On the Power of One-Way Automata with Quantum and Classical States[⋆]

Maria Paola Bianchi, Carlo Mereghetti, and Beatrice Palano

Dipartimento di Informatica, Università degli Studi di Milano
via Comelico 39, 20135 Milano, Italy
{bianchi,mereghetti,palano}@di.unimi.it

Abstract. We consider the model of one-way automata with quantum and classical states (QCFAs) introduced in [23]. We show, by a direct approach, that QCFAs with isolated cut-point accept regular languages only, thus characterizing their computational power. Moreover, we give a size lower bound for QCFAs accepting regular languages, and we explicitly build QCFAs accepting the word quotients and inverse homomorphic images of languages accepted by given QCFAs with isolated cut-point, maintaining the same cut-point, isolation, and polynomially increasing the size.

Keywords: quantum automata, regular languages, descriptional complexity.

1 Introduction

Since we can hardly expect to see a full-featured quantum computer in the near future, it is natural to investigate the simplest and most restricted model of computation where the quantum paradigm outperforms the classical one. Classically, one of the simplest model of computation is a finite automaton. Thus, *quantum finite automata* (QFAs) are introduced and investigated by several authors.

Originally, two models of QFAs are proposed: measure-once QFAs [9,16], where the probability of accepting words is evaluated by "observing" just once, at the end of input processing, and measure-many QFAs [13], having such an observation performed after each move. Several variations of these two models, motivated by different possible physical realizations, are then proposed. Thus, e.g., enhanced [19], reversible [10], Latvian [1], and measure-only QFAs [6] are introduced. Results in the literature (see, e.g., [1,3,15]) show that all these models of QFAs are strictly less powerful than deterministic finite automata (DFAs), although retaining a higher descriptional power (i.e., they can be significantly smaller than equivalent classical devices).

To enhance the low computational power of these "purely quantum" systems, *hybrid models* featuring both a quantum and a classical component are

[⋆] Partially supported by MIUR under the project "PRIN: Automi e Linguaggi Formali: Aspetti Matematici e Applicativi."

M. Holzer and M. Kutrib (Eds.): CIAA 2014, LNCS 8587, pp. 84–97, 2014.

studied. Examples of such hybrid systems are QFAs with open time evolution (GQFAs) [11,14], QFAs with control language (QFCs) [3,17], and QFAs with quantum and classical states (QCFAs) [23], this latter model being the one-way restriction of the model introduced in [2]. It is proved that the class of languages accepted with isolated cut-point by GQFAs and QFCs coincides with the class of regular languages, while for QCFAs it is only known that they can simulate DFAs. A relevant feature of these hybrid models is that they can naturally and directly simulate several variants of QFAs by preserving the size. This property makes each of them a good candidate as a general unifying framework within which to investigate size results for different quantum paradigms [4,5,8,18].

In this paper, we focus on the model of QCFAs. We completely characterize their computational power and study some descriptional complexity issues. It may be interesting to point out that the relevant difference between QFCs and QCFAs rely in the communication policy between the two internal components: in QCFAs a two-way information exchange between the classical and quantum parts is established, while in QFCs only the quantum component affects the dynamic of the classical one. Here, by a direct approach, we show that the two-way communication is not more powerful than one-way communication. In fact, we prove that QCFAs accept with isolated cut-point regular languages only (exactly as QFCs), thus characterizing their computational power. We obtain this result by studying properties of formal power series associated with QCFAs.

We continue the investigations on QCFAs by studying their descriptional power. Our approach for proving regularity of languages accepted with isolated cut-point by QCFAs enables us to give a lower bound for the size complexity of QCFAs, which is logarithmic in the size of equivalent DFAs, in analogy with QFCs [7]. Next, we study the size cost of implementing some language operations on QCFAs. Results for Boolean operations are provided in [23]. Here, we explicitly construct QCFAs accepting word quotients and inverse homomorphic images of languages accepted by given QCFAs with isolated cut-point, maintaining the same cut-point, isolation, and polynomially increasing the size. For other types of QFAs, these two latter operations are investigated, e.g., in [1,17].

2 Preliminaries

2.1 Linear Algebra

We quickly recall some notions of linear algebra, useful to describe the quantum world. For more details, we refer the reader to, e.g., [22]. The fields of real and complex numbers are denoted by $\mathbb{R}$ and $\mathbb{C}$, respectively. Given a complex number $z = a + ib$, we denote its *conjugate* by $z^* = a - ib$ and its *modulus* by $|z| = \sqrt{zz^*}$. We let $\mathbb{C}^{n\times m}$ and $\mathbb{C}^n$ (shorthand for $\mathbb{C}^{1\times n}$) denote, respectively, the set of $n\times m$ matrices and n-dimensional row vectors with entries in $\mathbb{C}$. We denote by $[\mathbf{0}]_{n\times m}$ ($[\mathbf{0}]_n$) the zero matrix in $\mathbb{C}^{n\times m}$ ($\mathbb{C}^{n\times n}$). The identity matrix in $\mathbb{C}^{n\times n}$ is denoted by I_n. We let $\mathbf{0}_n$ ($\mathbf{1}_n$) be the zero vector (the vector of all ones) in $\mathbb{C}^n$. When the dimension is clear from the context, we simply write $[\mathbf{0}]$, I, $\mathbf{0}$, and $\mathbf{1}$.

We let $e_j = (0,\ldots,0,1,0,\ldots,0)$ be the characteristic vector having 1 in its jth component and 0 elsewhere. Given a vector $\varphi \in \mathbb{C}^n$, we denote by $(\varphi)_j \in \mathbb{C}$ its jth component.

Given a matrix $M \in \mathbb{C}^{n\times m}$, we let M_{ij} denote its (i,j)th entry. The *transpose* of M is the matrix $M^T \in \mathbb{C}^{m\times n}$ satisfying ${M^T}_{ij} = M_{ji}$, while we let M^* be the matrix satisfying ${M^*}_{ij} = (M_{ij})^*$. The *adjoint* of M is the matrix $M^\dagger = (M^T)^*$. For matrices $A, B \in \mathbb{C}^{n\times m}$, their *sum* is the $n\times m$ matrix $(A+B)_{ij} = A_{ij} + B_{ij}$. For matrices $C \in \mathbb{C}^{n\times m}$ and $D \in \mathbb{C}^{m\times r}$, their *product* is the $n \times r$ matrix $(CD)_{ij} = \sum_{k=1}^{m} C_{ik}D_{kj}$. For matrices $A \in \mathbb{C}^{n\times m}$ and $B \in \mathbb{C}^{p\times q}$, their *direct sum* and *Kronecker (or tensor or direct) product* are the $(n+p)\times(m+q)$ and $np \times mq$ matrices defined, respectively, as

$$A \oplus B = \begin{pmatrix} A & [\mathbf{0}] \\ [\mathbf{0}] & B \end{pmatrix}, \qquad A \otimes B = \begin{pmatrix} A_{11}B & \cdots & A_{1m}B \\ \vdots & \ddots & \vdots \\ A_{n1}B & \cdots & A_{nm}B \end{pmatrix}.$$

When operations can be performed, we have that $(A\otimes B)\cdot(C\otimes D) = AC\otimes BD$ and $(A\oplus B)\cdot(C\oplus D) = AC\oplus BD$. For vectors $\varphi \in \mathbb{C}^n$ and $\psi \in \mathbb{C}^m$, their *direct sum* is the vector $\varphi \oplus \psi = (\varphi_1,\ldots,\varphi_n,\psi_1,\ldots,\psi_m) \in \mathbb{C}^{n+m}$.

