitions is deterministic.

A reversible finite automata (RFA) is a DFA $M = (Q, \Sigma, \delta, q_0, F)$ such that for every state $q \in Q$ and for every symbol $\sigma \in \Sigma$ there is at most one state $q' \in Q$ such that $\delta(q', \sigma) = q$, or, if there exist distinct states $q_1, q_2 \in Q$ and symbol $\sigma \in \Sigma$ such that $\delta(q_1, \sigma) = q = \delta(q_2, \sigma)$, then $\delta(q, \Sigma) = \{q\}$. The latter type of state is called a spin state because once an RFA enters it, it will never leave it. This definition is equivalent to the one used by Ambainis and Freivalds[AF98] and is an extension of Pin's[Pin87] definition.

2.5 Previous Work

Moore and Crutchfield[MC00] introduced a variant of the MO-QFA model and investigated the model in terms of quantum regular languages (QRLs). They showed several closure properties including closure under inverse homomorphisms and derived a method for bilinearizing the representation of an MO-QFA that transforms it into a generalized stochastic system.

Kondacs and Watrous[KW97] introduced a variant of the MM-QFA that was derived from their 2QFA model. Using a technique similar to Rabin's[Rab63], Kondacs and Watrous proved that 1-way QFAs that accept with bounded error are restricted to accepting a proper subset of the regular languages and that the language $L = \{a, b\}^*b$ is not a member of that subset.

Ambainis and Freivalds[AF98] showed that MM-QFAs could accept languages with probability higher than $\frac{7}{9}$ if and only if the language could be accepted by an RFA, which is equivalent to being accepted with certainty by an MM-QFA. In [ABFK99] Ambainis, Bonner, Freivalds, and Kikusts, construct a hierarchy of languages such that the ith language in the hierarchy can be accepted by a MM-QFA with at most probability p_i, where the series (p_i) converges to $\frac{1}{2}$ and is strictly decreasing.

Ambainis, Nayak, Ta-Shma, and Vazirani[ANTSV99], and Nayak[Nay99], investigated how efficiently MM-QFAs can be constructed compared to DFAs. They showed that for some languages the accepting MM-QFA is exponentially larger than the corresponding DFA.

In [AI99] Amano and Iwama studied a restricted version of the 2QFA model where the head was not allowed to move right. They showed that the emptiness problem for this model is undecidable. This is another instance where quantum mechanics provides computational power that is not achievable in the classical case.

3 MO-QFAs

3.1 Bounded Error Acceptance

The restriction that MO-QFAs accept with bounded error is as limiting as in the case of PFAs[Rab63]. Since MM-QFAs can only accept a proper subset of the regular languages if they are required to accept with bounded error and since every MO-QFA can be simulated exactly by an MM-QFA, the class **RMO** is a proper subset of the regular languages. The class **RMO** is exactly the class of languages accepted by group finite automata (GFAs), otherwise known as group languages, and whose syntactic semigroups are groups, see Eilenberg[Eil76]. This result is implied by Theorem 7 in [MC00] but is not stated in the paper. To prove this result we first need Lemma 3.1.

Lemma 3.1 *Let U be a unitary matrix. For any $\epsilon > 0$ there exists an integer $n > 0$ such that for all vectors x, where $\|x\|^2 \leq 1$, it is true that $\|(I - U^n)x\|^2 < \epsilon$.*

Proof: Let $m = dim(U)$. Since U is a normal matrix, U^n can be written as

$$U^n = PD^nP^{-1}$$

where P is a unitary matrix and D is the diagonal matrix of eigenvalues with the jth eigenvalue having the form $e^{i\pi r_j}$[Ort87]. If all eigenvalues in D are rotations through rational fractions of π, i.e. r_j is rational, then let $n = 2\prod_{j=1}^{m} q_j$ where q_j is the denominator of r_j. Thus $D^n = I$ and we are done.

Otherwise, at least one eigenvalue is a rotation of unity through an irrational fraction of π. Let $l \leq m$ be the number of these eigenvalues. For the other $m-l$ eigenvalues compute n, just as above, and let $D' = D^n$. The value of the jth element on the diagonal of D' is either 1 or $e^{i\pi n r_j}$ where r_j is some irrational real number. Consider taking D' to some power $k \in \mathbb{Z}^+$. The values that are 1 do not change, but the other l values that are of the form $e^{i\theta_j k}$ where $\theta_j = \pi n r_j$, form a vector that varies through a dense subset in an l-dimensional torus. Hence, there exists k such that the l-dimensional vector is arbitrarily close to $\vec{1}$. Thus, for any $\epsilon' > 0$ there exists a $k > 0$ such that

$\|(I - D'^k)\vec{1}\|^2 < \epsilon'$. Hence

$$\begin{aligned}
\|(I - U^{nk})x\|^2 &= \|(I - PD^{nk}P^{-1})x\|^2 \\
&= \|P(I - D'^k)P^{-1}x\|^2 \\
&\leq \|(I - D'^k)m\vec{1}\|^2 \\
&= m^2\|(I - D'^k)\vec{1}\|^2 \\
&\leq m^2\epsilon'.
\end{aligned}$$

Select ϵ' such that $\epsilon' < \frac{\epsilon}{m^2}$ to complete the proof. ■

Lemma 3.2, due to Bernstein and Vazirani[BV97], states that if two configurations are close, then the differences in probability distributions of the configurations is small. This lemma relates the closeness of configurations to the variation distance between their probability distributions and allows us to partition the set of reachable configurations into equivalence classes. The variation distance between two probability distributions is the maximum difference in the probabilities of the same event occurring with respect to both distributions.

Lemma 3.2 (Bernstein and Vazirani, 1997)
Let $|\psi\rangle$ and $|\varphi\rangle$ be two complex vector such that $\| |\psi\rangle\|^2 = \| |\varphi\rangle\|^2 = 1$ and $\| |\psi\rangle - |\varphi\rangle\|^2 < \epsilon$. The total variation distance between the probability distributions resulting from measurement of $|\psi\rangle$ and $|\varphi\rangle$ is at most 4ϵ.

Theorem 3.3 follows from these two lemmas.

Theorem 3.3 *A language L can be accepted by an MO-QFA with bounded error if and only if it can be accepted by a GFA.*

Proof: The 'if' direction follows from the fact that the transition function for a GFA is also a valid transition function for an MO-QFA that can accept the same language with certainty.

For the 'only if' direction, by contradiction, assume that there exists a language L that can be accepted by an MO-QFA with bounded error but cannot be accepted by a GFA. Since the class **RMO** is a subset of the regular languages, L must be regular. Let $M = (Q, \Sigma, \delta, q_0, F)$ be an MO-QFA that accepts L with bounded error. If two strings x and y take M into the same reachable configuration, then for any string z the probability of M accepting xz is equal to the probability of M accepting yz, which means that $xz \in L$ if and only if $yz \in L$. Therefore, the space of reachable configurations of M's computation can be partitioned into a finite number of equivalence classes defined by the corresponding minimal DFA for L.

Let $|\psi\rangle$ and $|\varphi\rangle$ denote reachable configurations of M and let $\sim_L$ be the right invariant equivalence relation induced by L. Since L cannot be accepted by a GFA, there must exist two distinct equivalence classes $[y]$ and $[y']$, an equivalence class $[x]$, and a symbol $\sigma \in \Sigma$, such that $[y\sigma] \sim_L [y'\sigma] \sim_L [x]$. If U_σ is the transition matrix for symbol σ, $|\psi\rangle \in [y]$ and $|\varphi\rangle \in [y']$ then $U_\sigma|\psi\rangle \in [x]$ and $U_\sigma|\varphi\rangle \in [x]$.

Since M accepts L with bounded error, let ϵ be the margin. By Lemma 3.1 there exists an integer $k > 0$ such that $\|(I - U_\sigma^k)|\psi\rangle\|^2 < \frac{\epsilon}{4}$ and $\|(I - U_\sigma^k)|\varphi\rangle\|^2 < \frac{\epsilon}{4}$. Hence, $U_\sigma^k|\psi\rangle \in [y]$ because if

$$\begin{aligned}
\|(I - U_\sigma^k)|\psi\rangle\|^2 &= \| \, |\psi\rangle - U_\sigma^k|\psi\rangle\|^2 \\
&= \|V(|\psi\rangle - U_\sigma^k|\psi\rangle)\|^2 \\
&< \frac{\epsilon}{4}
\end{aligned}$$

where V is an arbitrary unitary matrix, then by Lemma 3.2 the probability of $VU_\sigma^k|\psi\rangle$ being measured in a particular state is within ϵ of $V|\psi\rangle$ being measured in the same state; this probability is less than the margin. Similarly $U_\sigma^k|\varphi\rangle \in [y']$. Hence $[y] \sim_L [y\sigma^k]$ and $[y'] \sim_L [y'\sigma^k]$.

