Available online at www.sciencedirect.com

SCIENCE DIRECT

Theoretical Computer Science 356 (2006) 14–25

Theoretical Computer Science

www.elsevier.com/locate/tcs

Some formal tools for analyzing quantum automata☆

Alberto Bertoni, Carlo Mereghetti*, Beatrice Palano

Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano, via Comelico 39/41, 20135 Milano, Italy

Abstract

Results in the area of compact monoids and groups are useful in the analysis of quantum automata (1qfa's). In this paper:

(1) We settle isolated cut point Rabin's theorem in the context of compact monoids, and we prove a lower bound on the state complexity of 1qfa's accepting regular languages.
(2) We use a method pointed out by Blondel et al. [Decidable and undecidable problems about quantum automata, Technical Report RR2003-24, LIP, ENS Lyon, 2003] based on compact groups theory to design an algorithm for testing whether a k-tuple of 1qfa's is a classifier of words in Σ^*; this problem turns out to be undecidable if the completeness of the classifier is required.
(3) In the unary case, we give an exponential time algorithm for computing the descriptional complexity of periodic languages. Moreover, we present a probabilistic method to construct 1qfa's exponentially succinct in the period and polynomially succinct in the inverse of the bounded error.

Keywords: Quantum automata

1. Introduction

In the early 1980s, Feynman first suggests that the computational power of quantum mechanical processes might be beyond that of traditional computation models [19]. Discussing the notion of "quantum computer", Deutsch [18] introduces the quantum Turing machine as a physically realizable model for a quantum computer. From the point of view of structural complexity, the class BQP of problems solvable in polynomial time on quantum Turing machines is introduced [5].

The power of quantum paradigm crucially relies on the features of quantum systems: superposition, interference and observation. A well known result witnessing quantum power is Shor's algorithm for integer factorization which runs in polynomial time on a quantum computer [27]. Another relevant progress is made by Grover [21] who proposes a quantum algorithm for searching an item in an unsorted database containing n items in time $O(\sqrt{n})$.

☆ Partially supported by M.I.U.R. COFIN, under the projects "Linguaggi formali e automi: metodi, modelli e applicazioni", and "FIRB: Complessità descrizionale di automi e strutture correlate". Some results in this paper were presented in a preliminary form at the Seventh International Workshop on Descriptional Complexity of Formal Systems (DCFS05), Como, Italy, 2005.

* Corresponding author.
E-mail addresses: bertoni@dsi.unimi.it (A. Bertoni), mereghetti@dsi.unimi.it (C. Mereghetti), palano@dsi.unimi.it (B. Palano).

0304-3975/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2006.01.042

Some efforts have been made for constructing quantum devices, and their realizations seems to be a difficult task. For this reason, it can be useful to study the computational characteristics of simple devices such as 1-way quantum automata (1qfa's). Several models of 1qfa's have been introduced in the literature, among them measure-once [6,12,24], measure-many [2], reversible [20] 1qfa's and 1qfa's with control language [8]. A measure-once 1qfa evolves undisturbed on the whole input string, and only at the end an observation is performed, while in the other models an observation is performed after each input symbol reading. The behavior of a 1qfa is given by the set of words whose acceptance probability is larger than a fixed cut point.

1qfa's exhibit both advantages and disadvantages with respect to their classical (deterministic or probabilistic) counterpart. Basically, quantum superposition offers some computational advantages on probabilistic superposition. On the other hand, quantum dynamics are reversible: because of limitation of memory, it is sometimes impossible to simulate deterministic automata by quantum automata.

This paper shows some formal methods useful to analyze 1qfa's, by restricting to the simplest model, i.e., the measure-once. These methods should be able to study "continuous systems" (described by vectors and matrices with complex entries) having "discrete behaviors" (the accepted languages). The paper is dedicated to Christian Choffrut, who devoted great part of his research to analyze automata models by means of algebraic and computational methods (see, for instance [14,15]; for decidability questions on semigroups of matrices, see [16]).

After a brief introduction on quantum automata, in Section 3 we set Rabin's theorem (i.e., probabilistic languages recognized with isolated cut point are regular) in the more abstract context of compact monoids. As a consequence of this viewpoint, we prove a lower bound on the quantum state complexity of regular languages in terms of their deterministic state complexity (Theorem 2).

In Section 4, we present some elements of the elegant theory of compact groups. The relevant role played by this theory in the area of quantum automata, together with the decidability of the (first order) theory of real fields, have been pointed out by Blondel et al. [11], who developed a nice methodology for approaching some decidability questions on 1qfa's. They proved, for instance, that it is decidable whether a 1qfa A with rational amplitudes accepts with cut point $\frac{1}{2}$ the empty set, or whether a rational λ is an isolated cut point for A; notice that the corresponding problems for stochastic automata are undecidable [7,26]. We apply these tools for investigating problems related to the classification of words by means of quantum automata. A *k-quantum classifier* consists of 1qfa's $A_1, \ldots, A_k$ on input alphabet Σ satisfying: (1) each automaton accepts at least one word in Σ^*; (2) every word in Σ^* is accepted by at most one automaton. The intended meaning is that all automata compete for recognizing a word, but at most one automaton is the winner. A classifier is *complete* if, in addition, every word in Σ^* is accepted by some automaton.