A *Hilbert space* of dimension n is the linear space $\mathbb{C}^n$ of n-dimensional complex row vectors equipped with sum and product by elements in $\mathbb{C}$, in which the *inner product* $\langle\varphi,\psi\rangle = \varphi\psi^\dagger$ is defined, for $\varphi,\psi \in \mathbb{C}^n$. The *norm* of a vector $\varphi \in \mathbb{C}^n$ is given by $\|\varphi\| = \sqrt{\langle\varphi,\varphi\rangle}$. If $\langle\varphi,\psi\rangle = 0$ (and $\|\varphi\| = 1 = \|\psi\|$), than φ and ψ are *orthogonal* (*orthonormal*). Two subspaces $X, Y \subseteq \mathbb{C}^n$ are orthogonal if any vector in X is orthogonal to any vector in Y. In this case, we denote by $X \dotplus Y$ the linear space generated by $X \cup Y$. For vectors φ and ψ, $\|\varphi\otimes\psi\| = \|\varphi\|\cdot\|\psi\|$.

A matrix $M \in \mathbb{C}^{n\times n}$ is said to be *unitary* whenever $MM^\dagger = I = M^\dagger M$. Equivalently, M is unitary if and only if it preserves the norm, i.e., $\|\varphi M\| = \|\varphi\|$ for any $\varphi \in \mathbb{C}^n$. It is easy to see that, given two unitary matrices A and B, the matrices $A\oplus B$, $A\otimes B$, and AB are unitary as well.

A matrix $H \in \mathbb{C}^{n\times n}$ is said to be *Hermitian (or self-adjoint)* whenever $H = H^\dagger$. A matrix $P \in \mathbb{C}^{n\times n}$ is a *projector* if and only if P is Hermitian and idempotent, i.e., $P^2 = P$. Given the Hermitian matrix H, let $c_1,\ldots,c_s$ be its eigenvalues and $E_1,\ldots,E_s$ the corresponding eigenspaces. It is well known that each eigenvalue c_k is real, that E_i is orthogonal to E_j for $i \neq j$, and that $E_1 \dotplus \cdots \dotplus E_s = \mathbb{C}^n$. Thus, every vector $\varphi \in \mathbb{C}^n$ can be uniquely decomposed as $\varphi = \varphi_1 + \cdots + \varphi_s$ for unique $\varphi_j \in E_j$. The linear transformation $\varphi \mapsto \varphi_j$ is the projector $P(c_j)$ onto the subspace E_j. Actually, the Hermitian matrix H is biunivocally determined by its eigenvalues and projectors as $H = \sum_{i=1}^{s} c_i P(c_i)$. We note that $\{P(c_1),\ldots,P(c_s)\}$ is a complete set of mutually orthogonal projectors, i.e., $\sum_{i=1}^{s} P(c_i) = I$ and $P(c_i)P(c_j)^\dagger = [\mathbf{0}]$ for $i \neq j$. For the Hermitian matrix $H = \sum_{i=1}^{s} c_i P(c_i)$, we define the circulant matrix built on $P(c_1),\ldots,P(c_s)$ as

$$\Xi(H) = \begin{pmatrix} P(c_1) & P(c_2) & \cdots & P(c_s) \\ P(c_2) & P(c_3) & \cdots & P(c_1) \\ \vdots & \vdots & \ddots & \vdots \\ P(c_s) & P(c_1) & \cdots & P(c_{s-1}) \end{pmatrix}.$$

The following lemma will be useful later:

Lemma 1. *Given a Hermitian matrix H, the matrix $\Xi(H)$ is unitary.*

2.2 Languages and Formal Power Series

We assume familiarity with basics in formal language theory (see, e.g., [12]). The set of all words (including the empty word ε) over a finite alphabet Σ is denoted by Σ^*. For a word $\omega \in \Sigma^*$, we let: $|\omega|$ denote its length, ω_i its ith symbol, $\omega[j] = \omega_1\omega_2 \cdots \omega_j$ its prefix of length $0 \leq j \leq |\omega|$ with $\omega[0] = \varepsilon$. For any $n \geq 0$, we let $\Sigma^n = \{\omega \in \Sigma^* \mid |\omega| = n\}$.

For a language $L \subseteq \Sigma^*$ and two words $v, w \in \Sigma^*$, the *word quotient* of L with respect to v, w is the language $v^{-1}Lw^{-1} = \{x \in \Sigma^* \mid vxw \in L\}$. For two alphabets Σ, Δ, a language $L \subseteq \Delta^*$, and a homomorphism $\phi : \Sigma^* \to \Delta^*$, the *inverse homomorphic image* of L is the language $\phi^{-1}(L) = \{x \in \Sigma^* \mid \phi(x) \in L\}$. For a word $y \in \Delta^*$, we set $\phi^{-1}(y) = \{x \in \Sigma^* \mid \phi(x) = y\}$. Thus, we have $\phi^{-1}(L) = \bigcup_{y \in L} \phi^{-1}(y)$.

A *formal power series (in noncommuting variables)* with coefficients in $\mathbb{C}$ is any function $\rho : \Sigma^* \to \mathbb{C}$, usually expressed by the formal sum $\rho = \sum_{\omega \in \Sigma^*} \rho(\omega)\, \omega$. We denote by $\mathbb{C}\langle\langle\Sigma\rangle\rangle$ the set of formal power series $\rho : \Sigma^* \to \mathbb{C}$. An important subclass of $\mathbb{C}\langle\langle\Sigma\rangle\rangle$ is the class $\mathbb{C}^{\text{Rat}}\langle\langle\Sigma\rangle\rangle$ of *rational series* [20].

