Looking for Pairs that Hard to Separate: A Quantum Approach

Aleksandrs Belovs[1], J. Andres Montoya[2(✉)], and Abuzer Yakaryılmaz[3]

[1] CWI, Amsterdam, The Netherlands
stiboh@gmail.com
[2] Universidad Nacional de Colombia, Bogotá, Colombia
jamontoyaa@unal.edu.co
[3] National Laboratory for Scientific Computing, Petrópolis, RJ, Brazil
abuzer@lncc.br

Abstract. Determining the minimum number of states required by a deterministic finite automaton to separate a given pair of different words (to accept one word and to reject the other) is an important challenge. In this paper, we ask the same question for quantum finite automata (QFAs). We classify such pairs as easy and hard ones. We show that 2-state QFAs with real amplitudes can separate any easy pair with zero-error but cannot separate some hard pairs even in nondeterministic acceptance mode. When using complex amplitudes, 2-state QFAs can separate any pair in nondeterministic acceptance mode, and here we conjecture that they can separate any pair also with zero-error. Then, we focus on (a more general problem) separating a pair of two disjoint finite set of words. We show that QFAs can separate them efficiently in nondeterministic acceptance mode, i.e., the number of states is two to the power of the size of the small set.

Keywords: Quantum finite automaton · Zero-error · Nondeterminism · Succinctness · Promise problems

1 Introduction

Determining the minimum number of states required by a deterministic finite automaton (DFA) to separate any given pair of words is one of the famous open problems in automata theory [5]. We can generalize this question in a straightforward way by considering different computational models (e.g. see [16]).

We focus on quantum finite automata (QFAs). We classify such pairs as easy and hard ones. We show that 2-state QFAs with real amplitudes can separate any easy pair with zero-error but cannot separate some hard pairs even in nondeterministic acceptance mode. When using complex amplitudes, 2-state QFAs can separate any pair in nondeterministic acceptance mode and here we conjecture that they can separate any pair also with zero-error. Then, we focus on (a more general problem) separating a pair of two disjoint finite set of words.

Y.-S. Han and K. Salomaa (Eds.): CIAA 2016, LNCS 9705, pp. 213–223, 2016.
DOI: 10.1007/978-3-319-40946-7_18

We show that QFAs can separate them efficiently in nondeterministic acceptance mode, i.e., the number of states is two to the power of the size of the small set.

In the next section, we provide the necessary background. The results on separating pairs are given in Sect. 3. The results on separating two finite sets are presented in Sect. 4.

2 Background

We refer the reader to [13] for a pedagogical introduction to quantum finite automata (QFAs), to [2] for a comprehensive survey on QFAs, and to [11] for a complete reference on quantum computation.

We denote the alphabet by Σ, and we suppose that it does not contain the right end-marker \$. For any given word $x \in \Sigma$, $|x|$ represents the length of x, $|x|_\sigma$ represents the number of occurrences of symbol σ in x, and x_j represents the j-th symbol of x, where $\sigma \in \Sigma$ and $1 \leq j \leq |x|$. As a special case, if $|\Sigma| = 1$, then the automaton and languages can be called unary.

2.1 Easy and Hard Pairs

Throughout the paper, a pair of words (x, y) refers to two different words defined on the same alphabet. A pair of words (x, y) is called *easy* if x and y have different numbers of occurrences of a symbol, i.e., $\exists \sigma \in \Sigma \left(|x|_\sigma \neq |y|_\sigma\right)$. Otherwise, the pair is called *hard*. Remark that any pair with different lengths (and so any unary pair) is easy.

Any hard pair defined on an alphabet with at least three elements can be mapped to a binary hard pair as follows. Let (x, y) be a hard pair defined on $\{\sigma_1, \ldots, \sigma_k\}$ for some $k > 2$. Since the pair is hard, we have

$$|x|_{\sigma_i} = |y|_{\sigma_i}$$

for each $1 \leq i \leq k$. Then, there should be an index j $(1 \leq j \leq |x| = |y|)$ such that $x_j = \sigma_i \neq y_j = \sigma_{i'}$ for $i \neq i'$. If we delete all the other symbols and keep only σ_is and $\sigma_{i'}$s in x and y, we obtain two new words: x' and y', respectively. It is clear that (x', y') is a hard pair. So, instead of separating the hard pair (x, y), we can try to separate (x', y'). Algorithmically, we apply the identity operators on the symbols other than σ_i and $\sigma_{i'}$. Hence, unless otherwise specified, we focus on unary and binary words throughout the paper.