We assumed that $[x] \sim_L [y\sigma] \sim_L [y'\sigma]$ and showed that $[y] \sim_L [y\sigma^k]$ and $[y'] \sim_L [y'\sigma^k]$; therefore, $[y] \sim_L [x\sigma^{k-1}] \sim_L [y']$. Let z be the string that distinguishes $[y]$ and $[y']$. Then the string $\sigma^{k-1}z$ partitions $[x]$ into at least two distinct equivalence classes, but this is a contradiction. Therefore, there cannot exist a language L that can be accepted by an MO-QFA with bounded error but not by a GFA. ∎

Theorem 3.3 implies that $\mathbf{RMO}_\epsilon = \mathbf{RMO}_{\epsilon'}$ for all $\epsilon, \epsilon' > 0$, hence there are most two distinct classes of languages accepted by MO-QFAs, the restricted class **RMO**, which is equivalent to the class of languages accepted by a GFA, and the unrestricted class **UMO**.

It follows immediately from Theorem 3.3 that the class **RMO** is closed under boolean operations, inverse homomorphisms, and word quotients, and is not closed under homomorphisms.

3.2 Non-Regular Languages

Unlike the class **RMO**, the class **UMO** contains languages that are non-regular. This is not surprising given that Rabin[Rab63] proved a similar result for PFAs. In fact our proof closely mimics Rabin's[Rab63] technique.

Lemma 3.4 *Let $L = \{x \in \{a,b\}^* \mid |x|_a \neq |x|_b\}$, there exists a 2-state MO-QFA M that accepts L with cut-point 0.*

Proof: Let $M = (Q, \Sigma, \delta, q_0, F)$ where $Q = \{q_0, q_1\}$, $\Sigma = \{a, b\}$, $F = \{q_1\}$, and δ is defined by the transition matrices

$$U_a = U_b^{-1} = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

where α is an irrational fraction of π. Since U_a is a rotation matrix and α is an irrational fraction of π, the orbit formed by applying U_a to $|q_0\rangle$ is dense in the circle, and there exists only one k, such that $U_a^k|q_0\rangle = |q_0\rangle$, namely $k = 0$. This also holds for $U_b = U_a^{-1}$. Thus, $U(x)|q_0\rangle = |q_0\rangle$ if and only if the number of U_a rotations applied to $|q_0\rangle$ is equal to the number of U_b rotations, which is true if and only if the $|x|_a = |x|_b$. Otherwise, M has a non-zero probability of halting in state q_1. ∎

Lemma 3.4 implies that the class **RMO** is properly contained within the class **UMO** and therefore the two classes are distinct.

The MO-QFA in Lemma 3.4 solves the word problem for the infinite cyclic group: is the input word equal to the identity element in the group, where the group has only one generator element, say a, and its inverse $b = a^{-1}$. We can generalize this result to the general word problem for the free group. The word problem for a free group is to decide whether or not a product of a sequence of elements of the free group reduces to the identity[LZ77].

Lemma 3.5 *The word problem for the free group language can be accepted by an MO-QFA.*

Proof: Construct a free group of rotation matrices drawn from the group SO_3 as discussed by Wagon[Wag85]. Let $M = (Q, \Sigma, \delta, q_0, F)$ be a 3-state MO-QFA where $\Sigma = \{a, a^{-1}, b, b^{-1}, ...\}$ such that $|\Sigma|$ is equal to the sum of the number of rotation matrices and their inverses, δ is defined by the rotation matrices and their inverses, and $F = \{q_0\}$. The MO-QFA will accept identity words with certainty and reject non-identity words with a strictly non-zero probability, hence solving the word problem for the free group. ■

3.3 Equivalence of MO-QFAs

In classical automata theory there is an algorithm to determine if two automata are equivalent. We say that QFAs M and M' are equivalent if their probability distributions over Σ^* are the same: for every word $x \in \Sigma$, the probability of M accepting x is equal to the probability of M' accepting x. In order to determine if two MO-QFAs are equivalent we first bilinearize them using the method detailed by Moore and Crutchfield[MC00]; this yields two generalized stochastic systems. We then apply Paz's[Paz71, Page 21, Page 140] method for testing stochastic system equivalence to the generalized stochastic systems to determine if they have the same distribution.

3.4 Simulation of MO-QFAs by PFAs

Most classical computation is either deterministic or probabilistic, hence it is useful to ask how probabilistic automata compare to their quantum analogs. In the case of MO-QFAs, any language accepted by an MO-QFA can also be accepted by a PFA. If L can be accepted by an MO-QFA with bounded error, then it can also be accepted by a PFA with bounded error.

Theorem 3.6 *Let M be an MO-QFA that accepts L with cut-point λ then:*

1. *There exists a PFA that accepts L with some cut-point λ'.*
2. *If M accepts L with bounded error, then there exists a PFA that accepts L with bounded error.*

Proof: The second result follows from Theorem 3.3 because every GFA is also a PFA.

Since we can bilinearize M, L is a generalized cut-point event (GCE)[Paz71, Page 153]. Since the class of GCEs is equal to the class of probabilistic cut-point events

(PCEs)[Paz71, Page 153], which are accepted by PFAs, there exists a PFA that can accept L with some cut-point λ'. ■

Combining Theorem 3.6 with Lemma 3.5 yields a new insight into the languages accepted by PFAs:

Corollary 3.7 *The word problem for the free group language can be solved by a PFA.*

4 MM-QFAs

Measure-many quantum finite automata are more powerful than MO-QFAs because a measurement is performed after every transition. This allows the machine to terminate before reading the entire string and simulate the spin states of RFAs.

As mentioned before, an MM-QFA uses one end-marker while the Kondacs and Watrous [KW97] 1-way QFA uses two end-markers. The second marker does not add any more power to the model, see Appendix A, but makes constructing an MM-QFA easier because the MM-QFA can start in an arbitrary configuration. Hence, for the sake of conciseness and clarity we shall assume that some of the MM-QFAs constructed in the following proofs have two end-markers.

4.1 Closure Properties

Unlike the closure properties of the classes **RMO** and **UMO**, which can be derived easily, the closure properties of the classes **RMM** and **UMM** are not as evident and in one important case unknown. We show that the classes **RMM** and **UMM** are closed under complement, inverse homomorphism and word quotient. Similar to the class **RMO**, the class **RMM** is not closed under homomorphisms. It remains an open problem to determine whether the classes **RMM** and **UMM** are closed under boolean operations.

Theorem 4.1 proves that both classes are closed under complement and inverse homomorphisms by showing that each class $\mathbf{RMM}_\epsilon$ is closed under complement and inverse homomorphisms; closure under word quotient follows directly from the latter, given the presence of end-markers.

Theorem 4.1 *The class* $\mathbf{RMM}_\epsilon$ *is closed under complement, inverse homomorphisms, and word quotient.*

Proof: Closure under complement follows from the fact that we can exchange the accept and reject states of the MM-QFA. This exchanges the probabilities of acceptance and rejection but does not affect the margin.