One among possible characterizations of $\mathbb{C}^{\text{Rat}}\langle\langle\Sigma\rangle\rangle$ is given by the notion of linear representation. A *linear representation of dimension m* of a formal power series $\rho \in \mathbb{C}\langle\langle\Sigma\rangle\rangle$ is a triple $(\pi, \{A(\sigma)\}_{\sigma \in \Sigma}, \eta)$, with $\pi, \eta \in \mathbb{C}^m$ and $A(\sigma) \in \mathbb{C}^{m \times m}$, such that, for any $\omega \in \Sigma^*$, we have

$$\rho(\omega) = \pi A(\omega) \eta^\dagger = \pi \left(\prod_{i=1}^{|\omega|} A(\omega_i) \right) \eta^\dagger.$$

In [21], it is shown that *a formal power series is rational if and only if it has a linear representation (of finite dimension).*

Given a *real valued* $\rho \in \mathbb{C}\langle\langle\Sigma\rangle\rangle$ (i.e., with $\rho(\omega) \in \mathbb{R}$, for any $\omega \in \Sigma^*$) and a real cut-point λ, *the language defined by ρ with cut-point λ* is defined as the set

$$L_{\rho,\lambda} = \{\omega \in \Sigma^* \mid \rho(\omega) > \lambda\}.$$

The cut-point λ is said to be *isolated* if there exists a positive real δ such that $|\rho(\omega) - \lambda| > \delta$, for any $\omega \in \Sigma^*$.

We call *bounded series* any $\rho \in \mathbb{C}^{\text{Rat}}\langle\langle\Sigma\rangle\rangle$ admitting a linear representation $(\pi, \{A(\sigma)\}_{\sigma \in \Sigma}, \eta)$ such that $\|\pi A(\omega)\| \leq K$, for a fixed positive constant K and every $\omega \in \Sigma^*$. In [3], it is proved the following

Theorem 1. *Let $\rho \in \mathbb{C}^{\mathrm{Rat}}\langle\langle\Sigma\rangle\rangle$ be a real valued bounded series defining the language $L_{\rho,\lambda}$ with isolated cut-point λ. Then, $L_{\rho,\lambda}$ is a regular language.*

2.3 Finite Automata

A *deterministic finite automaton* (DFA) is a 5-tuple $\mathcal{D} = \langle S, \Sigma, \tau, s_1, F\rangle$, where S is the finite set of states, Σ the finite input alphabet, $s_1 \in S$ the initial state, $F \subseteq S$ the set of accepting states, and $\tau : S \times \Sigma \to S$ is the transition function. An input word is *accepted* by $\mathcal{D}$ if the induced computation starting from the initial state ends in some accepting state after consuming the whole input. The set $L_{\mathcal{D}}$ of all words accepted by $\mathcal{D}$ is called the accepted language. A linear representation for the DFA $\mathcal{D}$ is the 3-tuple $(\alpha, \{M(\sigma)\}_{\sigma\in\Sigma}, \beta)$, where $\alpha \in \{0,1\}^{|S|}$ is the characteristic row vector of the initial state, $M(\sigma) \in \{0,1\}^{|S|\times|S|}$ is the boolean transition matrix satisfying $(M(\sigma))_{ij} = 1$ if and only if $\tau(s_i, \sigma) = s_j$, and $\beta \in \{0,1\}^{|S|\times 1}$ is the characteristic column vector of the final states. The accepted language can now be defined as $L_{\mathcal{D}} = \{\omega \in \Sigma^* \mid \alpha M(\omega)\beta = 1\}$, where we let $M(\omega) = \prod_{i=1}^{|\omega|} M(\omega_i)$.

We introduce the model of a finite automaton with quantum and classical states [23]. In what follows, we denote by $\mathcal{U}(\mathbb{C}^n)$ ($\mathcal{O}(\mathbb{C}^n)$) the set of unitary (Hermitian) matrices on $\mathbb{C}^n$. As we will see, unitary matrices describe the evolution of the quantum component of the automaton, while Hermitian matrices represent observables to be measured.

Definition 1. *A* one-way finite automaton with quantum and classical states (QCFA) *is formally defined by the 9-tuple $\mathcal{A} = \langle Q, S, \Sigma, \Upsilon, \Theta, \tau, \pi_1, s_1, F\rangle$, where:*

- *Q is the finite set of orthonormal quantum basis states for the Hilbert space $\mathbb{C}^{|Q|}$ within which the quantum states are represented as vectors of norm 1,*
- *S is the finite set of classical states,*
- *Σ is the finite input alphabet; its extension by a right endmarker symbol $\sharp \notin \Sigma$ defines the tape alphabet $\Gamma = \Sigma \cup \{\sharp\}$,*
- *$\pi_1 \in \mathbb{C}^{|Q|}$ is the initial quantum state, satisfying $\|\pi_1\| = 1$,*
- *$s_1 \in S$ is the initial classical state,*
- *$F \subseteq S$ is the set of classical accepting states,*
- *$\Upsilon : S \times \Gamma \to \mathcal{U}(\mathbb{C}^{|Q|})$ is the mapping assigning, according to the current classical state and scanned tape symbol, a unitary transformation defining the evolution of the quantum state,*
- *$\Theta : S \times \Gamma \to \mathcal{O}(\mathbb{C}^{|Q|})$ is the mapping assigning, according to the current classical state and scanned tape symbol, a Hermitian matrix defining the observable to be measured on the quantum state,*
- *$\tau : S\times\Gamma\times\mathcal{C} \to S$ is the mapping defining the next classical state as a function of the current classical state, scanned tape symbol, and measurement outcome from a set $\mathcal{C}$.*

When addressing the *size*, we say that the QCFA $\mathcal{A}$ in Definition 1 has $|Q|$ quantum basis states and $|S|$ classical states.

Let us now explain in details how $\mathcal{A}$ works. Given an *input word* $\omega \in \Sigma^*$, we let $w = \omega\sharp$ be the associated *tape word* to be processed by $\mathcal{A}$. At any time along the computation on w, the quantum state of $\mathcal{A}$ is represented by a vector $\pi \in \mathbb{C}^{|Q|}$ with $\|\pi\| = 1$, while its classical state is an element from S. The computation starts in the quantum state π_1, in the classical state s_1, and by scanning w_1. Then, the transformations associated with symbols in w are applied in succession. Precisely, the transformation associated with a state $s \in S$ and a tape symbol $\gamma \in \Gamma$ consists of three steps:

- First: the unitary transformation $\Upsilon(s,\gamma)$ is applied to the current quantum state π, yielding the new quantum state $\pi' = \pi\Upsilon(s,\gamma)$.
- Second: the observable $\Theta(s,\gamma) = \sum_{i=1}^{m} c_i P(s,\gamma)(c_i)$ is measured on π', leading to one among the possible measurement outcomes from the set $\mathcal{C}(s,\gamma) = \{c_1,\ldots,c_m\}$. According to quantum mechanics principles, the outcome c_i is returned with probability $p_i = \|\pi' P(s,\gamma)(c_i)\|^2$, and correspondingly the quantum state π' collapses to the quantum state $\pi' P(s,\sigma)(c_i)/\sqrt{p_i}$.
- Third: the current classical state s switches to $\tau(s,\gamma,c_i)$, and the tape symbol γ is consumed.

The input word ω is *accepted* by $\mathcal{A}$ if the classical state reached after processing the right endmarker $\sharp$ of the corresponding tape word w is an accepting state, i.e., it belongs to F. Otherwise, ω is rejected. Clearly, accepting ω takes place with a certain probability we are now going to explicate.