We study the problems of deciding whether a family $A_1, \ldots, A_k$ of 1qfa's is a quantum classifier (k-Q.CLASSIFIER), or a complete quantum classifier (COMPLETE k-Q.CLASSIFIER). 1-Q.CLASSIFIER is equivalent to decide whether the language recognized by a 1qfa is not empty, while COMPLETE 1-Q.CLASSIFIER is equivalent to decide whether the language recognized by a 1qfa is Σ^*: these two problems with $k = 1$ were investigated in [11], where it is proved that the former is decidable, while the latter is undecidable. In this paper we extend these results to the general case.

In Section 5, we investigate the descriptional power of 1qfa's with isolated cut point versus that of deterministic automata in the case of unary languages (i.e., languages on alphabet Σ with $|\Sigma| = 1$). We show an exponential time algorithm for computing the quantum descriptional complexity of periodic languages and we discuss a method for constructing "succinct" 1qfa's recognizing a given language. As an application, we exhibit a Monte Carlo 1qfa recognizing the language $L_n = \{a^{kn} \mid k \in \mathbf{N}\}$ with bounded error ε and $O((1/\varepsilon^3) \log n)$ states; for every fixed $\varepsilon > 0$ and n prime, the construction is asymptotically optimal.

2. Preliminaries: 1-way quantum finite automata

By $\mathbf{C}^{n\times m}$ (resp., $\mathbf{C}^{(n)}$) we denote the set of $n \times m$ (resp., $n \times n$) matrices with complex entries.

Given a set $Q = \{q_1, \ldots, q_m\}$, every q_i can be represented by its characteristic vector $e_i = (0, \ldots, 1, \ldots, 0)$. A *quantum state* on Q is an element in $\mathbf{C}^{1\times m}$ given by a superposition $\pi = \sum_{k=1}^{m} \pi_k e_k$, where the coefficients $\pi_k \in \mathbf{C}$ are *amplitudes* and the norm $\| \pi \|$ of π is equal to 1. Every e_k is called *pure state*. Given an alphabet $\Sigma = \{\sigma_1, \ldots, \sigma_l\}$, with every symbol σ_i we associate a unitary matrix $U(\sigma_k) \in \mathbf{C}^{(m)}$, i.e., $\| \xi U(\sigma_k) \| = \| \xi \|$ for each $\xi \in \mathbf{C}^{1\times m}$. An

observable is described by an Hermitian matrix $\mathcal{O}$, i.e., $\mathcal{O} = \mathcal{O}^\dagger$, where $\mathcal{O}^\dagger$ denotes the adjoint of $\mathcal{O}$. The eigenvalues $c_1, \ldots, c_s$ of $\mathcal{O}$ are reals; by denoting $P_1, \ldots, P_s$ the projectors onto the corresponding eigenspaces, it holds that $\mathcal{O} = c_1 P_1 + \cdots + c_s P_s$. We recall that $P_i P_j = \mathbf{0}$ (the $m \times m$ zero matrix) for $1 \leqslant i \neq j \leqslant s$ and $\sum_{i=1}^{s} P_i = I$.

Suppose that a quantum system is described by the quantum state π. Then, we can operate

(1) *Evolution* $U(\sigma_j)$. In this case, the new state $\xi = \pi U(\sigma_j)$ is reached; this dynamics is reversible, since $\pi = \xi U^\dagger(\sigma_j)$.
(2) *Measurement of* $\mathcal{O}$. In this case, every result in $\{c_1, \ldots, c_s\}$ can be obtained; c_j is obtained with probability $\| \pi P_j \|^2$ and the state after such a measurement is $\pi P_j / \| \pi P_j \|$. The state transformation induced by a measurement is typically irreversible.

A (measure-once), 1qfa for short, with q pure states on the input alphabet Σ is a system $A = (\pi, \{U(\sigma)\}_{\sigma \in \Sigma}, \eta)$, where $\pi \in \mathbf{C}^{1 \times q}$ and $\|\pi\| = 1$, $U(\sigma) \in \mathbf{C}^{(q)}$ is a unitary matrix for each $\sigma \in \Sigma$, $\eta = (\eta_1, \ldots, \eta_q) \in \{0, 1\}^q$ is the characteristic vector of the (final) states.

The *stochastic event induced by* A is the function $p_A : \Sigma^* \to [0, 1]$ defined, for any $\sigma_1 \cdots \sigma_k \in \Sigma^*$, by

$$p_A(\sigma_1 \cdots \sigma_k) = \sum_{\eta_j = 1} \left| \left(\pi \left(\prod_{i=1}^{k} U(\sigma_i) \right) \right)_j \right|^2,$$

where $|z|$ is the modulus of $z \in \mathbf{C}$. Equivalently, the 1qfa $A = (\pi, \{U(\sigma)\}_{\sigma \in \Sigma}, \eta)$ can be specified by $A = (\pi, \{U(\sigma)\}_{\sigma \in \Sigma}, P)$, where $P \in \mathbf{C}^{(q)}$ is the projector on the subspace spanned by the final states. In this case, the event p_A can be obtained as

$$p_A(\sigma_1 \cdots \sigma_k) = \left\| \pi \left(\prod_{i=1}^{k} U(\sigma_i) \right) P \right\|^2.$$

Notice that the projector P biunivocally determines the observable $\mathcal{O} = 1 \cdot P + 0 \cdot (I - P)$, so that $p_A(\sigma_1 \cdots \sigma_k)$ is the probability of accepting $\sigma_1 \cdots \sigma_k$ after the evolution and the observation.