2.2 A Motivating Problem: Looking for Pairs that are Truly Hard to separate

Let w, v be two words of length n. What is the size of a minimal DFA separating those two words? The best upper bound is $O\left(n^{\frac{2}{5}} \log^{\frac{3}{5}}(n)\right)$ (see [12]), but we do not know of a set of pairs requiring such a large number of states.

Recall that DFAs can perform modular counting, and modular counting can be used to separate easy pairs using logarithmic number of states. Unfortunately the best lower bound is also $\Omega(\log(n))$ (see [8]), which was given by using the following set of pairs

$$S = \left\{ \left(0^{n-1}, 0^{n-1+lcm(1,2,\ldots,n)} \right) : n \geq 1 \right\}.$$

Thus, the hardest set of pairs registered in the literature is a set of easy pairs. We call those pairs as GK pairs (the initials of Goralcik and Koubek [8]). There are many reasons to believe that the set of GK pairs cannot be the hardest set of pairs. We can provide some evidence concerning this issue by considering some different models of automata for which it can be proved that the GK pairs are not the hardest pairs. Perhaps, more interesting, we can get some clues that could be used in the construction of a harder set of pairs, an infinite set of pairs requiring a superlogarithmic number of states.

Previous to this work we studied alternating finite state automata. We proved that easy pairs can be separated by those automata using $O(\log(\log(n)))$ states. And, on the other hand, it was proved that there exists an infinite set of pairs requiring $\Omega\left(\sqrt{\log(n)}\right)$ states. The proof of the lower bound is nonconstructive, and we do not know which are the pairs that require $\Omega\left(\sqrt{\log(n)}\right)$ states.

We have begun this work classifying pairs into two classes: easy and hard pairs. It is a rough classification which should be refined. Remark that hard pairs are not always hard to separate. Consider for instance a pair (x, y) such that $x_1 \neq y_1$. This pair can be separated by using a DFA with three states. We believe that studying some other models of automata can help us to establish a very much finer and pertinent classification.

In this work we consider quantum finite automata. We prove that easy pairs can be separated by QFAs with real amplitudes using two states. On the other hand, we prove that there are hard pairs that cannot be separated using only two states. We also consider QFAs with complex amplitudes. We conjecture that any pair can be separated by those automata using two states, and we prove that such a conjecture (and our motivating problem) has unexpected relations with some problems in the theory of Lie groups.

2.3 QFAs

Quantum finite automata (QFAs) are a non-trivial generalization of probabilistic finite automata [9,18]. Here we give the definition of the known simplest QFA model, called Moore-Crutchfield QFAs (MCQFAs) [10] since we can present our results (and our conjecture) based on this model.

An n-state MCQFA M, which operates on n-dimensional Hilbert space ($\mathcal{H}_n$, i.e., $\mathbb{C}^n$ with the inner product) is a 5-tuple

$$M = (Q, \Sigma, \{U_\sigma \mid \sigma \in \Sigma\}, |u_0\rangle, Q_a),$$

where $Q = \{q_1, \ldots, q_n\}$ is the set of states, $U_\sigma \in \mathbb{C}^{n \times n}$ is a unitary transition matrix whose (i,j)th entry represent the transition amplitude from the state q_j to the state q_i when reading symbol $\sigma \in \Sigma$ $(1 \leq i, j \leq n)$, $|u_0\rangle \in \mathbb{C}^n$ is the column vector representing the initial quantum state, and $Q_a \subseteq Q$ is the set of accepting states. The basis of $\mathcal{H}_n$ is formed by $\{|q_j\rangle \mid 1 \leq j \leq n\}$ where $|q_j\rangle$ has 1 at the j-th entry and 0 s in the remaining entries. At the beginning of the computation, M is in $|u_0\rangle$, either one of the basis states or a superposition (a linear combination) of basis states. Let $x \in \Sigma^*$ be a given input word. During reading the input x from left to right symbol by symbol, the quantum state of M is changed as follows:

$$|u_j\rangle = U_{x_j} |u_{j-1}\rangle,$$

where $1 \leq j \leq |x|$. After reading the whole word, the quantum state is measured to determine whether M is in an accepting state or not (a measurement on computational basis). Let the final quantum state, represented as $|u_f^x\rangle$ or $|u_f\rangle$, have the following amplitudes

$$|u_f^x\rangle = |u_f\rangle = |u_{|w|}\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Since the probability of observing jth state is $|\alpha_j|^2$, the input is accepted with probability $\sum_{q_j \in Q_a} |\alpha_j|^2$.