Given an MM-QFA M and a homomorphism h we construct an MM-QFA M' that accepts $h^{-1}(L)$. Let $M = (Q, \Sigma, \delta, Q_{acc}, Q_{rej})$ and $M' = (Q', \Sigma, \delta', Q'_{acc}, Q'_{rej})$. Assume that δ and δ' are defined in terms of matrices $\{U_\sigma\}_{\sigma\in\Sigma}$ and $\{U'_\sigma\}_{\sigma\in\Sigma}$. Unlike the proof for MO-QFAs in [MC00], the direct construction of

$$U'_\sigma = U(h(\sigma))$$

will not work because a measurement occurs between transitions, and combining transitions without taking this into account could produce incorrect configurations. After every transition some amount of probability amplitude is placed in the halting states and should not be allowed to interact with the non-halting states in the following transitions. This is achieved by storing the amplitude in additional states; this technique is also used in [ANTSV99]. Assume without loss of generality that

$$\begin{aligned} Q_{non} &= \{q_i \in Q \mid 0 \leq i < n_{non}\} \\ Q_{halt} &= \{q_i \in Q \mid n_{non} \leq i < n\} \end{aligned}$$

where $n = |Q|$ and $n_{non} = |Q_{non}|$. Let $m = \max_{\sigma \in \Sigma}\{|h(\sigma)|\}$ and let

$$Q' = Q \cup Q'_{halt}$$

where

$$\begin{aligned} Q'_{halt} &= \{q_i\}_{i=n+1}^{n+m(n-n_{non})} \\ Q'_{acc} &= Q_{acc} \cup \{q_{n+j(i-n_{non})} \in Q'_{halt} \mid q_i \in Q_{acc}, 1 \leq j \leq m\} \\ Q'_{rej} &= Q_{rej} \cup \{q_{n+j(i-n_{non})} \in Q'_{halt} \mid q_i \in Q_{rej}, 1 \leq j \leq m\}. \end{aligned}$$

Intuitively, we replicate the halting states m times; each replication is termed a halting state set.

We construct δ' from the matrices of δ. Let V_σ be a unitary block matrix

$$V_\sigma = U_{shift} \begin{bmatrix} U_\sigma & \\ & I_{m(n-n_{non})} \end{bmatrix}$$

where

$$U_{shift} = \begin{bmatrix} I_{n_{non}} & & \\ & & I_{n-n_{non}} \\ & I_{m(n-n_{non})} & \end{bmatrix}.$$

The matrix U_{shift} is a unitary matrix that shifts the amplitudes in the halting set i to the halting set $i+1$ and the amplitude in halting set m to halting set 0. In analogy to the MO-QFA case where $U'_\sigma = U(h(\sigma))$, for MM-QFAs let

$$U'_\sigma = V(h(\sigma)) = V_{x_k} V_{x_{k-1}} \ldots V_{x_1}$$

where $h(\sigma) = x = x_1 x_2 \ldots x_k$ and $k \leq m$.

After every x_i sub-transition the halting amplitude is shifted and stored in the $m+1$ halting sets of states. When the sub-transition is done, the amplitude in halt state set 0 is zero, which is what is required to prevent unwanted interactions. A minimum of m sub-transitions must occur before halting set m contains non-zero amplitude, but no more than m sub-transitions will ever occur; therefore halting set 0 will never receive non-zero amplitude from halting set m. Since M' has the same distribution as M, the margin will not decrease.

Closure under word quotient follows from closure under inverse homomorphism and the presence of both end-markers. ■

Just like the class **RMO**, the class **RMM** is not closed under homomorphisms.

Theorem 4.2 *The class* **RMM** *is not closed under homomorphisms.*

Proof: Let $L = \{a, b\}^*c$ and define a homomorphism h to be $h(a) = a$, $h(b) = b$, and $h(c) = b$. Since L can be accepted by an RFA, $L \in$ **RMM** [AF98], but $h(L) = \{a, b\}^*b \notin$ **RMM**, the result follows. ■

A more interesting question is whether the classes **RMM** and **UMM** are closed under boolean operations. Unlike MO-QFAs that have two types of states: accept and reject, MM-QFAs have three types of states: accept, reject, and non-halt. Consequently, the standard procedure of taking the tensor product of two automata to obtain their intersection or union does not work. A general method of intersecting two MM-QFAs is not known. Thus, it is not known whether **RMM** and **UMM** are closed under boolean operations.

4.2 Bounded Error Acceptance

The restriction of bounded error acceptance reduces the class of languages that an MM-QFA can accept to a proper subclass of the regular languages[KW97]. To study the languages in class **RMM**, we look at their corresponding minimal automata. Ambainis and Freivalds[AF98] showed that if the minimal DFA $M(L) = (Q, \Sigma, \delta, q_0, F)$ contains an irreversible construction, defined by two distinct states $q_1, q_2 \in Q$ and strings $x, y, z \in \Sigma^*$ such that $\delta(q_1, x) = \delta(q_2, x) = q_2$, $\delta(q_2, y) \in F$ and $\delta(q_2, z) \notin F$, then an RFA cannot accept L and an MM-QFA cannot accept it with a probability greater than $\frac{7}{9}$; this condition is both sufficient and necessary.

We derive a similar necessary condition for a language L to be a member of the class **RMM**. This condition, called the partial order condition, is a relaxed version of a condition defined by Meyer and Thompson[MT69]. A language L is said to satisfy the partial order condition if the minimal DFA for L satisfies the partial order condition. A DFA satisfies the partial order condition if it does not contain two distinguishable states $q_1, q_2 \in Q$ such that there exists strings $x, y \in \Sigma^+$ where $\delta(q_1, x) = \delta(q_2, x) = q_2$, and $\delta(q_2, y) = q_1$. States q_1 and q_2 are said to be distinguishable if there exists a string $z \in \Sigma^*$ such that $\delta(q_1, z) \in F$ and $\delta(q_2, z) \notin F$ or vice versa[HU79]. Using a result in [KW97], Theorem 4.3 proves that the partial order condition is necessary for an MM-QFA to accept L with bounded error.

Theorem 4.3 *If* $M = (Q, \Sigma, \delta, q_0, F)$ *is a minimal DFA for language* L *that does not satisfy the partial order condition then* $L \notin$ **RMM**.

Proof: By contradiction, assume that $L \in$ **RMM**. Let $L_b = \{a, b\}^*b$. Since the minimal DFA for L does not satisfy the partial order condition there exist states $q_1, q_2 \in Q$ and strings $x, y \in \Sigma^+$ as defined above and a distinguishing string $z \in \Sigma^*$ such that $\delta(q_1, z) \notin F$ if and only if $\delta(q_2, z) \in F$. Without loss of generality assume that $\delta(q_1, z) \notin F$ and $\delta(q_2, z) \in F$.

Let s be the shortest string such that $\delta(q_0, s) = q_1$. Let $L' = s^{-1}Lz^{-1}$. By Theorem 4.1, $L' \in \mathbf{RMM}$. Define the homomorphism h as

$$\begin{aligned} h(a) &= xy \\ h(b) &= x \\ h(\Sigma - \{a, b\}) &= xy, \end{aligned}$$

where the last definition is for completeness. Let $L'' = h^{-1}(L')$. By Theorem 4.1 $L'' \in \mathbf{RMM}$. But $L'' = L_b \notin \mathbf{RMM}$, a contradiction. ■

The partial order condition is so named because once the state q_2 is visited, there is no path back to state q_1. Thus, there exists a partial order on the states of the DFA. We do not know whether this condition is also sufficient for MM-QFA acceptance with bounded error. While we do not know whether the class **RMM** is closed under boolean operations, Theorem 4.6 relates closure under intersection to the partial order condition.

Lemma 4.4 *Let M be a DFA that satisfies the partial order condition. The minimal DFA M' that accepts $L(M)$ satisfies the partial order condition.*

Proof: Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA and $M' = (Q', \Sigma, \delta', q'_0, F')$ be the corresponding minimal DFA. Assume by contradiction that M' does not satisfy the partial order condition. Hence, M' has two states that correspond to the equivalence classes $[q'_1]$ and $[q'_2]$ such that $[q'_1]x \sim_L [q'_2]x \sim_L [q'_2]$ and $[q'_2]y \sim_L [q'_1]$. By the Myhill-Nerode theorem[HU79], the equivalence classes partition the set of reachable states in Q. Hence, for each equivalence class $[q'_i]$ there is a corresponding subset of Q. Let Q_1 and Q_2 denote the subsets of Q corresponding to the equivalence classes $[q'_1]$ and $[q'_2]$ and assign an arbitrary order on each subset. Select the first state, say $p_1 \in Q_1$, and define the set $R = \{q \in Q_2 \mid \exists n, m \in \mathbb{Z}^+,\ \delta(p_1, x^m) = \delta(q, x^n) = q\}$. If there exists a state $r \in R$ and string $y \in \Sigma^+$ such that $\delta(r, y) = p_1$, then M does not satisfy the partial order condition, and this is a contradiction. Otherwise, there does not exist a $y \in \Sigma^+$ such that $\delta(r, y) = p_1$ for all $r \in R$. In this case there is a partial order on p_1 and on $Q_1 \backslash \{p_1\}$ because p_1 will never be visited again if M reads a sufficient number of xs. Remove p_1 from Q_1 and repeat the procedure on $p_2 \in Q_1$. After a finite number of iterations we will either find a p_i that satisfies our requirements, which means that M does not satisfy the partial order condition and is a contradiction, or none of the states in Q_1 will have the required characteristics, in which case M' satisfies the partial order condition. Therefore, if M satisfies the partial order condition, so will its minimal equivalent M'. ■