Let $\mathcal{U}^{(q)}$ be the set of $q \times q$ unitary matrices. Another equivalent way of specifying the 1qfa A is by writing $A = (\pi, \mu, P)$, where $\mu : \Sigma^* \to \mathcal{U}^{(q)}$ is the morphism defined as $\mu(\sigma_1 \cdots \sigma_k) = \prod_{i=1}^{k} U(\sigma_i)$, for $\sigma_1 \cdots \sigma_k \in \Sigma^*$. In this case, for $w \in \Sigma^*$, the event induced by A writes as $p_A(w) = \|\pi \mu(w) P\|^2$.

Given an event $p : \Sigma^* \to [0, 1]$ and a real $\lambda \in [0, 1]$, *the language* $L_{p,\lambda}$ *defined by* p *with cut point* λ is the set

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

The cut point is *isolated* if there exists a positive real δ such that $|p(w) - \lambda| \geqslant \delta$, for any $w \in \Sigma^*$. Moreover, if p is induced by the 1qfa A, then $L_{p,\lambda}$ is said to be recognized by A with cut point λ (isolated by δ), and we write $L_{A,\lambda}$. Without loss of generality, we will assume $\lambda = \frac{1}{2}$. The relevance of isolated cut point recognition on automata is due to the fact that, in this case, we can arbitrarily reduce the classification error probability of a string x by repeating a constant number of times (not depending on the length of x) its parsing and taking the majority of the answers. A well known result in [12] states that the class of languages accepted by 1qfa's with isolated cut point coincides with the class of group languages [25], a proper subclass of regular languages.

A language $L \subseteq \Sigma^*$ is said to be recognized by A in *Monte Carlo mode* (with bounded error ε) if and only if there exists $\varepsilon \in (0, \frac{1}{2})$ such that, for any $x \in \Sigma^*$, $x \in L$ implies $p_A(x) = 1$, and $x \notin L$ implies $p_A(x) \leqslant \varepsilon$.

3. 1-way quantum automata and monoids

A fundamental result in the area of stochastic automata is Rabin's theorem [26]: every language recognized by a probabilistic automaton with isolated cut point is regular. In this section we settle this result in a more abstract context, suitable for applications to quantum automata. Moreover, by a constructive variant of Rabin's method, we give an (optimal) estimation of the quantum state complexity of regular languages.

A natural metric on the linear space $\mathbf{C}^{(n)}$ is induced by the Euclidean norm. For any $A \in \mathbf{C}^{(n)}$:

$$\|A\| = \max_{\|x\|=1} \|xA\|.$$

Consider now a morphism $\mu : \Sigma^* \to \mathbf{C}^{(n)}$ and let $\mu(\Sigma^*)$ denote its image. The (metric) closure of $\mu(\Sigma^*)$ is the set $\overline{\mu(\Sigma^*)}$ consisting of $\mu(\Sigma^*)$ plus its limit points. $\mu(\Sigma^*)$ is bounded whenever $\sup_{A\in\mu(\Sigma^*)} \|A\| < \infty$; in this case, $\overline{\mu(\Sigma^*)}$ is compact. Yet, since matrix product is a continuous function, then $\overline{\mu(\Sigma^*)}$ is a compact monoid.

Example 1. The norm of every unitary matrix is 1. As a consequence, if $\mu(\Sigma)$ consists of unitary matrices, then $\overline{\mu(\Sigma^*)}$ is a compact monoid.

Example 2. Suppose A is an $n \times n$ stochastic matrix. Then, it can be easily proved that $\|A\| \leqslant \sqrt{n}$. Therefore, if $\mu(\Sigma)$ consists of stochastic matrices, then $\overline{\mu(\Sigma^*)}$ is a compact monoid.

Rabin's theorem can be stated as follows:

Theorem 1. *Let $\overline{\mu(\Sigma^*)}$ be a compact monoid. Given $L \subseteq \Sigma^*$, if*

$$\inf_{x\in L,\ y\notin L} \|\mu(x) - \mu(y)\| > 0$$

then L is regular.