2.4 Promise Problems

The disjoint languages $X \subseteq \Sigma^*$ and $Y \subseteq \Sigma^*$ are said to be separated by M exactly or zero-error if any $x \in X$ is accepted by M with probability 1 and any $y \in Y$ is accepted by M with probability 0, or vice versa. If $|X| = |Y| = 1$, then it is said that the corresponding pair is separated by M exactly. In case of one-sided bounded error, any $x \in X$ is accepted with probability 1 and any $y \in Y$ is accepted with probability at most $p < 1$, or vice versa. If $|X| = |Y| = 1$, then it is said that the pair is separated by M with one-sided bounded-error.

Nondeterministic QFA is a theoretical model and it is defined as a special acceptance mode of a QFA, also known as recognition with cutpoint 0 [17]. The disjoint languages $X \subseteq \Sigma^*$ and $Y \subseteq \Sigma^*$ are said to be separated by a nondeterministic MCQFA M if any $x \in X$ is accepted by M with some nonzero probability and any $y \in Y$ is accepted by M with probability 0, or vice versa. If $|X| = |Y| = 1$, then it is said that the pair is separated by nondeterministic M.

3 Separating Pairs with 2 States

In this section, we present our results on separating pairs.

3.1 MCQFAs with Real Amplitudes

First at all we prove that any easy pair can be separated by a 2-state MCQFA with real amplitudes (all components of the initial states and the transition matrices are real numbers).

Theorem 1. *Any given pair of unary words (a^d, a^{d+t}) ($d \geq 0$ and $t > 0$) can be exactly separated by a MCQFA, say $R_{d,t}$.*

Proof. We define a unary 2-state MCQFA denoted with the symbol $R_{d,t}$. Let $\{q_1, q_2\}$ be the set of states. Note that any possible quantum state of such automaton is a point on the unit circle, where $|q_1\rangle$ is $(1, 0)$ and $|q_2\rangle$ is $(0, 1)$. Automaton $R_{d,t}$ is defined by the following specifications (remark that R stands for rotation).

- The initial state is $\cos(\frac{d\pi}{2t})\,|q_1\rangle - \sin(\frac{d\pi}{2t})\,|q_2\rangle$, the point on the unit circle obtained by making a clockwise rotation with angle $\frac{d\pi}{2t}$ (d times $\frac{\pi}{2t}$) when starting at the point $|q_1\rangle$.
- The single unitary operator is a counter-clockwise rotation with angle $\frac{\pi}{2t}$.
- The single accepting state is q_1.

After reading a^d, the automaton is in $|q_1\rangle$ and so it is accepted with probability 1, and, after reading a^{d+t}, the automaton is in $|q_2\rangle$ and so it is accepted with probability 0. □

Corollary 1. *Any easy pair of words can be separated exactly by a 2-state MCQFA with real amplitudes.*

There exist hard pairs of words that can be exactly separated by a 2-state MCQFA with real amplitudes, for instance, the pair (ab, ba): Let $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}^T$ be the initial state, and we apply U_a and U_b when reading symbols a and b, respectively, where

$$U_a = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \text{ and } U_b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then, after reading the words ab and ba, we obtain the following final states:

$$\left|u_f^{ab}\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and

$$\left|u_f^{ba}\right\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Therefore, the pair (ab, ba) can be exactly separated by 2-state MCQFAs with real amplitudes.

However, such automata cannot distinguish all pairs of words, as exemplified by the following simple result.