Lemma 4.5 *Let L' and L'' be languages that satisfy the partial order condition. Then $L = L' \cap L''$ also satisfies the partial order condition.*

Proof: Let $M' = (Q', \Sigma, \delta', q'_0, F')$ be the minimal DFA accepting the language L' and let $M'' = (Q'', \Sigma, \delta'', q''_0, F'')$ be the minimal DFA accepting the language L''. We first construct an automaton M that accepts $L' \cap L''$ by combining M' and M'' using a direct product. Define $M = (Q, \Sigma, \delta, q_{00}, F)$ where $Q = Q' \times Q''$, $q_{00} = (q'_0, q''_0)$, $F = \{(q', q'') \in Q \mid q' \in F' \ \wedge\ q'' \in F''\}$ and $\delta((q', q''), \sigma) = (\delta'(q', \sigma), \delta''(q'', \sigma))$.

We argue that if M' and M'' satisfy the partial order condition, then so will M. Assume, by contradiction, that M does not satisfy the partial order condition. Then there exist two states $q_{ij} = (q'_i, q''_j)$ and $q_{kl} = (q'_k, q''_l)$ and strings $x, y, z \in \Sigma^+$ such that $\delta(q_{ij}, x) = \delta(q_{kl}, x) = q_{kl}$, $\delta(q_{kl}, y) = q_{ij}$ and $\delta(q_{ij}, z) \in F$ if and only if $\delta(q_{kl}, z) \notin F$. In the first case assume that either $i \neq k$ or $j \neq l$, and without loss of generality, assume the former. Then there exists state $q'_i \in Q'$ and state $q'_k \in Q'$ such that $\delta'(q'_i, x) = \delta'(q'_k, x) = q'_k$, $\delta_1(q'_k, y) = q'_i$. But this means that M' does not satisfy the partial order condition, a contradiction. In the second case assume that $i = k$ and $j = l$. This implies that $q_{ij} = q_{kl}$ and hence there cannot exist a string z that distinguishes the two states, also a contradiction. Therefore M must satisfy the condition.

Since M satisfies the partial order condition and accepts L, by Lemma 4.4 the minimal automaton that accepts L satisfies the partial order condition, and hence L itself, satisfies the partial order condition. ■

Theorem 4.6 *If the partial order condition is sufficient for acceptance with bounded error by MM-QFAs then the class* **RMM** *is closed under intersection.*

Proof: By Lemma 4.5 the intersection of two languages that satisfy the partial order condition is a language that satisfies the partial order condition. ■

One method for proving that the class **RMM** is not closed under intersection involves intersecting two languages in **RMM** and showing that the resulting language is not in **RMM**. By Theorem 4.6 this method will not work unless the partial order condition is insufficient. To study whether the partial order condition is sufficient, as well as necessary, we show that a well known class of languages can be accepted by an MM-QFA with bounded error.

4.3 Piecewise Testable Sets

A piecewise testable set is a boolean combination of sets of the form

$$L_z = \Sigma^* z_1 \Sigma^* z_2 \Sigma^* ... \Sigma^* z_n \Sigma^*$$

where $z_i \in \Sigma$ [Per94]. Intuitively, L_z is the language of strings that contain the successive symbols of z as a subsequence; we call such a language a partial piecewise testable set.

Piecewise testable sets, introduced by Simon in [Sim75], form a natural family of star-free languages. Such sets define a class of computations that wait for a partially ordered sequence of trigger events (input symbols); if a trigger event (symbol) is read that is not next in the sequence, it is simply ignored. Another natural interpretation of piecewise testable sets is subsequence searching. Consider a language where a word is said to be in the language if it contains a finite boolean combination of subsequences. Such a language is a piecewise testable set and word acceptance corresponds to searching the words for the required subsequences. Finally, such languages belong to a class of languages whose MM-QFAs have an arbitrarily large, but finite, set of ordered states.

We show, by construction, that MM-QFAs can accept partial piecewise testable sets with bounded error. The MM-QFAs we construct accept with one-sided error and are what we call 'end-decisive'. We say that an MM-QFA accepts with positive one-sided error if it accepts strings in the language with non-zero probability and rejects strings not in the language with certainty. We say that an MM-QFA accepts with negative one-sided error if it accepts strings in the language with certainty and rejects strings not in the language with non-zero probability.

We say that an MM-QFA is end-decisive if it will not be observed in an accept state until the end-marker $ is read. An MM-QFA is co-end-decisive, if it will not be observed in a reject state until the end-marker is read.

Classes of languages that are accepted by end-decisive MM-QFAs with the same one-sided error, i.e., all positive or all negative, are closed under intersection and union. Furthermore, if language L can be accepted by an end-decisive MM-QFA with bounded error, and language L' can be accepted by an end-decisive MM-QFA with bounded one-sided error, then the union or intersection of L and L' can be accepted by an end-decisive MM-QFA with bounded error. To construct these MM-QFAs we introduce two useful concepts: junk states and trigger chains.

A junk state is a halting state of an end-decisive or co-end-decisive MM-QFA. If the MM-QFA is end-decisive, then all its junk states are reject states. If the MM-QFA is co-end-decisive, then all its junk states are accept states. An end-decisive or co-end-decisive MM-QFA may be observed in a junk state at any point of the computation. While junk states are either accept or reject states, we treat the junk state as a separate halting state. Any accept or reject state that is not a junk state is called a decisive state. Intuitively, a junk state signals a failed computation.

Each, end-decisive or co-end-decisive automata that accepts with bounded error has probability, bounded by some constant $\tau < 1$ of ending up in a junk state and a probability $1-\tau$ of ending up in a decisive state. If $\tau \not< 1$ then the amount of probability amplitude ending up in a decisive state can become arbitrary small, dropping below any fixed margin. Thus, τ must be strictly less than one for the MM-QFA to accept with bounded error; τ is independent of the input string x.

A trigger chain is a construction of junk states and transition matrices that causes a reduction in amplitude of a particular state only if the amplitude of another state is decreased, presumably by some previous transition. Trigger chains correspond directly to partial piecewise testable sets. Consider the matrix

$$X = \begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{2} & -\frac{1}{\sqrt{2}} & \frac{1}{2} \end{bmatrix}.$$

This matrix is a special case of a transition matrix introduced by Ambainis and Freivalds[AF98]. This matrix operates on three states and is a triggering mechanism of the chain. Consider the vectors

$$|\psi\rangle = (\alpha, 0, \beta)^T$$

and

$$X|\psi\rangle = \left(\frac{\alpha}{2} + \frac{\beta}{2}, \frac{\alpha}{\sqrt{2}} - \frac{\beta}{\sqrt{2}}, \frac{\alpha}{2} + \frac{\beta}{2}\right)^T.$$

The vectors $|\psi\rangle$ and $X|\psi\rangle$ are equal if and only if $\alpha = \beta$. If $\alpha \neq \beta$ then the amplitudes of the first and third state are averaged, with the remainder of the amplitude going into the second state. We define a generalized version of X by embedding it into a larger identity block matrix. Define X_i to be

$$X_i = \begin{bmatrix} I_i & & \\ & X & \\ & & I_{s-i-3} \end{bmatrix}$$

where I_m is an $m \times m$ identity matrix, X is defined as above, and s is the number of states, i.e. the size of X_i. The matrix X_i operates on a triple of states, q_i through to q_{i+2}. We assume that state q_{i+1}, the second state, is a junk state unless otherwise noted.

Theorem 4.7 *Let L_z be a partial piecewise testable set. There exists an end-decisive MM-QFA that accepts L_z with bounded positive one-sided error.*

Proof: We construct an MM-QFA M with $m+1$ states that accepts L_z where $z = z_0 z_1 ... z_n$ and $m = 2n+4$.