Let $\mathcal{C} = \bigcup_{s\in S,\,\gamma\in\Gamma} \mathcal{C}(s,\gamma)$ be the set of measurement outcomes of all observables associated with $\mathcal{A}$. Indeed, in a standard fashion, we can define τ^* as the extension to $\bigcup_{i\geq 0}(S \times \Gamma^i \times \mathcal{C}^i)$ of the classical evolution $\tau : S \times \Gamma \times \mathcal{C} \to S$. More precisely, for any $s \in S$, $w \in \Gamma^n$, $y \in \mathcal{C}^n$, we let

$$\begin{aligned}&\tau^*(s,\varepsilon,\varepsilon) = s, \text{ and}\\ &\tau^*(s,w[j],y[j]) = \tau(\tau^*(s,w[j-1],y[j-1]),w_j,y_j) \text{ for } 1 \leq j \leq n.\end{aligned}$$

So, for a tape word $w = \omega\sharp \in \Sigma^{n-1}\sharp$, the probability that $\mathcal{A}$ accepts the corresponding input word ω can be written as

$$\mathcal{E}_{\mathcal{A}}(\omega) = \sum_{\{y \in \mathcal{C}^n \;\mid\; \tau^*(s_1,w,y) \in F\}} \|\pi_1 A(w,y)\|^2, \quad \text{with} \tag{1}$$

$$A(w,y) = \prod_{i=1}^{n} \Upsilon(\tau^*(s_1,w[i-1],y[i-1]),w_i) P(\tau^*(s_1,w[i-1],y[i-1]),w_i)(y_i)$$

and the convention that $P(s,\gamma)(c) = [\mathbf{0}]$ whenever $c \notin \mathcal{C}(s,\gamma)$. We maintain this convention throughout the rest of the paper. The function $\mathcal{E}_{\mathcal{A}} : \Sigma^* \to [0,1]$ is usually known as the *stochastic event induced by* $\mathcal{A}$. We notice that, in principle, $\mathcal{A}$ may exhibit a nonzero probability of accepting non well-formed inputs, i.e., words in $\Gamma^* \setminus \Sigma^*\sharp$. However, it is easy to see that, by augmenting the classical component with two new states, we can obtain a qcfa behaving as $\mathcal{A}$ on words in $\Sigma^*\sharp$ and rejecting with certainty words in $\Gamma^*\setminus\Sigma^*\sharp$. So, without loss of generality, throughout the rest of the paper, we will always be assuming the QCFA $\mathcal{A}$ to have this latter behavior.

We let $\rho_{\mathcal{A}} \in \mathbb{C}\langle\langle\Gamma\rangle\rangle$, the *real valued formal power series associated with* $\mathcal{A}$, be defined as $\rho_{\mathcal{A}}(\omega\sharp) = \mathcal{E}_{\mathcal{A}}(\omega)$ for every $\omega \in \Sigma^*$, and yielding 0 on words in $\Gamma^* \setminus \Sigma^*\sharp$. *The language accepted by* $\mathcal{A}$ *with cut-point* λ is defined to be the set

$$L_{\mathcal{A},\lambda} = (L_{\rho_{\mathcal{A}},\lambda})\sharp^{-1} = \{\omega \in \Sigma^* \ \mid \ \mathcal{E}_{\mathcal{A}}(\omega) > \lambda\}.$$

As for formal power series, the cut-point λ is said to be *isolated* if there exists a positive real δ such that $|\mathcal{E}_{\mathcal{A}}(\omega) - \lambda| > \delta$, for any $\omega \in \Sigma^*$. Acceptance with δ-isolated $\lambda = 1/2$ is also known in the literature as *bounded error acceptance* with error probability $1/2 - \delta$. It may be verified that, by adding one quantum basis state, isolated cut-point acceptance may be turned into bounded error acceptance.

As a final observation, we note that, for the model of QCFA in Definition 1, acceptance is determined by accepting states in the classical component. Alternatively, acceptance could be settled in the quantum component through an accepting/rejecting outcome of the measurement on $\sharp$. These two models of acceptance are actually equivalent.

3 Characterizing the Power of QCFAs

The fact that any regular language can be accepted by a QCFA comes trivially, due to the presence of the classical component (see [23] for formal details). Here, we focus on the converse, and show that the language accepted by any QCFA $\mathcal{A}$ with isolated cut-point is regular. To this aim, we prove that the associated formal power series $\rho_{\mathcal{A}}$ is bounded rational, and so we can apply Theorem 1. This direct approach also enables us to state a size lower bound for QCFAs accepting regular languages with isolated cut-point.

Consider a QCFA $\mathcal{A} = \langle Q, S = \{s_1, \ldots, s_k\}, \Sigma, \Upsilon, \Theta, \tau, \pi_1, s_1, F\rangle$, with q quantum basis states, k classical states, and $\mathcal{C} = \bigcup_{s\in S,\gamma\in\Gamma} \mathcal{C}(s,\gamma)$ the set of all possible measurement outcomes. We let the linear representation of the classical component be the 3-tuple $\langle \alpha, \{T(\gamma, c)\}_{\gamma\in\Gamma, c\in\mathcal{C}}, \beta\rangle$, where $\alpha = e_1 \in \{0,1\}^k$ is the characteristic vector of the initial state s_1, $\beta \in \{0,1\}^k$ is the characteristic vector of the set F of accepting states, and $T(\gamma, c) = \sum_{i=1}^k e_i^T \otimes e_{\mathrm{next}(i)}$, with $\mathrm{next}(i) = j \Leftrightarrow s_j = \tau(s_i, \gamma, c)$, is the $k \times k$ transition matrix on $\gamma \in \Gamma$, $c \in \mathcal{C}$ induced by τ. Moreover, we let $D(s_i, \gamma, c) = e_i^T \otimes e_{\mathrm{next}(i)}$ be the $k \times k$ matrix $T(\gamma, c)$ "restricted" to the ith row.

We let the 3-tuple $\mathrm{Li}(\mathcal{A}) = \langle \varphi_1, \{M(\gamma)\}_{\gamma\in\Gamma}, \eta\rangle$, with $\varphi_1 \in \mathbb{C}^{q^2k}$, $\eta \in \{0,1\}^{q^2k}$, and $M(\gamma) \in \mathbb{C}^{q^2k\times q^2k}$, be defined as:

- $\varphi_1 = \alpha \otimes \pi_1 \otimes \pi_1^*$,
- $M(\gamma) = \sum_{s\in S,\, c\in\mathcal{C}} D(s, \gamma, c) \otimes \Upsilon(s, \gamma)P(s, \gamma)(c) \otimes \Upsilon^*(s, \gamma)P^*(s, \gamma)(c)$,
- $\eta = \sum_{j=1}^q \beta \otimes e_j \otimes e_j$.

We are going to prove that $\mathrm{Li}(\mathcal{A})$ *is a linear representation of the formal power series* $\rho_{\mathcal{A}}$, meaning that $\rho_{\mathcal{A}}$ *is rational*, as pointed out in Section 2.2.