Theorem 2. *No 2-state non-deterministic MCQFA with real entries can separate two words $x, y \in \{a^2, b^2\}^*$ provided that $|x|_a = |y|_a$ and $|x|_b = |y|_b$.*

Proof. Consider any such MCQFA, and let U_a and U_b be the transition matrices corresponding to a and b, respectively. The operators U_a^2 and U_b^2 are rotations in $\mathbb{R}^2$, hence, they commute. Thus,

$$\left|u_f^x\right\rangle = U_b^{|x|_b} U_a^{|x|_a} \left|u_0\right\rangle = U_b^{|y|_b} U_a^{|y|_a} \left|u_0\right\rangle = \left|u_f^y\right\rangle,$$

and no final measurement can distinguish these two identical final states. □

Remark 1. It follows from the above results that GK pairs can be separated by using 2 states. On the other hand, it was constructively proved that there exist pairs requiring at least three states.

3.2 MCQFAs with Complex Amplitudes

In the previous section, we show that 2-state MCQFAs with real entries cannot separate all pairs of words. We conjecture that 2-state MCQFAs with complex entries (some components of the initial states and the transition matrices can be complex numbers) can exactly separate any pair of words. This conjecture is related to some problems in the theory of Lie groups (see below).

Theorem 3. *Any pair of words can be separated by a 2-state MCQFA with complex amplitudes in nondeterministic acceptance mode.*

Proof. Now, we describe an explicit 2-state nondeterministic MCQFA that can separate any given pair. For our purpose, we use an already known QFA algorithm given in [1]. For a given binary word $x \in \{a, b\}^*$, M_x is a 3-state ($\{q_1, q_2, q_3\}$) MCQFA. The initial state is $|q_1\rangle$ and the accepting states are q_2 and q_3. The unitary operators for symbols a and b are given below:

$$U_a = \frac{1}{5}\begin{pmatrix} 4 & 3 & 0 \\ -3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix} \text{ and } U_b = \frac{1}{5}\begin{pmatrix} 4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & 4 \end{pmatrix}$$

We define the initial state as follows:

$$\left|u_0\right\rangle = U_{x_1}^{-1} U_{x_2}^{-1} \cdots U_{x_{|x|}}^{-1} \left|q_1\right\rangle$$

Then, the final quantum state for x is

$$\left|u_f^x\right\rangle = U_{x_{|x|}} \cdots U_{x_2} U_{x_1} U_{x_1}^{-1} U_{x_2}^{-1} \cdots U_{x_{|x|}}^{-1} \left|q_1\right\rangle = \left|q_1\right\rangle$$

So, the accepting probability of M on x is zero. i.e., $f_M(x) = 0$. On the other hand, for any given word $y \neq x$, the final quantum state for y is different from $|q_1\rangle$:

$$\left|u_f^y\right\rangle = U_{y_{|y|}} \cdots U_{y_2} U_{y_1} U_{x_1}^{-1} U_{x_2}^{-1} \cdots U_{x_{|x|}}^{-1} \left|q_1\right\rangle = \alpha_1 \left|q_1\right\rangle + \alpha_2 \left|q_2\right\rangle + \alpha_3 \left|q_3\right\rangle, \quad (1)$$

where $|\alpha_1|$ is always less than 1 when $x \neq y$ [1]. Then, the accepting probability of M on y is nonzero. i.e., $f_M(y) > 0$.

Therefore, we can say that nondeterminsitic MCQFA M_x separates x from any other word. Based on a conversion technique given in [1], we can convert M_x into a 2-state ($\{p_1, p_2\}$) MCQFA, say N_x, defined on $\mathbb{C}^2$ such that, after reading the same word, the probability of observing q_1 is 1 if and only if the probability of observing p_1 is 1. □

We conjecture that any pair can be separated by a 2-state MCQFA with complex amplitudes and zero-error. Let us discuss some facts concerning the conjecture.

Let $w \in \left\{a, b, a^{-1}, b^{-1}\right\}^n$, and let $SU\ (2)$ be the group of 2×2 unitary matrices whose determinant is equal to 1. Suppose that $w = w_1 \cdots w_n$, and let $f_w : SU\ (2) \times SU\ (2) \to SU\ (2)$ be the *word map* defined by

$$f_w\left(M, N\right) = \prod_{i \leq n} A_i$$

where given $i \leq n$, the matrix $A_i \in SU\ (2)$ is defined as

$$A_i = \begin{cases} M & \text{if } w_i = a \\ N & \text{if } w_i = b \\ M^{-1} & \text{if } w_i = a^{-1} \\ N^{-1} & \text{if } w_i = b^{-1} \end{cases}.$$

Remark 2. The notion of word map can be extended in a straightforward way to any group different of $SU\ (2)$. We are interested in the word maps that are defined over the special unitary groups.