Proof. Since $\overline{\mu(\Sigma^*)}$ is bounded, then we have $\|\mu(w)\| \leqslant H$, for a suitable constant H and every $w \in \Sigma^*$. Suppose that L is not regular. Hence, there is an infinite sequence $\{w_j\}$ of words in Σ^* such that, for $i \neq j$, there is a word z_{ij} satisfying $w_j z_{ij} \in L$ if and only if $w_i z_{ij} \notin L$. Then:

$$\begin{aligned} 0 &< \inf_{i\neq j} \|\mu(w_j z_{ij}) - \mu(w_i z_{ij})\| = \inf_{i\neq j} \|(\mu(w_j) - \mu(w_i))\mu(z_{ij})\| \\ &\leqslant \inf_{i\neq j} \|\mu(w_j) - \mu(w_i)\| H. \end{aligned}$$

This is impossible. In fact, $\overline{\mu(\Sigma^*)}$ being compact, it is possible to extract a subsequence $\{\mu(w_{m_j})\}$ of $\{\mu(w_j)\}$ that converges, implying

$$\inf_{i\neq j} \|\mu(w_{m_j}) - \mu(w_{m_i})\| = 0. \qquad \square$$

This result can be extensively applied to 1qfa's. In fact, it can be proved that the probabilistic events realized by several models of 1qfa's are rational power series generated by generalized real automata (π, μ, η) where $\overline{\mu(\Sigma^*)}$ is bounded [8]. It follows that the classes of languages recognized by models of 1qfa's such as measure-once, measure-many, reversible 1qfa's, 1qfa's with control language [6,8,12,20,24] are subclasses (possibly proper) of regular languages. For some of these subclasses, providing a characterization is still an open problem [3,20].

The proof of Theorem 1 is not constructive. Nevertheless, in the probabilistic context, it suggests a technique for stating a lower bound on the number of states of a stochastic automaton accepting a given regular language with isolated cut point [26]. Here, we apply such a technique for estimating the quantum descriptional complexity of a regular language L, i.e., the number of states of the smallest 1qfa recognizing it with isolated cut point (if any). More precisely, denoting by $|A|$ the number of states of the 1qfa A, we state:

Definition 1.
- $D_{\mathrm{Q}}(L, \delta) = \min\{|A| : L \text{ is recognized by the 1qfa } A \text{ with cut point isolated by } \delta\}$.
- $D_{\mathrm{Q}}(L) = \min_{\delta>0} D_{\mathrm{Q}}(L, \delta)$.

Since L is regular, it is natural to compare $D_{\mathrm{Q}}(L, \delta)$ with the classical descriptional complexity $D_{\mathrm{C}}(L)$ of L, i.e. the number of states of the minimum deterministic automaton for L. By using Rabin's technique, in [1] it is proved that $D_{\mathrm{Q}}(L, \delta) = \Omega(\log D_{\mathrm{C}}(L)/\log\log D_{\mathrm{C}}(L))$, for any given $\delta > 0$. Here, we improve this result:

Theorem 2.

$$D_{\mathrm{Q}}(L, \delta) \geqslant \frac{\log D_{\mathrm{C}}(L)}{2\log(1 + 2/\delta)}.$$

Proof. Consider a minimum d-state 1qfa $A = (\pi, \mu, (\eta_1, \ldots, \eta_d))$ recognizing L with cut point isolated by δ, so that $d = D_Q(L, \delta)$. Let $\mathcal{M} = \{\pi\mu(w) \mid w \in \Sigma^*\}$ and $\theta = \inf_{w\in L, v\notin L} \|\pi\mu(w) - \pi\mu(v)\|$. We can partition $\mathcal{M}$ according to the equivalence relation $\equiv_\theta \subseteq \mathcal{M} \times \mathcal{M}$ defined as follows: for $1 \leqslant i < k$

$$\alpha \equiv_\theta \beta \quad \Leftrightarrow \quad \text{there exist } \pi_1, \ldots, \pi_k \in \mathcal{M} \text{ with } \pi_1 = \alpha, \pi_k = \beta, \|\pi_i - \pi_{i+1}\| \leqslant \theta.$$

The equivalence classes of $\equiv_\theta$ are called θ-components. According to Rabin's construction [26], their number gives an upper bound for $D_C(L)$.

Now, let X_i be a representative of the ith θ-component, and consider the sphere of radius $\theta/2$ centered in X_i. It is clear that such a sphere is disjoint from the analogous sphere centered in X_j, for $i \neq j$. Moreover, all these spheres are contained in the sphere of radius $1 + \theta/2$ centered in $(0, \ldots, 0)$. Since the volume of a d-dimensional sphere of radius r is cr^{2d}, for a suitable constant c (depending on d), there exist at most

$$\frac{c(1+\theta/2)^{2d}}{c(\theta/2)^{2d}} = \left(1 + \frac{2}{\theta}\right)^{2d}$$

spheres, and this number is an upper bound for $D_C(L)$. To prove the thesis, it is sufficient to show that $\delta \leqslant \theta$, or equivalently that $\delta \leqslant \|\pi\mu(w) - \pi\mu(v)\|$ for all $w \in L$, $v \notin L$. To this regard, set $\pi\mu(w) = (z_1, \ldots, z_d)$ and $\pi\mu(v) = (z'_1, \ldots z'_d)$, with $w \in L$ and $v \notin L$. Then