For each link in the trigger chain we require a junk state and a non-halting state. We order the states to correspond with the description of the X_i matrices. Specifically, the first $2n+2$ states are the non-halting states, interleaved with junk states. Each triple of states $(q_{2i}, q_{2i+1}, q_{2i+2})$ corresponds to a link of the trigger chain, of which there are $n+1$. State q_{2n+1} is the decisive accept state and state q_{2n+3} is the decisive reject state. The junk states are rejecting states.

Let $m = 2n+4$ and $M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ where

$$\begin{aligned} Q &= \{q_0, ..., q_m\} \\ Q_{junk} &= \{q_i \in Q \mid 0 < i < 2n \ \wedge \ i \equiv 1 \bmod 2\} \cup \{q_{2n+4}\} \\ Q_{acc} &= \{q_{2n+1}\} \\ Q_{rej} &= \{q_{2n+3}\}. \end{aligned}$$

Define δ by the transition matrices $\{U_\sigma\}_{\sigma\in\Sigma}$. Each transition matrix U_σ consists of a product of matrices:

$$U_\sigma = U_{\sigma,0} U_{\sigma,1} ... U_{\sigma,n}$$

where the matrices $U_{\sigma,i}$ implement the triggers.

Define $U_{\sigma,i}$ to be

$$U_{\sigma,i} = \begin{cases} S & i = 0 \ \wedge \ z_0 = \sigma \\ X_{2i-2} & 1 \leq i \leq n \ \wedge \ z_i = \sigma \\ I_{m+1} & \text{otherwise} \end{cases}$$

where

$$S = \begin{bmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I_{m-1} \end{bmatrix}.$$

The matrix S shifts the amplitude of q_0 to the junk state q_1. This is the first trigger that is activated when z_0 is read.

Finally, let the transition matrix for the end-marker \$ be

$$U_\$ = FX_{2n}$$

where

$$F = \begin{bmatrix} R & & & & & & & \\ & \ddots & & & & & & \\ & & R & & & & & \\ & & & 0 & 0 & 0 & 0 & 1 \\ & & & 0 & 1 & 0 & 0 & 0 \\ & & & 0 & 0 & 0 & 1 & 0 \\ & & & 0 & 0 & 1 & 0 & 0 \\ & & & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and the matrix

$$R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The matrix F sends all amplitude into the junk states. The matrix X_{2n} sends some minimum amount of amplitude into an accept state if the amplitudes of states q_{2n} and q_{2n+2} differ.

The initial configuration of the machine is $|\psi_{init}\rangle = (\alpha_0, \alpha_1, ..., \alpha_m)^T$ where

$$\alpha_i = \begin{cases} \frac{1}{\sqrt{n+2}} & 0 \leq i \leq 2n+2 \ \wedge \ i \equiv 0 \pmod 2 \\ 0 & \text{otherwise} \end{cases}$$

i.e. the amplitude is evenly distributed among all non-halting states.

The only decisive accepting state in the machine is q_{2n+1}, and amplitude only flows into it when the end-marker is read. In order for it to get a non-zero amplitude, the amplitudes of states q_{2n} and q_{2n+2} must differ. Since all non-halting states start with the same amplitude, and since the amplitude of state q_{2n+2} will not change during the execution of the machine until the end-marker is read, the amplitude of state q_{2n-2} must change in order for the amplitude of state q_{2n} to change. Following the same argument, state q_{2i} will not change in amplitude, until state q_{2i-2} changes in amplitude. Furthermore, the change in amplitude of state q_{2i} is governed by the matrix components X_{2i-2} and X_{2i}. Hence, the initial change of amplitude of state q_{2i} depends exclusively on a change in amplitude of state q_{2i-2} and is governed by component X_{2i-2} that is located in the transition matrix U_{z_i}. If any other transition matrix is applied, then the amplitude of state q_{2i} will not change. Hence, M can read $(\Sigma - \{z_i\})^*$ without changing the amplitude of state q_{2i}, but, as soon as z_i is read, component X_{2i-2} will be applied and q_{2i} will have a decreased amplitude, provided state q_{2i-2} already had a decrease of its amplitude. Finally, the amplitude of any state q_{2i} will never increase beyond its initial value, and once the amplitude of state q_{2i} decreases, it will never increase beyond $\frac{1}{\sqrt{n+2}}(1-(\frac{1}{2})^{n+1})$. For the case of symbol z_0, the amplitude of state q_0 is changed by matrix S to 0 and is the starting trigger. When the end-marker is read a minimum of $\frac{1}{\sqrt{2(n+2)}}(\frac{1}{2})^{n+1}$ of amplitude is placed into the accepting state only if the amplitude of state q_{2n} has decreased. The amplitude from q_{2n+2} is channeled into a decisive reject state. The rest of the amplitude, from the remaining $n+1$ non-halting states is channeled into junk states. If the amplitudes of q_{2n} and q_{2n+2} do not differ then all amplitude is channeled into junk and decisive reject states.

The probability of M accepting a string not in the language is 0, while the probability of M accepting a string in the language is at least $\frac{1}{n+2}(\frac{1}{2})^{2n+3}$. We select the cut-point to be strictly between the two values. ∎

Any boolean combination of partial piecewise testable sets may be expressed as a union of intersections of partial piecewise testable sets and complements of partial piecewise testable sets, i.e.,

$$\bigcup_{i=0}^{s}\left(\bigcap_{j=0}^{t}\tilde{L}_{ij}\right) \tag{2}$$

where $\tilde{L}_{ij}$ is a partial piecewise testable set or the complement thereof.

We first show how to construct the implicants of the above expression, i.e. $\cap_{j=0}^{t}\tilde{L}_{ij}$, and then, how to take the union of the implicants. An implicant can be written in the form

$$\bigcap_{j=0}^{t}\tilde{L}_{ij}=\left(\bigcap_{j=0}^{r}L_{ij}\right)\bigcap\left(\bigcap_{j=r}^{t}\overline{L}_{ij}\right),$$

where the L_{ij}s are partial piecewise testable sets. By De Morgan's rule, the latter part of this expression can be rewritten as $\overline{\cup_{j=r}^{t}L_{ij}}$. Let $L^{\cap}{}_i=\cap_{j=0}^{r}L_{ij}$, let $L^{\cup}{}_i=\cup_{j=r}^{t}L_{ij}$, and let $L_i=L^{\cap}{}_i\cap\overline{L^{\cup}{}_i}$.

First, we show that $L^{\cap}{}_i$ can be accepted by an end-decisive MM-QFA with bounded positive one-sided error. Second, we show that $\overline{L^{\cup}{}_i}$ can be accepted by an end-decisive MM-QFA with bounded error. Third, we show that L_i can be accepted by an end-decisive MM-QFA with bounded error. Finally, we show that $\cup_{i=0}^{s}L_i$ can be accepted by an end-decisive MM-QFA with bounded error. We first need two composition lemmas.

We say that an MM-QFA M accepts L with cut-point λ and maximum margin η if for all $x\in\Sigma^*$,

$$\lambda-\eta<\Pr[M(x)=\text{accept}]<\lambda+\eta.$$

Usually, the maximum margin will be exponentially greater than the margin ϵ; this creates problems when we compose automata.

Lemma 4.8 *Let M and M' be end-decisive MM-QFAs that accept L and L' respectively, with cut-points λ and λ', margins ϵ and ϵ', and maximum margins η and η'.*

There exists an end-decisive MM-QFA M'' such that the inequalities

$$(\lambda+\epsilon)\cdot(\lambda'+\epsilon') \le \Pr[M''(x)=\text{accept}] \le (\lambda+\eta)\cdot(\lambda'+\eta') \quad \forall x \in L \cap L', \quad (3)$$
$$(\lambda-\eta)\cdot(\lambda'+\epsilon') \le \Pr[M''(x)=\text{accept}] \le (\lambda-\epsilon)\cdot(\lambda'+\eta') \quad \forall x \in \overline{L} \cap L', \quad (4)$$
$$(\lambda+\epsilon)\cdot(\lambda'-\eta') \le \Pr[M''(x)=\text{accept}] \le (\lambda+\eta)\cdot(\lambda'-\epsilon') \quad \forall x \in L \cap \overline{L'}, \quad (5)$$
$$(\lambda-\eta)\cdot(\lambda'-\eta') \le \Pr[M''(x)=\text{accept}] \le (\lambda-\epsilon)\cdot(\lambda'-\epsilon') \quad \forall x \in \overline{L} \cap \overline{L'} \quad (6)$$

are satisfied.