Given $x, y \in \{a, b\}^*$, if $y = y_1 \cdots y_n$ and $x = x_1 \cdots x_n$, we set

$$yx^{-1} = y_n \cdots y_1 x_1^{-1} \cdots x_n^{-1}$$

Notice that if the matrix $R_{\frac{\pi}{2}} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ belongs to the image of $f_{yx^{-1}}$ (i.e., if the image of $f_{yx^{-1}}$ contains a rotation by $\frac{\pi}{2}$), then one can choose $(M, N) \in f_{yx^{-1}}^{-1}\left(R_{\frac{\pi}{2}}\right)$, and use the pair (M, N) to built a 2-state MCQFA separating the pair (x, y) with zero-error. Thus, the problem of separating any pair using two quantum states is closely related to the problem of surjectivity of word maps in the special unitary group $SU\ (2)$.

The word map f_w is a continuous map defined over a topological space (the Lie group $SU\ (2)$) that is compact and connected. Moreover, it satisfies the following condition:

For all $M, N, U \in SU\ (2)$, the equality

$$f_w\left(U^\dagger M U, U^\dagger N U\right) = U^\dagger f_w\left(M, N\right) U$$

holds.

The above facts imply that the image of f_w is of the form

$$\left\{V \in SU\ (2) : U \text{ has eigenvalues } e^{\pm\theta}\ 0 \leq \theta \leq \alpha\right\}$$

for some real $\alpha = \alpha(w)$. Remark that if $\alpha\left(yx^{-1}\right) \geq \frac{\pi}{2}$, then the pair (x, y) can be separated with zero-error.

A famous result of Borel [4] implies that the image of f_w is dense in the Zariski topology. However, it does not imply that the image is dense in the ordinary topology. Actually, it can be very far from that. As shown by Thom [14], given $\varepsilon > 0$, there exists a word w_ϵ such that $\alpha(w_\varepsilon) < \varepsilon$. The results of Thom do not imply the existence of a pair (x, y) such that $\alpha\left(yx^{-1}\right) < \frac{\pi}{2}$. Actually, there are some additional results in the theory of word maps suggesting that such a bad pair cannot exist.

Let $\boldsymbol{F}_2$ be the free group with two generators, it consists of finite words over $\left\{a, b, a^{-1}, b^{-1}\right\}^*$ with the concatenation operation, modulo the relations $aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = \epsilon$, where ϵ is the empty word. Notice that if w and u are equal, as elements of $\boldsymbol{F}_2$, then $f_w = f_u$. Given $x, y \in \boldsymbol{F}_2$, the commutator of x and y is the element $xyx^{-1}y^{-1}$, which we denote with the symbol $[x, y]$. The derived subgroup of $\boldsymbol{F}_2$, denoted with the symbol $\boldsymbol{F}_2^{(1)}$, is the subgroup generated by all the commutators. The second derived subgroup, denoted with the symbol $\boldsymbol{F}_2^{(2)}$, is the derived subgroup of $\boldsymbol{F}_2^{(1)}$. Elkasapy and Thom [7] showed that if $w \notin \boldsymbol{F}_2^{(2)}$, then the corresponding word map $f_w : SU\ (n) \times SU\ (n) \to SU\ (n)$ is surjective for infinitely many n. We prove, below, that for all pair (x, y) the word $yx^{-1} \notin \boldsymbol{F}_2^{(2)}$. Notice that if for all $w \notin \boldsymbol{F}_2^{(2)}$ the word map $f_w : SU\ (2) \times SU\ (2) \to SU\ (2)$ is surjective, then any pair can be separated by using two qubits and zero-error. This last fact provides additional motivation to study this type of word maps.

Theorem 4. *For any two different words $x, y \in \{a, b\}^*$, the element xy^{-1} lies outside of the second derived subgroup $\boldsymbol{F}_2^{(2)}$.*

Proof. An element $w \in \boldsymbol{F}_2$ lies in the first derived subgroup of $\boldsymbol{F}_2$, if and only if, the total degree of both a and b in w is equal to zero. That is, $xy^{-1} \notin \boldsymbol{F}_2^{(1)}$ if and only if (x, y) is an easy pair.