$$\begin{aligned}
2\delta &\leqslant \sum_{\eta_i=1} |z_i|^2 - \sum_{\eta_i=1} |z'_i|^2 \\
&= \sum_{\eta_i=1} (|z_i| - |z'_i|) \cdot (|z_i| + |z'_i|) \\
&\leqslant \left(\sum_{\eta_i=1} (|z_i| - |z'_i|)^2\right)^{1/2} \left(\sum_{\eta_i=1} (|z_i| + |z'_i|)^2\right)^{1/2} \quad \text{(by Schwarz inequality)} \\
&\leqslant \left(\sum_{\eta_i=1} |z_i - z'_i|^2\right)^{1/2} \left[\left(\sum_{\eta_i=1} |z_i|^2\right)^{1/2} + \left(\sum_{\eta_i=1} |z'_i|^2\right)^{1/2}\right] \quad \text{(by triang. ineq.)} \\
&\leqslant \|\pi\mu(w) - \pi\mu(v)\|(\|\pi\mu(w)\| + \|\pi\mu(v)\|) = 2\|\pi\mu(w) - \pi\mu(v)\|. \qquad \square
\end{aligned}$$

The lower bound $\Omega(\log n)$ shown in this theorem is optimal since, in [2], the language $L_n = \{a^{kn} \mid k \in \mathbf{N}\}$ is proved to be recognizable with isolated cut point by a 1qfa with $O(\log n)$ states. Notice that deterministic, nondeterministic or probabilistic automata accepting L_n require n states (for n prime, in the probabilistic case).

4. 1-way quantum automata and compact groups

We have seen that $\overline{\mu(\Sigma^*)}$ is a compact monoid if there exists a positive constant H satisfying $\| \mu(w) \| \leqslant H$, for every $w \in \Sigma^*$. If $\mu(\sigma)$ is a unitary matrix, for every $\sigma \in \Sigma$, we can say more:

Theorem 3. *Let $\mu : \Sigma^* \to \mathcal{U}^{(n)}$ be a morphism. Then $\overline{\mu(\Sigma^*)}$ is a compact group.*

Proof. Since matrix product and the inverse are continuous functions in $\mathcal{U}^{(n)}$, it suffices to prove that $A \in \overline{\mu(\Sigma^*)}$ implies $A^{-1} \in \overline{\mu(\Sigma^*)}$. To this regard, consider the power sequence $\{A^k\}_{k\geqslant 0}$. Since $\{A^k\}_{k\geqslant 0} \subseteq \overline{\mu(\Sigma^*)}$, and since $\overline{\mu(\Sigma^*)}$ is compact, there exists a subsequence of $\{A^k\}_{k\geqslant 0}$ that converges. So, for any $\varepsilon > 0$, there are $m_\varepsilon, n_\varepsilon$ such that $\| A^{m_\varepsilon} - A^{n_\varepsilon} \| \leqslant \varepsilon$. Suppose that $m_\varepsilon > n_\varepsilon$, and set $h_\varepsilon = m_\varepsilon - n_\varepsilon - 1$. Then, we get

$$\| A^{h_\varepsilon} - A^{-1} \| = \| (A^{m_\varepsilon} - A^{n_\varepsilon})A^{-n_\varepsilon - 1} \| \leqslant \| A^{m_\varepsilon} - A^{n_\varepsilon} \| \leqslant \varepsilon.$$

This shows that $\lim_{\varepsilon\to 0} A^{h_\varepsilon} = A^{-1}$, and hence $A^{-1} \in \overline{\mu(\Sigma^*)}$. $\square$

As an important consequence of Theorem 3, we have that the compact group $\overline{\mu(\Sigma^*)}$ coincides with the zero set of a finite set $\{p_1, \ldots, p_s\}$ of real polynomials [11,17]. More precisely, let $X = \{x_{ij}, y_{ij} \mid 1 \leqslant i, j \leqslant n\}$ denote a set of real variables and let $\mathbf{R}[X]$ be the set of polynomials with variables in X and coefficients in $\mathbf{R}$. Given a polynomial $p(x_{ij}, y_{ij})$ and a matrix $M \in \mathbf{C}^{(n)}$, we say that M is a zero of p, and write $p(M) = 0$, whenever $p(\mathrm{Re}(M_{ij}), \mathrm{Im}(M_{ij})) = 0$, where Re and Im denote the real and the imaginary part of a complex number, respectively. Thus, $\overline{\mu(\Sigma^*)} = \{M \in \mathbf{C}^{(n)} \mid p_i(M) = 0, \text{ for every } 1 \leqslant i \leqslant s\}$.

A central concept is that of invariant:

Definition 2. Let $\mu : \Sigma^* \to \mathcal{U}^{(n)}$ be a morphism generating the compact group $\overline{\mu(\Sigma^*)}$. An invariant of the group is a polynomial $p \in \mathbf{R}[X]$ satisfying $p(\mu(w)X) = p(X)$, for any $w \in \Sigma^*$.

We denote by $\mathbf{R}^{\mu}[X]$ the set of invariants of $\overline{\mu(\Sigma^*)}$. Invariants can be used to define matrix membership in $\overline{\mu(\Sigma^*)}$, as given in the following [11].