We begin by the following lemma which, very roughly speaking, says that a state vector of $\mathrm{Li}(\mathcal{A})$ "embodies" the evolution of the classical part of $\mathcal{A}$ in its first components (namely, by the operator $T(w, y)$ below), while the others account for the dynamics of the quantum part (by the operator $A(w, y)$):

Lemma 2. *For any $w \in \Gamma^n$ and $y \in \mathcal{C}^n$, we let $M(w) = \prod_{i=1}^n M(w_i)$ and $T(w, y) = \prod_{i=1}^n T(w_i, y_i)$. Then, for any two vectors $v_1, v_2 \in \mathbb{C}^q$, we have*

$$(\alpha \otimes v_1 \otimes v_2^*)M(w) = \sum_{y\in\mathcal{C}^n} \alpha\, T(w, y) \otimes v_1\, A(w, y) \otimes (v_2\, A(w, y))^* .$$

This enables us to state

Theorem 2. *Given a* QCFA $\mathcal{A}$*, the associated formal power series $\rho_{\mathcal{A}}$ is rational.*

Proof. It suffices to show that $\mathrm{Li}(\mathcal{A}) = \langle \varphi_1, \{M(\gamma)\}_{\gamma\in\Gamma}, \eta\rangle$ is a linear representation for $\rho_{\mathcal{A}}$, i.e.:

$$\rho_{\mathcal{A}}(w) = \varphi_1 M(w)\, \eta^\dagger, \quad \text{for any } w \in \Gamma^n.$$

Indeed, by Lemma 2, we have

$$\begin{aligned}
\varphi_1 M(w)\, \eta &= \left(\sum_{y\in\mathcal{C}^n} \alpha\, T(w, y) \otimes \pi_1\, A(w, y) \otimes (\pi_1\, A(w, y))^*\right) \cdot \sum_{j=1}^{q} \beta^\dagger \otimes {e_j}^\dagger \otimes {e_j}^\dagger \\
&= \sum_{y\in\mathcal{C}^n} \alpha\, T(w, y)\beta^\dagger \ \cdot \sum_{j=1}^{q} \left|(\pi_1\, A(w, y))_j\right|^2 \\
&= \sum\nolimits_{\{y \,\in\, \mathcal{C}^n \ \mid \ \tau^*(s_1, w, y) \,\in\, F\}} \|\pi_1 A(w, y)\|^2 ,
\end{aligned}$$

which, according to (1), is $\mathcal{E}_{\mathcal{A}}(\omega)$ if $w = \omega\sharp \in \Sigma^{n-1}\sharp$, and 0 otherwise. □

To show boundedness of $\rho_{\mathcal{A}}$, we need a generalization of Lemma 1 in [3]:

Lemma 3. *For a given $n \geq 0$, let $\{U(y[i-1]) \mid y \in \mathcal{C}^n, 1 \leq i \leq n\}$ be a set of unitary matrices, and $\{R(y[i-1])(y_i) \mid y \in \mathcal{C}^n, 1 \leq i \leq n\}$ a set of matrices such that, for any $0 \leq i \leq n-1$ and any word $\hat{y} \in \mathcal{C}^i$, the nonzero matrices in the set $\{R(\hat{y})(c) \mid c \in \mathcal{C}\}$ define an observable (i.e., they form a complete set of mutually orthogonal projectors). Then, for any complex vector π, we get*

$$\sum_{y\in\mathcal{C}^n} \left\|\pi \prod_{i=1}^{n} U(y[i-1])R(y[i-1])(y_i)\right\|^2 = \|\pi\|^2. \tag{2}$$

We are now ready to prove boundedness of the series associated with QCFAs:

Theorem 3. *Given a* QCFA $\mathcal{A}$*, the associated formal power series $\rho_{\mathcal{A}}$ is bounded.*

Proof. Consider the linear representation $\mathrm{Li}(\mathcal{A}) = \langle \varphi_1, \{M(\gamma)\}_{\gamma \in \Gamma}, \eta \rangle$ of $\rho_{\mathcal{A}}$. We show that, for any $w \in \Gamma^n$, we get $\|\varphi_1 M(w)\| \leq 1$. Indeed, we have

$$\begin{aligned} \|\varphi_1 M(w)\| &= \left\| \sum_{y \in \mathcal{C}^n} \alpha T(w,y) \otimes (\pi_1 A(w,y)) \otimes (\pi_1 A(w,y))^* \right\| && \text{(by Lemma 2)} \\ &\leq \sum_{y \in \mathcal{C}^n} \|\alpha T(w,y)\| \cdot \|\pi_1 A(w,y)\|^2 && \text{(by triangular inequality)} \\ &= \sum_{y \in \mathcal{C}^n} \|\pi_1 A(w,y)\|^2 = \|\pi_1\|^2 = 1 && \text{(by Lemma 3 on } A(w,y)\text{).} \end{aligned}$$

□

In conclusion, we get our main result

Theorem 4. *The class of languages accepted by* QCFAs *with isolated cut-point coincides with the class of regular languages.*

Proof. As observed at the beginning of this section, QCFAs accept all regular languages. For the converse, Theorems 1, 2, and 3 ensures that, for any QCFA $\mathcal{A}$ and any isolated cut-point λ, the language $L_{\rho_A,\lambda}$ is regular. This, together with the fact that regular languages are closed under word quotient, clearly implies that $L_{\mathcal{A},\lambda} = (L_{\rho_A,\lambda})\sharp^{-1}$ is regular. □

A natural question arising from Theorem 4 is the size-cost of converting a given QCFA $\mathcal{A}$ into a language-equivalent DFA. Starting from the linear representation $\mathrm{Li}(\mathcal{A})$ which has dimension q^2k, we can apply the Rabin-like technique presented in [7] to get an equivalent DFA whose number of states is bounded as:

Theorem 5. *For any* QCFA *$\mathcal{A}$ with q quantum basis states, k classical states, and δ-isolated cut-point λ, there exists a m-state* DFA *accepting $L_{\mathcal{A},\lambda}$, with*

$$m \leq \left(1 + \frac{4\sqrt{qk}}{\delta}\right)^{q^2k}.$$

We quickly point out that this result can be used "the other way around", to get a size lower bound for QCFAs accepting regular languages, namely: any QCFA with q quantum states, k classical states, and δ-isolated cut point accepting a regular language whose minimal DFA has μ states, must satisfy

$$qk \geq \left(\frac{\log(\mu)}{\log(5/\delta)}\right)^{\frac{4}{9}}.$$

The optimality of such lower bound is an open problem. As a partial answer, we can immediately state that the optimal lower bound cannot be raised to $\omega(\log(\mu))$, since an asymptotically optimal lower bound of $\log(\mu)/(2\log(1+2/\delta))$ is obtained in [5] for measure-once quantum automata, which are easily simulated by QCFAs with the same number of quantum basis states and 3 classical states [23].