Proof: Let $M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ and $M' = (Q', \Sigma, \delta', q_0', Q'_{acc}, Q'_{rej})$ be end-decisive MM-QFAs that accept L and L'. Using these two MM-QFAs we construct an MM-QFA $M'' = (Q'', \Sigma, \delta'', q_0'', Q''_{acc}, Q''_{rej})$ that satisfies the above inequalities.

Let $Q'' = Q \times Q'$ and $q_0'' = (q_0, q_0')$. The sets of halting states are defined as

$$\begin{aligned} Q''_{acc} &= \{(q_i, q_j') \in Q'' \mid q_i \in Q_{acc} \ \wedge \ q_j' \in Q'_{acc}\}, \\ Q''_{rej} &= \{(q_i, q_j') \in Q'' \mid (q_i \in Q_{rej} \ \vee \ q_j' \in Q'_{rej}), \} \end{aligned}$$

and the transition function δ'' is defined as

$$\delta''((q, q'), \sigma, (r, r')) = \delta(q, \sigma, r) \cdot \delta'(q', \sigma, r'),$$

which is a tensor product of the transition functions δ and δ'.

Since M and M' are end-decisive, i.e., the accepting states will only have non-zero amplitude when the end-marker is read; thus the MM-QFA M'' will be end-decisive.

By the tensor product construction, the probability of M'' accepting x is

$$\Pr[M''(x) = \text{accept}] = \Pr[M(x) = \text{accept}] \cdot \Pr[M'(x) = \text{accept}].$$

Since

$$\begin{aligned} \lambda+\epsilon \le \Pr[M(x)=\text{accept}] &\le \lambda+\eta \quad &\forall x \in L, \\ \lambda-\eta \le \Pr[M(x)=\text{accept}] &\le \lambda-\epsilon \quad &\forall x \notin L, \\ \lambda'+\epsilon' \le \Pr[M'(x)=\text{accept}] &\le \lambda'+\eta' \quad &\forall x \in L', \\ \lambda'-\eta' \le \Pr[M'(x)=\text{accept}] &\le \lambda'-\epsilon' \quad &\forall x \notin L', \end{aligned}$$

multiplying out the probabilities yields the inequalities 3, 4, 5, and 6. ■

Corollary 4.9 *Let M and M' be end-decisive MM-QFAs that accept L and L' respectively, with bounded positive one-sided error. There exists an end-decisive MM-QFA that accepts $L \cap L'$ with bounded positive one-sided error.*

Proof: Let λ, λ', ϵ, and ϵ' be the respective cut-points and margins of MM-QFAs M and M'. Since $\lambda - \epsilon = \lambda' - \epsilon' = 0$, $\lambda + \epsilon > 0$, and $\lambda' + \epsilon' > 0$, the result follows from Lemma 4.8. ■

We mentioned before that the maximum maximum margin of a MM-QFA that accepts language L could be exponentially greater than the margin. This prevents us from directly constructing intersections or unions of languages that are accepted by end-decisive MM-QFAs with bounded error. To get around this problem we use a tensor power technique to magnify the ratio of the probability of a true positive to the probability of a false positive.

Lemma 4.10 *Let M be an end-decisive MM-QFA that accepts words in L with probability at least $\lambda+\epsilon$ and accepts words not in L with probability at most $\lambda-\epsilon$. For any positive integer n there exists an MM-QFA M' that accepts words in L with probability at least $(\lambda+\epsilon)^n$, and accepts words not in L with probability at most $(\lambda-\epsilon)^n$.*

Proof: Using Lemma 4.8 to compose n copies of M yields the result. ■

We first use Lemma 4.10 to construct finite unions of languages that are accepted by end-decisive MM-QFAs with bounded error.

Lemma 4.11 *Let M be an MM-QFA that accepts L with bounded error and let M' be an MM-QFA that accept L' with bounded error. There exists an MM-QFA M'' that accepts $L'' = L \cup L'$ with bounded error.*

Proof: Assume that M accepts words in L with probability at least $\lambda+\epsilon$ and accepts words not in L with probability at most $\lambda-\epsilon$. Similarly, assume that M' accepts words in L' with probability at least $\lambda'+\epsilon'$ and accepts words not in L' with probability at most $\lambda'-\epsilon'$.

Using Lemma 4.10 let M_s be the sth tensor power of M and M'_t be the tth tensor power of M'.

Let $M_s = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ and $M'_t = (Q', \Sigma, \delta', q'_0, Q'_{acc}, Q'_{rej})$, where $Q = \{q_0, ..., q_{n-1}\}$ and $Q' = \{q'_0, ..., q'_{m-1}\}$. Let δ and δ' be represented by the unitary matrices U_σ and U'_σ respectively.

Let $M'' = (Q'', \Sigma, \delta'', Q''_{acc}, Q''_{rej})$ where $Q'' = \{q''_0, ..., q''_{n+m-1}\}$, δ'' is represented by the matrices

$$U''_\sigma = \begin{bmatrix} U_\sigma & 0 \\ 0 & U'_\sigma \end{bmatrix},$$

$Q''_{acc} = \{q''_i \in Q'' \mid q_i \in Q_{acc} \lor q'_{i-n} \in Q'_{acc}\}$, and $Q''_{rej} = \{q''_i \in Q'' \mid q_i \in Q_{rej} \lor q'_{i-n} \in Q'_{rej}\}$. The automata is initialized with the amplitude evenly divided between the states q''_0 and q''_n, i.e., each state contains $\frac{1}{\sqrt{2}}$ amplitude. Intuitively, M and M' run in parallel, not interacting unless one of the two crashes. In that case the computation is over.

If $x \in L \cap L'$ then

$$\Pr[M''(x) = \text{accept}] \geq \frac{(\lambda+\epsilon)^s + (\lambda'+\epsilon')^t}{2},$$

if $x \in L \cap \overline{L'}$ then

$$\Pr[M''(x) = \text{accept}] \geq \frac{(\lambda+\epsilon)^s}{2},$$

if $x \in \overline{L} \cap L'$ then

$$\Pr[M''(x) = \text{accept}] \geq \frac{(\lambda'+\epsilon')^t}{2},$$

and if $x \in \overline{L} \cap \overline{L'}$ then

$$\Pr[M''(x) = \text{accept}] \leq \frac{(\lambda-\epsilon)^s + (\lambda'-\epsilon')^t}{2},$$

The last case corresponds to $x \notin L''$. By setting s and t appropriately, we can ensure that

$$(\lambda - \epsilon)^s + (\lambda' - \epsilon')^t \ll \min\{(\lambda + \epsilon)^s, (\lambda' + \epsilon')^t\}.$$

Hence, the MM-QFA M'' accepts $L \cup L'$ with bounded error. Furthermore, M'' is end-decisive because both M_s and M_t are end-decisive. ■

Corollary 4.12 *Let M and M' be end-decisive MM-QFAs that accept L and L' respectively, with bounded positive one-sided error. There exists an end-decisive MM-QFA that accepts $L \cup L'$ with bounded positive one-sided error.*

Proof: Since $\lambda - \epsilon = \lambda' - \epsilon' = 0$, the same argument as in Corollary 4.9 applies. ■

One useful property of languages that are accepted by end-decisive MM-QFAs with bounded positive one-sided error is that we can usually construct end-decisive MM-QFAs that can accept the complement such languages with bounded error. We say that an end-decisive MM-QFA accepts with positive amplitude, if the amplitude in it's accept states is always non-negative.

Lemma 4.13 *Let L be a language that is accepted by an end-decisive MM-QFA with bounded positive one-sided error and positive amplitude. There exists an end-decisive MM-QFA that accepts $\overline{L}$ with bounded error.*

Proof: Let $M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ be an end-decisive MM-QFA that accepts L with bounded positive one-sided error. Since M rejects all strings not in L with certainty, for every computation of M on $x \notin L$ zero amplitude is placed into the accepting states of M. Let $n = |Q|$, let $a = |Q_{acc}|$ and assume that $Q_{acc} = \{q_{n-1}, q_{n-2}, ..., q_{n-a}\}$.