Theorem 4. *Let $M \in \mathbf{C}^{(n)}$. Then $M \in \overline{\mu(\Sigma^*)}$ if and only if $p(M) = p(I)$, for every $p \in \mathbf{R}^{\mu}[X]$.*

As a consequence, it is not hard to show (see [11]) that $\overline{\mu(\Sigma^*)}$ coincides with the zero set of the polynomials contained in

$$\mathcal{I}^{\mu} = \{p \in \mathbf{R}[X] \mid p(\mu(\sigma)X) = p(X) \text{ for every } \sigma \in \Sigma, \text{ and } p(I) = 0\}.$$

This fact yields two relevant consequences:

(1) If, for every $\sigma \in \Sigma$, $\mu(\Sigma)$ is a unitary matrix with rational or algebraic entries, it is computationally easy to verify whether $p \in \mathbf{R}[X]$ belongs to $\mathcal{I}^{\mu}$.

(2) $\overline{\mu(\Sigma^*)}$ is also the zero set of the ideal $\mathcal{J}^{\mu}$ generated by $\mathcal{I}^{\mu}$. By Hilbert's basis theorem [4], $\mathcal{J}^{\mu}$ is finitely generated. i.e., there exists a finite subset $\{p_1, \ldots, p_s\} \subset \mathbf{R}[X]$ generating the ideal $\mathcal{J}^{\mu}$. As a consequence, $M \in \overline{\mu(\Sigma^*)}$ if and only if $p_1(M) = p_2(M) = \cdots = p_s(M) = 0$. So, there exists a finite set of polynomials witnessing matrix membership in $\overline{\mu(\Sigma^*)}$.

These elements, together with the decidability of the (first order) theory of real fields, have been emphasized in the area of quantum automata by Blondel et al. [11].

The first order theory $\mathcal{T}_{\mathrm{OF}}$ of ordered fields (see, e.g. [13]) is expressed by the first order language L_{OF} having 0, 1 as constants, $+, \cdot$ as binary operations, and $\leqslant$ as binary relation. $\mathcal{T}_{\mathrm{OF}}$ has all the field axioms, the linear order axioms, and the additional axioms

$$x \leqslant y \Rightarrow x + z \leqslant y + z,$$
$$x \leqslant y \wedge 0 \leqslant z \Rightarrow x \cdot z \leqslant y \cdot z.$$

Atomic formulas in L_{OF} are equalities or inequalities between polynomials with integer coefficients. The language L_{OF} is particularly expressive: the real sets definable by L_{OF}-formulas are called semi-algebraic sets. Tarski [28] showed the existence of an effective quantifier elimination procedure for the theory of real numbers in L_{OF}. Unfortunately, the worst-case complexity is double-exponential [29]. However, for formulas with a fixed number of quantifier blocks, the time complexity is single-exponential.

In [11], a nice methodology is proposed for attacking some decidability problems on 1qfa's, obtaining surprising results. For instance, they proved that it is decidable whether a 1qfa A with rational amplitudes accepts with cut point $\frac{1}{2}$ the empty set, or whether a rational λ is an isolated cut point for A. Notice that the corresponding problems for stochastic automata are undecidable [7,26].

We are now going to apply the method in the frame of classification problems using quantum finite automata.

A *k-quantum classifier*, for $k \geqslant 2$, is a system $C = \langle A_1, \ldots, A_k \rangle$, where $A_1, \ldots, A_k$ are 1qfa's on alphabet Σ such that $L_{A_i,1/2} \neq \emptyset$ and $L_{A_i,1/2} \cap L_{A_j,1/2} = \emptyset$, for $1 \leqslant i, j \leqslant k$ and $i \neq j$. The intended meaning is that all automata compete for recognizing a word, but at most one automaton is the winner.

As the reader may easily observe, for a quantum classifier, either a word $w \in \Sigma^*$ is not classified, or it is classified in that class j such that $w \in L_{A_j,1/2}$, with $1 \leqslant j \leqslant k$.

A classifier C is *complete* whenever *all* words are classified, i.e., $\bigcup_{j=1}^{k} L_{A_j,1/2} = \Sigma^*$; in this case, the family $\{L_{A_j,1/2}\}_{j=1,\ldots,k}$ is a partition of Σ^*.

Two natural problems related to quantum classifiers are the following:

k-Q.CLASSIFIER

- INSTANCE: 1qfa's $A_1, \ldots, A_k$ on alphabet Σ.
- QUESTION: Is $\langle A_1, \ldots, A_k\rangle$ a k-quantum classifier?

COMPLETE k-Q.CLASSIFIER

- INSTANCE: 1qfa's $A_1, \ldots, A_k$ on alphabet Σ.
- QUESTION: Is $\langle A_1, \ldots, A_k\rangle$ a complete k-quantum classifier, i.e., is $L_{A_1,1/2}, \ldots, L_{A_k,1/2}$ a partition of Σ^*?