4 Size-Cost of Language Operations on QCFAs

By the characterization in the previous section, we immediately get that the class of languages accepted by QCFAs with isolated cut-point is closed under word quotients and inverse homomorphic images. Here, we are going to explicitly construct QCFAs that accept word quotients and inverse homomorphic images of regular languages defined by QCFAs. This allows us to study the cost, in terms of quantum basis states and classical states, of implementing such operations on QCFAs.

It is well known that on DFAs both word quotients and inverse homomorphisms can be easily implemented without increasing the number of states. Here, we perform such operations on QCFAs by polynomially increasing the size and preserving cut-point and isolation.

We begin by approaching the construction of QCFAs for word quotients. We construct QCFAs for accepting $\sigma^{-1}L$ and $L\sigma^{-1}$, for given $\sigma \in \Sigma$ and a language $L \subseteq \Sigma^*$ accepted by a QCFA with isolated cut-point. By iterating these constructions, one obtains a QCFA for $v^{-1}Lw^{-1}$, for given $v, w \in \Sigma^*$.

Theorem 6. *Let $L \subseteq \Sigma^*$ be a language accepted with δ-isolated cut-point λ by a* QCFA *A with q quantum basis states and k classical states. Then, for any given $\sigma_0 \in \Sigma$, there exists a* QCFA *B with at most q^2 quantum basis states and $k+1$ classical states that accepts $\sigma_0^{-1}L$ with δ-isolated cut-point λ.*

Proof. Let the QCFA $A = \langle Q, S, \Sigma, \Upsilon, \Theta, \tau, \pi_0, s_0, F\rangle$. To avoid too heavy technicalities, we assume that all observables associated with A exhibit the same set $\mathcal{C} = \{c_0, \ldots, c_{h-1}\}$ of outcomes. So, for any $s \in S$ and $\sigma \in \Sigma \cup \{\sharp\}$, we have $\Theta(s,\sigma) = \sum_{j=0}^{h-1} c_j P(s,\sigma)(c_j)$. However, our technique can be easily adapted to the general case.

We construct the QCFA $B = \langle \hat{Q}, S \cup \{\hat{s}_0\}, \Sigma, \hat{\Upsilon}, \hat{\Theta}, \hat{\tau}, \hat{\pi}_0, \hat{s}_0, F\rangle$ such that:

- $\hat{Q} = \{e_j \otimes \pi \ \mid \ \pi \in Q, \ e_j \in \mathbb{C}^h, 1 \le j \le h\}$,
- $\hat{\pi}_0 = \bigoplus_{j=0}^{h-1} \pi_0 \Upsilon(s_0,\sigma_0) P(s_0,\sigma_0)(c_j)$,
- for $s \in S$ and $\sigma \in \Sigma \cup \{\sharp\}$, we set $\hat{\Upsilon}(s,\sigma) = \bigoplus_{j=0}^{h-1} \Upsilon(s,\sigma)$, and $\hat{\Upsilon}(\hat{s}_0,\sigma) = \bigoplus_{j=0}^{h-1} \Upsilon(\tau(s_0,\sigma_0,c_j),\sigma)$,
- for $s \in S \cup \{\hat{s}_0\}$ and $\sigma \in \Sigma \cup \{\sharp\}$, we set $\hat{\Theta}(s,\sigma) = \sum_{j=0}^{h-1} \sum_{i=0}^{h-1} \hat{c}_{i,j} \hat{P}(s,\sigma)(\hat{c}_{i,j})$, with $\hat{P}(s,\sigma)(\hat{c}_{i,j}) = [\mathbf{0}]_{(j-1)q} \oplus P(s_{l_j},\sigma)(c_i) \oplus [\mathbf{0}]_{(h-j)q}$ and $s_{l_j} = \tau(s_0,\sigma_0,c_j)$ if $s = \hat{s}_0$, otherwise $s_{l_j} = s$. We let $\hat{\mathcal{C}} = \{\hat{c}_{i,j} \ \mid \ 0 \le i,j \le h-1\}$ be the set of the outcomes of all observables associated with B,
- for $s \in S$ and $\sigma \in \Sigma \cup \{\sharp\}$, we set $\hat{\tau}(s,\sigma,\hat{c}_{i,j}) = \tau(s,\sigma,c_i)$, and $\hat{\tau}(\hat{s}_0,\sigma,\hat{c}_{i,j}) = \tau^*(s_0,\sigma_0\sigma,c_jc_i)$.

We describe intuitively how the QCFA B on input $\omega\sharp$ mimics the computation of A on input $\sigma_0\omega\sharp$. The initial quantum state $\hat{\pi}_0$ consists of h blocks. Each one represents the unitary evolution of A on σ_0 from states π_0 and s_0, followed by one among the h projections associated with the observable $\Theta(s_0,\sigma_0)$. Upon reading the first input symbol, B implements in the jth block the evolution in A associated with the classical state $\tau(s_0, \sigma_0, c_j)$ and symbol ω_1, followed by a measurement yielding the result $\hat{c}_{i,j}$. Such a measurement simulates the outcome sequence $c_j c_i$ possibly obtained in A while processing the input prefix $\sigma_0\omega_1$. From ω_2 on, the computation of A is simulated in the jth block, in which an outcome $\hat{c}_{i,j}$ corresponds to the outcome c_i in A. One may verify that the probability that B accepts ω coincides with the probability that A accepts $\sigma_0\omega$. Clearly, B has $k+1$ classical states and $hq \leq q^2$ quantum basis states. □

Theorem 7. *Let $L \subseteq \Sigma^*$ be a language accepted with δ-isolated cut-point λ by a* QCFA *A with q quantum basis states and k classical states. Then, for any given $\sigma_0 \in \Sigma$, there exists a* QCFA *B with at most q^2 quantum basis states and k classical states that accepts $L\sigma_0^{-1}$ with δ-isolated cut-point λ.*

Proof. Let the QCFA $A = \langle Q, S, \Sigma, \Upsilon, \Theta, \tau, \pi_0, s_0, F\rangle$. As in the previous proof, all the observables of A are assumed of the form $\Theta(s,\sigma) = \sum_{j=0}^{h-1} c_j P(s,\sigma)(c_j)$.