We use M to construct an end-decisive MM-QFA M' to accept $\overline{L}$ with bounded error. Let $M' = (Q', \Sigma, \delta', q_0, Q'_{acc}, Q'_{rej})$ where

$$\begin{aligned} Q' &= Q \cup \{q_n, q_{n+1}, ..., q_{n+3a}\} \\ Q'_{rej} &= Q_{rej} \cup Q_{acc} \cup \{q_{n+i} \in Q' \mid i \equiv 2 \bmod 3\} \\ Q'_{acc} &= \{q_{n+i} \in Q' \mid i \equiv 0 \bmod 3\} \end{aligned}$$

and the transition function δ' is extended in the following manner. For all symbols except the end-marker, the transition function for M' is defined by the matrices

$$U'_\sigma = \begin{bmatrix} U_\sigma & \\ & I_{3a} \end{bmatrix}.$$

The end-marker transition is defined by the matrix

$$U'_\$ = \begin{bmatrix} U_\$ & \\ & I_{3a} \end{bmatrix} X,$$

where matrix X performs an averaging and cleanup operation. We define X in terms of 4×4 sub-matrices. Every accept state $q_{n-a+i} \in Q_{acc}$ in M becomes a reject state in M'. Additionally, for each such state, 3 additional states were added to M', q_{n+3i}, q_{n+3i+1}, and q_{n+3i+2}, these are an accepting, a non-halting, and a rejecting state respectively. The matrix X operates on the 4-tuples of states $(q_{n-a+i}, q_{n+3i}, q_{n+3i+1}, q_{n+3i+2})$. Each operation is localized to the 4-tuple of states and hence can be described by a 4×4 matrix X_i. Assume that the order of rows and columns of the matrix correspond to the order in the 4-tuple. Let

$$X_i = \overbrace{\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}}^{\text{cleanup}} \overbrace{\begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} & \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & \\ \frac{1}{2} & -\frac{1}{\sqrt{2}} & \frac{1}{2} & \\ & & & 1 \end{bmatrix}}^{averaging}.$$

Since M accepts with positive amplitude, the amplitude in state q_{n-a+i} will be non-negative. If the non-halting state q_{n+3i+1} contains a fixed amount of amplitude α, and the old accept state q_{n-a+i} contains β amplitude. Then, the averaging operation places $\frac{\alpha-\beta}{\sqrt{2}}$ amplitude in the accept state q_{n+3i}. Then, the cleanup operation places any amplitude remaining in the non-halting state q_{n+3i+1} into the reject state q_{n+3i+2}.

We initialize M' in the same way as M except that a fraction of the amplitude is placed in the new non-halting states. These states behave as reservoirs until the end-marker is read. The amount of amplitude placed in the states is greater than the maximum amount of amplitude that any accepting state may ever contain.

If $x \in L$ then at least one of the accept states of M will contain a minimum amount of positive amplitude. Hence, the amount of amplitude in at least one of the accept states of M' will be strictly less than $\frac{\alpha}{\sqrt{2}}$, by some fixed amount. If $x \notin L$ then all accept states of M' will have exactly $\frac{\alpha}{\sqrt{2}}$ amplitude in them.

Hence, if $x \in L$ the probability of M' accepting x will be strictly less than if $x \notin L$. Hence, M' accepts $\overline{L}$ with bounded error. Since the accept states are only observed after the end-marker is read, M' is end-decisive. ∎

If L is a language that can be accepted by an end-decisive MM-QFA with bounded error and L' is a language that can be accepted by an end-decisive MM-QFA with bounded positive one-sided error, then we use Lemma 4.10 to construct an MM-QFA that accepts the intersection of the two languages.

Lemma 4.14 *Let M be an end-decisive MM-QFA that accepts L with bounded error and let M' be an end-decisive MM-QFA that accept L' with bounded positive one-sided error. There exists an MM-QFA M'' that accepts $L'' = L \cap L'$ with bounded error.*

Proof: Let MM-QFA M accept L with cut-point λ, margin ϵ, and maximum margin η, and let MM-QFA M' accept M' with cut-point λ', margin ϵ', and maximum margin η'.

First, consider the inequalities in Lemma 4.8 that occur when we compose the MM-QFAs M and M' using the tensor technique. Since MM-QFA M' accepts with bounded positive one-sided error, the inequalities are:

$$
\begin{array}{rll}
(\lambda+\epsilon)\cdot(\lambda'+\epsilon') \leq \Pr[N(x)=\text{accept}] \leq (\lambda+\eta)\cdot(\lambda'+\eta') & \forall x \in L\cap L', \\
(\lambda-\eta)\cdot(\lambda'+\epsilon') \leq \Pr[N(x)=\text{accept}] \leq (\lambda-\epsilon)\cdot(\lambda'+\eta') & \forall x \in \overline{L}\cap L', \\
(\lambda+\epsilon)\cdot 0 \leq \Pr[N(x)=\text{accept}] \leq (\lambda+\eta)\cdot 0 & \forall x \in L\cap \overline{L'}, \\
(\lambda-\eta)\cdot 0 \leq \Pr[N(x)=\text{accept}] \leq (\lambda-\epsilon)\cdot 0 & \forall x \in \overline{L}\cap \overline{L'}.
\end{array}
$$

These reduce to three cases:

$$
\Pr[M''(x)=\text{accept}] \geq (\lambda+\epsilon)\cdot(\lambda'+\epsilon') \quad \forall x \in L\cap L', \tag{7}
$$

$$
\Pr[M''(x)=\text{accept}] \leq (\lambda-\epsilon)\cdot(\lambda'+\eta') \quad \forall x \in \overline{L}\cap L', \tag{8}
$$

$$
\Pr[M''(x)=\text{accept}] = 0 \quad \forall x \in \overline{L'}. \tag{9}
$$

If we can guarantee that

$$(\lambda-\epsilon)\cdot(\lambda'+\eta') < (\lambda+\epsilon)\cdot(\lambda'+\epsilon')$$

then the tensor technique is sufficient to construct the intersection. Let M_n be the nth tensor composition of M. By Lemma 4.10 M_n accepts words in L with probability at least $(\lambda+\epsilon)^n$ and accepts words not in L with probability at most $(\lambda-\epsilon)^n$. Construct MM-QFA M'' by composing M_n with M' using the tensor technique; for sufficiently large constant n the inequality

$$(\lambda-\epsilon)^n\cdot(\lambda'+\eta') < (\lambda+\epsilon)^n\cdot(\lambda'+\epsilon')$$

will be satisfied. Thus, MM-QFA M'' accepts L'' end-decisively with bounded error. ■

We are now assemble our array of tools to construct an arbitrary boolean combination of partial piecewise testable sets.

Theorem 4.15 *Piecewise testable sets can be accepted by end-decisive MM-QFAs with bounded error.*

Proof: Let L be a piecewise testable set. We first rewrite it in canonical form:

$$
\begin{aligned}
L &= \bigcup_{i=0}^{s}\bigcap_{j=0}^{t}\tilde{L}_{ij} \\
&= \bigcup_{i=0}^{s}\left(\cap_{j=0}^{r}L_{ij}\bigcap\cap_{j=r}^{t}\overline{L}_{ij}\right) \\
&= \bigcup_{i=0}^{s}\left(\cap_{j=0}^{r}L_{ij}\bigcap\overline{\cup_{j=r}^{t}L_{ij}}\right) \\
&= \bigcup_{i=0}^{s}\left(L^{\cap}{}_{i}\bigcap\overline{L^{\cup}{}_{i}}\right) \\
&= \bigcup_{i=0}^{s}L_i
\end{aligned}
$$

By Theorem 4.7 we can construct end-decisive MM-QFAs that accept partial piecewise testable sets, L_{ij} with bounded positive one-sided error. Using these constructions and Corollaries 4.9 and 4.12, we can construct end-decisive MM-QFAs that accept languages ${L^{\cap}}_i$ and ${L^{\cup}}_i$ with bounded positive one-sided error.

The constructions in Theorem 4.7 only channel non-negative amplitude into their accept states, furthermore, the constructions in Lemmas 4.8 and 4.11 do not negate amplitude. Consequently, the constructions for languages ${L^{\cap}}_i$ and ${L^{\cup}}_i$ only channel positive amplitude into their accept states. Hence, said constructions accept with positive amplitude. Since ${L^{\cup}}_i$ is also accepted with bounded positive one-sided error, by Lemma 4.13, we can construct an end-decisive MM-QFA that can accept $\overline{{L^{\cup}}_i}$ with bounded error.