First of all, we prove

Theorem 5. *For any $k \geqslant 2$, k-Q.CLASSIFIER is decidable.*

Proof. By [11], we have that testing whether a 1qfa recognizes a nonempty set with cut point $1/2$ is decidable. Hence, it is sufficient to prove that, given two 1qfa's $A_1 = (\pi_1, \mu_1, P_1)$ and $A_2 = (\pi_2, \mu_2, P_2)$, it is decidable to test whether $L_{A_1,1/2} \cap L_{A_2,1/2} = \emptyset$. To this purpose, we observe that the set $\{(A_1, A_2) \mid L_{A_1,1/2} \cap L_{A_2,1/2} \neq \emptyset\}$ is exactly the set

$$\{(A_1, A_2) | \exists w \in \Sigma^* (\parallel \pi_1 \mu_1(w) P_1 \parallel^2 > \tfrac{1}{2} \wedge \parallel \pi_2 \mu_2(w) P_2 \parallel^2 > \tfrac{1}{2})\}.$$

This set is defined by an existential quantification on a recursive test (i.e., $\parallel \pi_1 \mu_1(w) P_1 \parallel^2 > \frac{1}{2} \wedge \parallel \pi_2 \mu_2(w) P_2 \parallel^2 > \frac{1}{2}$), and hence is semi-decidable. Then, to show the decidability of $\{(A_1, A_2) \mid L_{A_1,1/2} \cap L_{A_2,1/2} = \emptyset\}$, it is enough to prove its semi-decidability.

Without loss of generality, we can assume that A_1 and A_2 have the same induced morphism. To this regard, let us quickly introduce some notations. For matrices $A \in \mathbf{C}^{(n)}$ and $B \in \mathbf{C}^{(m)}$ and for vectors $\pi \in \mathbf{C}^{1\times n}$ and $\eta \in \mathbf{C}^{1\times m}$, their direct sum is, respectively

$$A \oplus B = \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix}, \quad \pi \oplus \eta = (\pi_1, \ldots, \pi_n, \eta_1, \ldots, \eta_m).$$

Now, consider the 1qfa's $A_1 = (\pi_1, \mu_1, P_1)$ and $A_2 = (\pi_2, \mu_2, P_2)$. We can set $\mu = \mu_1 \oplus \mu_2$, and define the automata $B_1 = (\pi_1 \oplus (0, \ldots, 0), \mu, P_1 \oplus \mathbf{0})$ and $B_2 = ((0, \ldots, 0) \oplus \pi_2, \mu, \mathbf{0} \oplus P_2)$. It is easy to verify that $L_{A_1,1/2} = L_{B_1,1/2}$ and $L_{A_2,1/2} = L_{B_2,1/2}$.

Let now $\{p_k \mid k \in \mathbf{N}\}$ be a computable total ordering on polynomials with rational (or algebraic) coefficients. Given a morphism μ with $\mu(\sigma)$ unitary matrix with rational entries, for every, $\sigma \in \Sigma$, we know that $\overline{\mu(\Sigma^*)}$ is exactly the zero set of

$$\mathcal{I}^{\mu} = \left\{ p_k \,\middle|\, \bigwedge_{\sigma\in\Sigma} p_k(\mu(\sigma)X) = p_k(X), \text{ and } p(I) = 0 \right\}.$$

It is easy to see that $\mathcal{I}^{\mu}$ is recursive. Now, take the ideal generated by $\mathcal{I}^{\mu}$:

$$\mathcal{J}^{\mu} = \left\{ p_s \,\middle|\, \exists m \exists j_1, \ldots, j_m, k_1, \ldots, k_m \left(p_s = \sum_{i=1}^{m} p_{j_i} p_{k_i}, \text{ with } p_{j_1}, \ldots, p_{j_m} \in \mathcal{I}^{\mu} \right) \right\}.$$

This ideal is defined via an existential quantification on a recursive predicate, and this gives that $\mathcal{J}^{\mu}$ is recursively enumerable. Thus, there exists a total recursive enumerating function $t_{\mu} : \mathbf{N} \to \mathbf{N}$ such that $\mathcal{J}^{\mu} = \{p_{t_{\mu}(n)} \mid n \in \mathbf{N}\}$.

Consider the following procedure:

INPUT: $A_1 = (\pi_1, \mu, P_1)$, $A_2 = (\pi_2, \mu, P_2)$

```
F := 0; k := 0; Ψ := ∅;
while F = 0 do
 begin
   Ψ := Ψ ∪ {p_{t_μ(k)}};
   if ∀X ( ⋀_{p∈Ψ} p(X) = 0 ⇒ ‖ π1 X P1 ‖^2 ⩽ 1/2 ∨ ‖ π2 X P2 ‖^2 ⩽ 1/2 ) then
```

```
      F := 1;
    k := k + 1;
  end
output(F)
```

We note that the test $\forall X \left(\bigwedge_{p\in\Psi} p(X) = 0 \Rightarrow \| \pi_1 X P_1 \|^2 \leqslant \frac{1}{2} \vee \| \pi_2 X P_2 \|^2 \leqslant \frac{1}{2} \right)$ in the if-statement is a formula in the language L_{OF}, and hence decidable (e.g., by Tarski's quantifier elimination method). Let us now examine the behavior of the procedure:

- Suppose $L_{A_1,1/2} \cap L_{A_2,1/2} \neq \emptyset$. In this case, there exists a matrix $M \in \mu(\Sigma^*)$ satisfying $\| \pi_1 X P_1 \|^2 > \frac{1}{2} \wedge \| \pi_2 X P_2 \|^2 > \frac{1}{2}$. Moreover, M satisfies $\bigwedge_{p\in\mathcal{I}^\mu} p(M) = 0$ as well. Hence, the test in the if-statement is never passed and the procedure loops.
- Suppose $L_{A_1,1/2} \cap L_{A_2,1/2} = \emptyset$. By Hilbert's basis theorem [4], $\mathcal{J}^\mu$ is finitely generated, say, by the polynomials $\Phi = \{p_{t_\mu(k_1)}, \ldots, p_{t_\mu(k_s)}\}$. Let $K = \max\{k_1, \ldots, k_s\}$. After K iterations of the while-loop, Ψ will clearly contain Φ. Hence, the test in the if-statement will be passed, and the procedure will halt returning 1.