Now assume that (x, y) is a hard pair. It is well known that $\boldsymbol{F}_2^{(1)}$ is a free group. A set of generators for $\boldsymbol{F}_2^{(1)}$ is the set

$$T = \left\{\left[a^k, b^l\right] : k, l > 0\right\}$$

Notice that $\left[a^k, b^l\right]^{-1} = \left[b^l, a^k\right]$. Again, $w \in \boldsymbol{F}_2^{(1)}$ lies in $\boldsymbol{F}_2^{(2)}$, if and only if, the unique decomposition of w into the elements of T contains each $\left[a^k, b^l\right]$ with total degree 0.

Given $x \in \{a, b\}^*$, we have a decomposition of the form

$$x = \prod_i \left[a^{k_i}, b^{l_i}\right]^{\varepsilon_i} \cdot a^{|x|_a} b^{|x|_b}$$

where, for all i, we have $k_i + l_i > k_{i-1} + l_{i-1}$ and $\varepsilon_i = \pm 1$. Now, it is not hard to see that $xy^{-1} \in \boldsymbol{F}_2^{(2)}$, if and only if, $x = y$. □

Remark 3. We say that (x, y) is a bad pair if $\alpha\left(yx^{-1}\right) < \frac{\pi}{2}$. If there exist such bad pairs, then it would be interesting to find the minimum number of states that are necessary to separate such bad pairs by using a DFA. Recall that one of our motivating problems is the construction of a set of pairs requiring a superlogarithmic number of states to be separated. It would also be interesting if this problem is related to the theory of word maps and Lie groups.

4 Separating Two Finite Sets

In this section, we focus on a more general problem: Separating two finite languages. Let $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_n\}$ be two disjoint set of binary words by assuming that $m \leq n$ (the sets are exchanged, otherwise). We consider the case of nondeterministic MCQFAs.

4.1 Nondeterministic MCQFAs

We use the MCQFA algorithm given at the end of the proof of Theorem 3. Let $N(X) = \{N_{x_1}, N_{x_2}, \ldots, N_{x_m}\}$ be the set of 2-state MCQFAs mentioned there. We can obtain a MCQFA, say N_X, by tensoring all MCQFAs in $N(X)$,

$$N_X = N_{x_1} \otimes N_{x_2} \otimes \cdots \otimes N_{x_m},$$

i.e., executing all of them in parallel. The tensor product is obtained in a straightforward way. The set of states of N_X is $\{p_1, p_2\}^m$. If $|u_{j,0}\rangle$ is the initial state of N_{x_j} and $U_{j,a}$ ($U_{j,b}$) is the unitary operator for symbol a (b), then the initial state of N_X is

$$|u_{1,0}\rangle \otimes |u_{2,0}\rangle \otimes \cdots \otimes |u_{m,0}\rangle$$

and the unitary operator for symbol a (b) is

$$U_{1,a} \otimes U_{2,a} \otimes \cdots \otimes U_{m,a} \quad (U_{1,b} \otimes U_{2,b} \otimes \cdots \otimes U_{m,b}),$$

where $1 \leq j \leq m$. Similarly, if $\left|u_{j,f}^{y}\right\rangle$ is the final state of N_{x_j} and β_j is the amplitude of the state $|p_2\rangle$ after reading binary word y, then the final state of N_X on y will be

$$\left|u_{1,f}^{y}\right\rangle \otimes \left|u_{2,f}^{y}\right\rangle \otimes \cdots \otimes \left|u_{m,f}^{y}\right\rangle$$

and so the amplitude of $|(p_2, p_2, \ldots, p_2)\rangle$ will be

$$\beta = \beta_1 \beta_2 \cdots \beta_m.$$

Therefore, it is clear that, if $x_j = y$, then β will be zero since β_j is zero. More generally, $\beta = 0$ if and only if $y \in X$. Thus, by picking $(p_2, p_2, \ldots, p_2)$ as the single accepting state of M_X, we can obtain the machine that separates any given word from a word in X. Remark that the number of states of N_X is 2^m.