Since ${L^{\cap}}_i$ is accepted by an end-decisive MM-QFA with bounded positive one-sided error and $\overline{{L^{\cup}}_i}$ is accepted by an end-decisive MM-QFA with bounded error, by Lemma 4.14 we can construct an end-decisive MM-QFA that accepts $L_i = {L^{\cap}}_i \cap \overline{{L^{\cup}}_i}$ with bounded error.

Since the languages L_i can be accepted by end-decisive MM-QFAs with bounded error, by Lemma 4.11, we can construct an end-decisive MM-QFA that accepts $L = \cup_i L_i$ with bounded error. ■

5 Conclusions

We defined two models of 1-way quantum finite automata: the measure-once model that performs one measurement at the end of the computation, and the measure-many model that performs a measurement after every transition. The measure-many model is strictly more powerful than the measure-once but is more difficult to characterize.

When restricted to accepting with bounded error, measure-once automata can only accept group languages, while unrestricted measure-once automata can accept irregular sets and in particular, can solve the word problem on the free group. Any language accepted by a MO-QFA can also be accepted by a PFA, therefore PFAs can also solve the word problem on the free group. We also sketched an algorithm for determining equivalence of two MO-QFAs.

The measure-many automaton is difficult to characterize. We have shown that the two classes of languages, those accepted with and without bounded error, are closed under complement and inverse homomorphisms; it is still an open question if these classes are closed under boolean operations. We defined the partial order condition for languages and proved that it is a necessary condition for a language to be accepted by an MM-QFA with bounded error. We also showed that piecewise testable sets can be accepted with bounded error by MM-QFAs, and in the process detailed several novel construction techniques.

We do not know if the partial order condition is also a sufficient condition for bounded acceptance. If it is then the two classes of languages accepted by an MM-QFA are closed under intersection.

References

[ABFK99] A. Ambainis, R. Bonner, R. Freivalds, and A. Kikusts. Probabilities to accept languages by quantum finite automata. In *Computation and Combinatorics*, volume 1627 of *Lecture Notes on Computer Science*, 1999.

[AF98] A. Ambainis and R. Freivalds. 1-way quantum finite automata: Strengths, weaknesses and generalizations. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 332–342, November 1998.

[AI99] M. Amano and K. Iwama. Undecideability of quantum finite automata. In *Proceedings of the 31st Annual ACM Symposium on the Theory of Computing*, pages 368–375, 1999.

[ANTSV99] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. In *Proceedings of the 31st Annual ACM Symposium on the Theory of Computing*, pages 376–383, 1999.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal of Computing*, pages 1411–1473, October 1997.

[Eil76] S. Eilenberg. *Automata, Languages and Machines*, volume B. Academic Press, New York, 1976.

[HU79] J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages and Computation.* Addison-Wesley Publishers, Reading, Massachusetts, 1979.

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

[LZ77] R. Lipton and Y. Zalcstein. Word problem solvable in logspace. *Journal of the ACM*, 24(3):523–526, July 1977.

[MC00] C. Moore and J. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237:275–306, 2000.

[MT69] A. Meyer and C. Thompson. Remarks on algebraic decomposition of automata. *Mathematical Systems Theory*, 3(2):110–118, 1969.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, 1999.

[Ort87] J. Ortega. *Matrix Theory.* Plenum Press, New York, New York, 1987.

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

[Per94] D. Perrin. Finite automata. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 1. Elsevier Science Publisher, 1994.

[Pin87] J. Pin. On languages accepted by finite reversible automata. In *Proceedings of the 14th International Colloquium on Automata, Languages and Programming*, volume 267 of *Lecture Notes on Computer Science*, pages 237–249, 1987.

[Rab63] M. Rabin. Probabilistic automata. *Information and Control*, 6:230–245, 1963.

[Sim75] I. Simon. Peicewise testable events. In *Proc. of the 2nd GI Conf*, volume 33 of *Lecture Notes on Computer Science*, 1975.

[Wag85] S. Wagon. *The Banach-Tarski Paradox.* Cambridge University Press, New York, New York, 1985.

A End-Marker Theorems

Theorem A.1 *Let M be an MO-QFA that has both left and right end-markers. There exists an MO-QFA M' that uses only one end-marker and is equivalent to M.*

Proof: Let $M = (Q, \Sigma, \delta, q_0, F)$ be an MO-QFA with left and right end-markers, effectively allowing M to start in any possible configuration. Define $M' = (Q, \Sigma, \delta', q_0, F)$ from M. Let δ be defined in terms of the transition matrices $\{U_\sigma\}_{\sigma\in\Sigma}$. We define δ' from δ in the following way: for every $\sigma \in \Sigma$ let

$$U'_\sigma = U_{\not c}^{-1} U_\sigma U_{\not c}$$

and let

$$U'_\$ = U_\$ U_{\not c}$$

Now consider what happens when M and M' read a string $x = x_1 ... x_n$. Since

$$\begin{aligned} U'(x\$) &= U'_\$ U'_{x_n} ... U'_{x_1} \\ &= U_\$ U_{\not c} U_{\not c}^{-1} U_{x_n} U_{\not c} ... U_{\not c}^{-1} U_{x_1} U_{\not c} \\ &= U_\$ U_{x_n} ... U_{x_1} U_{\not c} \\ &= U(\not c x\$), \end{aligned}$$

the probability of M accepting x is equal to the probability of M' accepting x. Thus one end-marker on the right suffices, and by symmetry one left end-marker would also suffice. Therefore, an MO-QFA starting in configuration $|q_0\rangle$ can simulate an MO-QFA starting in any arbitrary configuration. ■

Theorem A.2 *Let M be an MM-QFA that has both left and right end-markers. There exists an MM-QFA M' that uses only a right end-marker and is equivalent to M.*

Proof: Let $M = (Q, \Sigma, \delta, Q_{acc}, Q_{rej})$ be an MM-QFA that uses two end-markers and accepts L. Assume without loss of generality that

$$\begin{aligned} Q_{non} &= \{q_i \in Q \mid 0 \leq i < n_{non}\} \\ Q_{acc} &= \{q_i \in Q \mid n_{non} \leq i < n_{acc}\} \\ Q_{rej} &= \{q_i \in Q \mid n_{acc} \leq i < n_{rej} = n = |Q|\}, \end{aligned}$$

which facilitates a simpler description of M'. We construct $M' = (Q', \Sigma, \delta', Q'_{acc}, Q'_{rej})$ that accepts L with only the right end-marker. Let $Q' = Q \cup \{q_n, q_{n+1}, ..., q_{2n-n_{non}}\}$, $Q'_{acc} = \{q_{n+i-n_{non}} \in Q' \mid q_i \in Q_{acc}\}$ and $Q'_{rej} = \{q_{n+i-n_{non}} \in Q' \mid q_i \in Q_{rej}\}$. Assume that δ is defined in terms of transition matrices $\{U_\sigma\}_{\sigma \in \Sigma}$. The construction of $\{U'_\sigma\}_{\sigma \in \Sigma}$ is similar to that in the proof of Theorem A.1. Let I_l represent an identity matrix of size l and $m = n - n_{non}$. We define δ' in terms of its unitary block matrices. For all $\sigma \in \Sigma$ let

$$\begin{aligned} U'_\sigma &= \begin{bmatrix} U_{¢}^{-1} & \\ & I_m \end{bmatrix} S \begin{bmatrix} U_\sigma & \\ & I_m \end{bmatrix} \begin{bmatrix} U_{¢} & \\ & I_m \end{bmatrix} \\ U'_{\$} &= S \begin{bmatrix} U_{\$} & \\ & I_m \end{bmatrix} \begin{bmatrix} U_{¢} & \\ & I_m \end{bmatrix} \end{aligned}$$

where

$$S = \begin{bmatrix} I_{n_{non}} & & \\ & & I_m \\ & I_m & \end{bmatrix}$$

transfers (sweeps) all probability amplitude from states in the old halting states to the new halting states. The old halting states, those in Q_{acc} and Q_{rej}, are no longer halting states in M'. The operation of M' is similar to the operation of the QFA constructed in Theorem A.1, The "sweeping" operation saves the amplitude that was in the old states, while it performs the $U_{¢}^{-1}$ operation in the new halting states (since otherwise the $U_{¢}^{-1}$ would corrupt the amplitude stored in the original halting states). ■