We construct the QCFA $B = \langle \hat{Q}, S, \Sigma, \hat{\Upsilon}, \hat{\Theta}, \hat{\tau}, \hat{\pi}_0, s_0, F\rangle$ such that:

- $\hat{Q} = \{e_j \otimes \pi \mid \pi \in Q,\ e_j \in \mathbb{C}^h, 1 \leq j \leq h\}$,
- $\hat{\pi}_0 = \pi_0 \oplus \mathbf{0}_{q(h-1)}$,
- for $s \in S$ and $\sigma \in \Sigma$, we set $\hat{\Upsilon}(s,\sigma) = \Upsilon(s,\sigma) \oplus I_{q(h-1)}$, and $\hat{\Upsilon}(s,\sharp) = \left(\bigoplus_{j=0}^{h-1} \Upsilon(s,\sigma_0)\right) \cdot \Xi(\Theta(s,\sigma_0)) \cdot \left(\bigoplus_{j=0}^{h-1} \Upsilon(\tau(s,\sigma_0,c_j),\sharp)\right)$, where $\Xi(\Theta(s,\sigma_0))$ is the unitary circulant matrix addressed in Lemma 1.
- for $s \in S$ and $\sigma \in \Sigma \cup \{\sharp\}$, we set $\hat{\Theta}(s,\sigma) = \sum_{j=0}^{h-1}\sum_{i=0}^{h-1} \hat{c}_{i,j}\hat{P}(s,\sigma)(\hat{c}_{i,j})$, with $\hat{P}(s,\sigma)(\hat{c}_{i,j}) = [\mathbf{0}]_{(j-1)q} \oplus P(s_{l_j},\sigma)(c_i) \oplus [\mathbf{0}]_{(h-j)q}$ and $s_{l_j} = \tau(s,\sigma_0,c_j)$ if $\sigma = \sharp$, otherwise $s_{l_j} = s$. We let $\hat{\mathcal{C}} = \{\hat{c}_{i,j} \mid 0 \leq i,j \leq h-1\}$ be the set of the outcomes of all observables associated with B,
- for $s \in S$ and $\sigma \in \Sigma$, we set $\hat{\tau}(s,\sigma,\hat{c}_{i,j}) = \tau(s,\sigma,c_i)$ and $\hat{\tau}(s,\sharp,\hat{c}_{i,j}) = \tau^*(s,\sigma_0\sharp,c_jc_i)$.

The initial quantum state $\hat{\pi}_0$ consists of h blocks, all being zero blocks except the first being π_0. On the symbols of the tape word $\omega\sharp$ preceding the endmarker, B implements in the first block the same computation as A, leading to a state vector $\pi' \oplus \mathbf{0}_{q(h-1)}$. Upon reading $\sharp$, the application of the operator $\hat{\Upsilon}(s,\sharp)$ has the effect of storing the vector $\pi'\Upsilon(s,\sigma_0)P(s,\sigma_0)(c_j)\Upsilon(\tau(s,\sigma_0,c_j),\sharp)$ in the jth block. Moreover, the outcome $\hat{c}_{i,j}$ of the measurement on $\sharp$ in B corresponds to the outcome sequence c_jc_i possibly obtained in A while processing the input suffix $\sigma_0\sharp$. Clearly, the probability that B accepts ω coincides with the probability that A accepts $\omega\sigma_0$. The number of classical states in B remains k, while the number of quantum states is $hq \leq q^2$. □

Let us now focus on constructing QCFAs for inverse homomorphic images. We recall that a homomorphism $\phi : \Sigma^* \to \Delta^*$ of a free monoid into another is entirely defined by the image of each symbol in Σ.

Theorem 8. *Let $L \subseteq \Sigma^*$ be a language accepted with δ-isolated cut-point λ by a* QCFA *A with q quantum basis states and k classical states. Then, for any given* *homomorphism* $\phi : \Sigma \to \Delta^*$, *with* $m = \max\{|\phi(\sigma)| \mid \sigma \in \Sigma\}$, *there exists a* QCFA B *with at most* q^{m+1} *quantum basis states and* $q^m k$ *classical states that accepts* $\phi^{-1}(L)$ *with* δ*-isolated cut-point* λ.

Proof. For reader's ease of mind, we exhibit our construction for a homomorphism $\phi\colon \{a,b\} \to \{\alpha,\beta\}^*$ defined as $\phi(a) = \alpha\beta$ and $\phi(b) = \beta$, so that $m = 2$. Yet, we consider the language L to be accepted by a QCFA A with binary observables. These assumptions do not substantially affect the generality of our construction. So, let the QCFA $A = \langle Q, S, \{\alpha,\beta\}, \Upsilon, \Theta, \tau, \pi_0, s_0, F\rangle$, where all observables are assumed to have the form $\Theta(s,\sigma) = 0 \cdot P(s,\sigma)(0) + 1 \cdot P(s,\sigma)(1)$ and hence with $\mathcal{C} = \{0,1\}$ as set of outcomes.

We construct the QCFA $B = \langle \hat{Q}, \hat{S}, \{a,b\}, \hat{\Upsilon}, \hat{\Theta}, \hat{\tau}, \hat{\pi}_0, (s_0,0), \hat{F}\rangle$ such that:

- $\hat{Q} = \{e_j \otimes \pi \mid \pi \in Q,\ e_j \in \mathbb{C}^4, 1 \le j \le 4\}$,
- $\hat{S} = \{(s,j) \mid s \in S,\ 0 \le j \le 3\}$,
- $\hat{\pi}_0 = \pi_0 \oplus \mathbf{0}_{3q}$,
- for $(s,0) \in \hat{S}$, we set $\hat{\Upsilon}((s,0),a) = \begin{pmatrix} A_0 & A_1 \\ A_1 & A_0 \end{pmatrix} \cdot \begin{pmatrix} B_0 & [\mathbf{0}] \\ [\mathbf{0}] & B_1 \end{pmatrix}$, where

$$A_i = \Upsilon(s,\alpha)P(s,\alpha)(i) \oplus \Upsilon(s,\alpha)P(s,\alpha)(i),$$

$$B_i = \begin{pmatrix} \Upsilon(\tau(s,\alpha,i),\beta)P(\tau(s,\alpha,i),\beta)(0) & \Upsilon(\tau(s,\alpha,i),\beta)P(\tau(s,\alpha,i),\beta)(1) \\ \Upsilon(\tau(s,\alpha,i),\beta)P(\tau(s,\alpha,i),\beta)(1) & \Upsilon(\tau(s,\alpha,i),\beta)P(\tau(s,\alpha,i),\beta)(0) \end{pmatrix},$$

  and $\hat{\Upsilon}((s,0),b) = C \oplus C$, where

$$C = \begin{pmatrix} \Upsilon(s,\beta)P(s,\beta)(0) & \Upsilon(s,\beta)P(s,\beta)(1) \\ \Upsilon(s,\beta)P(s,\beta)(1) & \Upsilon(s,\beta)P(s,\beta)(0) \end{pmatrix};$$

  for $(s,j) \in \hat{S}$ with $j \neq 0$, we set

$$\hat{\Upsilon}((s,j),a) = \Pi^j \cdot \hat{\Upsilon}((s,0),a), \quad \hat{\Upsilon}((s,j),b) = \Pi^j \cdot \hat{\Upsilon}((s,0),b),$$

  where $\Pi = \begin{pmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{pmatrix} \otimes I_q$ is the circular block permutation matrix,
- for $(s,j) \in \hat{S}$ and $\sigma \in \{a,b\}$, we set $\hat{\Theta}((s,j),\sigma) = \sum_{i=0}^{3} c_i \cdot [\mathbf{0}]_{iq} \oplus I_q \oplus [\mathbf{0}]_{(3-i)q}$,
- for $(s,j) \in \hat{S}$ and $0 \le i \le 3$, we set $\hat{\tau}((s,j),a,c_i) = (\tau^*(s,\alpha\beta,\mathrm{bin}_2(i)),i)$, and $\hat{\tau}((s,j),b,c_i) = (\tau^*(s,\beta,\mathrm{bin}_1(i)),i)$, where $\mathrm{bin}_2(i)$ is the binary representation of i on 2 bits, while $\mathrm{bin}_1(i) = 0^{-1}\mathrm{bin}_2(i) \cup 1^{-1}\mathrm{bin}_2(i)$,
- $\hat{F} = \{(s,j) \in \hat{S} \mid s \in F\}$.