Theorem 5. *The disjoint binary finite languages X and Y ($1 \leq |X| \leq |Y|$) can be separated by nondeterministic MCQFAs with $2^{|X|}$ states.*

5 Concluding Remarks

The motivating problem of our research is the problem of quantifying the number of states that are required to separate a given pair of words using DFAs. This problem has its roots in machine learning [16], and it has been intensively studied, but in despite of all the efforts, so few is known about it. We believe that we can shed some light on this elusive problem, by considering the same kind of questions for different models of automata. In previous research we studied alternating finite state automata. In this work we studied QFAs, and in the extended version of this paper [3] we consider the novel model of affine automata [6,15]. We think that these questions are interesting in their own rigth, and that they deserve further investigation.

Acknowledgement. We thank Andreas Thom for the discussions on our conjecture and anonymous reviewers for their helpful comments. The first author acknowledges the support provided by FP7 FET Proactive project QALGO. The second author acknowledges the support provided by Universidad Nacional de Colombia project Hermes 32083. The third author acknowledges the support provided by CAPES, grant 88881.030338/2013-01. Moreover, some parts of the work were done while the third author was visiting Bogotá, Colombia in December 2014.

References

1. Ambainis, A., Watrous, J.: Two-way finite automata with quantum and classical states. Theor. Comput. Sci. **287**(1), 299–311 (2002)
2. Ambainis, A., Yakaryılmaz, A.: Automata: from mathematics to applications. In: Automata and Quantum Computing (to appear). arXiv:1507.01988
3. Belovs, A., Montoya, J.A., Yakaryılmaz, A.: Can one quantum bit separate any pair of words with zero-error? Technical report (2016). arXiv:1602.07967
4. Borel, A.: On free subgroups of semisimple groups. L'Enseignement Mathématique **29**, 151–164 (1983)
5. Demaine, E.D., Eisenstat, S., Shallit, J., Wilson, D.A.: Remarks on separating words. In: Holzer, M. (ed.) DCFS 2011. LNCS, vol. 6808, pp. 147–157. Springer, Heidelberg (2011)
6. Díaz-Caro, A., Yakaryılmaz, A.: Affine computation and affine automaton. In: Computer Science - Theory and Applications. LNCS, vol. 9691, pp. 1–15. Springer (2016). arXiv:1602.04732
7. Elkasapy, A., Thom, A.: About Gotô's method showing surjectivity of word maps. Indiana Univ. Math. J. **63**(5), 1553–1565 (2014). arXiv:1207.5596
8. Goralčík, P., Koubek, V.: On discerning words by automata. In: Kott, L. (ed.) Automata, Languages and Programming. LNCS, vol. 226. Springer, Heidelberg (1986)
9. Hirvensalo, M.: Quantum automata with open time evolution. Int. J. Nat. Comput. **1**(1), 70–85 (2010)
10. Moore, C., Crutchfield, J.P.: Quantum automata and quantum grammars. Theor. Comput. Sci. **237**(1–2), 275–306 (2000)
11. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information, 10th edn. Cambridge University Press, Cambridge (2010)

12. Robson, J.M.: Separating strings with small automata. Inf. Process. Lett. **30**(4), 209–214 (1989)
13. Say, A.C.C., Yakaryılmaz, A.: Quantum finite automata: a modern introduction. In: Calude, C.S., Freivalds, R., Kazuo, I. (eds.) Gruska Festschrift. LNCS, vol. 8808, pp. 208–222. Springer, Heidelberg (2014)
14. Thom, A.: Convergent sequences in discrete groups. Can. Math. Bull. **56**(2), 424–433 (2013). arXiv:1003.4093
15. Villagra, M., Yakaryılmaz, A.: Language recognition power and succintness of affine automata. In: Calude, C.S., Dinneen, M.J. (eds.) UCNC 2015. LNCS, vol. 9252. Springer, Heidelberg (2015)
16. Yakaryılmaz, A., Montoya, J.A.: On discerning strings with finite automata. In: 2015 Latin American Computing Conference, pp. 1–5. IEEE (2015)
17. Yakaryılmaz, A., Say, A.C.C.: Languages recognized by nondeterministic quantum finite automata. Quantum Inf. Comput. **10**(9&10), 747–770 (2010)
18. Yakaryılmaz, A., Say, A.C.C.: Unbounded-error quantum computation with small space bounds. Inf. Comput. **279**(6), 873–892 (2011)