The evolution matrices of the QCFA B can be regarded as block matrices with blocks of dimension $q \times q$. For $0 \le i,j \le 3$, the (i,j)th block of $\hat{\Upsilon}((s,i),a)$ is $\Upsilon(s,\alpha)P(s,\alpha)(j_1)\Upsilon(\tau(s,\alpha,j_1),\beta)P(\tau(s,\alpha,j_1),\beta)(j_2)$ with $j_1 j_2 = \mathrm{bin}_2(j)$, while the (i,j)th block of $\hat{\Upsilon}((s,i),b)$ is $\Upsilon(s,\alpha)P(s,\alpha)(j)$ for $j = 0,1$, and is $[\mathbf{0}]_q$ for $j = 2,3$. Analogously, $\hat{\pi}_0$ consists of 4 blocks, all being zero blocks except the first being π_0. On reading a (b), the evolution matrix in B simulates the sequence of evolutions and measurements of A while processing $\alpha\beta$ (β), and stores each possible resulting quantum state in each block. Then, the observable acts on the jth block, and the outcome c_j represents the outcome sequence $\mathrm{bin}_2(j)$ ($\mathrm{bin}_1(j)$; notice that the possible outcomes of the measurements on b are only c_0 and c_1) in A. At any time, only one block of the quantum state of B is nonzero. This information is encoded in the classical state so that the evolution matrix in B selected by the classical state always stores in the jth block the result of the simulation of A for the outcome sequence $\mathrm{bin}_2(j)$ ($\mathrm{bin}_1(j)$). The function $\hat{\tau}$ mimics the transition function τ in the state first component, and stores in the second component the index of the nonzero block of the quantum state of B. One may verify that the probability that B accepts ω coincides with the probability that A accepts $\phi^{-1}(\omega)$. The number of classical states is $2^2k = |\mathcal{C}|^m k \leq q^m k$, while the number of quantum basis states is $2^2q = |\mathcal{C}|^m q \leq q^{m+1}$. □

References

1. Ambainis, A., Beaudry, M., Golovkins, M., Kikusts, A., Mercer, M., Thérien, D.: Algebraic results on quantum automata. Theory of Comp. Sys. 39, 165–188 (2006)
2. Ambainis, A., Watrous, J.: Two-way finite automata with quantum and classical states. Theoretical Computer Science 287, 299–311 (2002)
3. Bertoni, A., Mereghetti, C., Palano, B.: Quantum computing: 1-way quantum automata. In: Ésik, Z., Fülöp, Z. (eds.) DLT 2003. LNCS, vol. 2710, pp. 1–20. Springer, Heidelberg (2003)
4. Bertoni, A., Mereghetti, C., Palano, B.: Small size quantum automata recognizing some regular languages. Theoretical Computer Science 340, 394–407 (2005)
5. Bertoni, A., Mereghetti, C., Palano, B.: Some formal tools for analyzing quantum automata. Theoretical Computer Science 356, 14–25 (2006)
6. Bertoni, A., Mereghetti, C., Palano, B.: Trace monoids with idempotent generators and measure-only quantum automata. Natural Computing 9, 383–395 (2010)
7. Bianchi, M.P., Mereghetti, C., Palano, B.: Size Lower Bounds for Quantum Automata. In: Mauri, G., Dennunzio, A., Manzoni, L., Porreca, A.E. (eds.) UCNC 2013. LNCS, vol. 7956, pp. 19–30. Springer, Heidelberg (2013)
8. Bianchi, M.P., Palano, B.: Behaviours of unary quantum automata. Fundamenta Informaticae 104, 1–15 (2010)
9. Brodsky, A., Pippenger, N.: Characterizations of 1-way quantum finite automata. SIAM J. Computing 5, 1456–1478 (2002)
10. Golovkins, M., Kravtsev, M.: Probabilistic reversible automata and quantum automata. In: Ibarra, O.H., Zhang, L. (eds.) COCOON 2002. LNCS, vol. 2387, pp. 574–583. Springer, Heidelberg (2002)
11. Hirvensalo, M.: Quantum automata with open time evolution. Int. J. Natural Computing Research 1, 70–85 (2010)
12. Hopcroft, J.E., Motwani, R., Ullman, J.D.: Introduction to Automata Theory, Languages, and Computation. Addison-Wesley, Reading (2001)
13. Kondacs, A., Watrous, J.: On the power of quantum finite state automata. In: Proc. 38th Symposium on Foundations of Computer Science (FOCS 1997), pp. 66–75 (1997)

14. Li, L., Qiu, D., Zou, X., Li, L., Wu, L., Mateus, P.: Characterizations of one-way general quantum finite automata. Theoretical Computer Science 419, 73–91 (2012)
15. Mercer, M.: Lower bounds for generalized quantum finite automata. In: Martín-Vide, C., Otto, F., Fernau, H. (eds.) LATA 2008. LNCS, vol. 5196, pp. 373–384. Springer, Heidelberg (2008)
16. Moore, C., Crutchfield, J.: Quantum automata and quantum grammars. Theoretical Computer Science 237, 275–306 (2000)
17. Mereghetti, C., Palano, B.: Quantum finite automata with control language. Theoretical Informatics and Applications 40, 315–332 (2006)
18. Mereghetti, C., Palano, B.: Quantum automata for some multiperiodic languages. Theoretical Computer Science 387, 177–186 (2007)
19. Nayak, A.: Optimal lower bounds for quantum automata and random access codes. In: Proc. 40th Symp. Found. Comp. Sci (FOCS 1999), pp. 369–376 (1999)
20. Salomaa, A., Soittola, M.: Automata theoretic aspects of formal power series. In: Texts and Monographs in Computer Science. Springer (1978)
21. Schützenberger, M.P.: On the definition of a family of automata. Information and Control 4, 245–270 (1961)
22. Shilov, G.: Linear Algebra. Prentice Hall (1971); Reprinted by Dover (1977)
23. Zheng, S., Qiu, D., Li, L., Gruska, J.: One-Way finite automata with quantum and classical states. In: Bordihn, H., Kutrib, M., Truthe, B. (eds.) Dassow Festschrift 2012. LNCS, vol. 7300, pp. 273–290. Springer, Heidelberg (2012)