In conclusion, we have designed a procedure that halts on the elements of the set $\{(A_1, A_2) \mid L_{A_1,1/2} \cap L_{A_2,1/2} = \emptyset\}$, and loops otherwise. This shows the semi-decidability to testing whether $L_{A_1,1/2} \cap L_{A_2,1/2} = \emptyset$, and concludes the proof. □

On the contrary, we show that

Theorem 6. *For any $k \geqslant 2$,* COMPLETE k-Q.CLASSIFIER *is undecidable.*

Proof. We first need to show the undecidability of the following simple problem. Let $E = \{w \in \Sigma^* \mid |w| \bmod 2 = 0\}$ be the set of even length strings. We call EVEN the problem of deciding, given a 1qfa A on the alphabet Σ, whether $L_{A,1/2} = E$. By [11], we know that testing whether $L_{A,1/2} = \Sigma^*$ is undecidable. We reduce this latter problem to EVEN, thus yielding the undecidability of EVEN as well.

Given the q-state 1qfa $A = (\pi, \{U(\sigma)\}_{\sigma\in\Sigma}, P)$, let us construct the $2q$-state 1qfa $\hat{A} = (\hat{\pi}, \{\hat{U}(\sigma)\}_{\sigma\in\Sigma}, \hat{P})$, where $\hat{\pi}$ is the $1 \times 2q$ vector $(\pi, 0, \ldots, 0)$, for any $\sigma \in \Sigma$, $\hat{U}(\sigma)$ is the $2q \times 2q$ unitary matrix $\begin{pmatrix} \mathbf{0} & U(\sigma) \\ I & \mathbf{0} \end{pmatrix}$, and $\hat{P}$ is the $2q \times 2q$ matrix $\begin{pmatrix} P & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$. It is easy to verify that $p_{\hat{A}}(\varepsilon) = p_A(\varepsilon)$ and, for any $\sigma_1 \cdots \sigma_n \in \Sigma^+$:

$$p_{\hat{A}}(\sigma_1 \cdots \sigma_n) = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ p_A(\sigma_1\sigma_3 \cdots \sigma_{n-1}) & \text{if } n \text{ is even.} \end{cases}$$

Hence, given $\sigma_1 \cdots \sigma_n \in \Sigma^+$, for any $w \in \sigma_1\Sigma\sigma_2\Sigma \cdots \sigma_n\Sigma$ we get $p_{\hat{A}}(w) = p_A(\sigma_1 \cdots \sigma_n)$. Since $E = \{\varepsilon\} \cup \bigcup_{\sigma_1\cdots\sigma_n\in\Sigma^+} \sigma_1\Sigma\sigma_2\Sigma \cdots \sigma_n\Sigma$, we conclude that $L_{A,1/2} = \Sigma^*$ if and only if $L_{\hat{A},1/2} = E$. Therefore, if the problem EVEN were decidable then we would be able to decide whether $L_{A,1/2} = \Sigma^*$, which is a contradiction.

We are now ready to show the undecidability of COMPLETE k-Q.CLASSIFIER by reducing EVEN to it. Fixed k, i, with $0 \leqslant i \leqslant k-2$, let us define the language $L_{k,i} = \{w \in \Sigma^* \mid |w| \bmod 2(k-1) = 2i+1\}$. This is a group language, and hence it is recognized by a quantum (actually deterministic) automaton $A_i^{(k)}$. Moreover, it is easy to see that $\{L_{A_i^{(k)},1/2}\}_{i=0,\ldots,k-2}$ partitions the set of odd length strings of Σ^*.

For reducing EVEN to COMPLETE k-Q.CLASSIFIER, with every 1qfa A on alphabet Σ we associate the k-tuple $(A, A_0^{(k)}, A_1^{(k)}, \ldots, A_{k-2}^{(k)})$. In fact, $L_{A,1/2} = E$ if and only if $L_{A,1/2} \cup L_{A_0^{(k)},1/2} \cup \cdots \cup L_{A_{k-2}^{(k)},1/2} = \Sigma^*$. This reasoning shows that testing whether $(A, A_0^{(k)}, A_1^{(k)}, \ldots, A_{k-2}^{(k)})$ is a complete k-quantum classifier can be used to decide whether $L_{A,1/2} = E$, which is undecidable. □

5. Quantum descriptional complexity: the unary case

In this section, we study the quantum descriptional complexity $D_{\mathrm{Q}}(L)$ (see Definition 1, Section 3) in case L is a unary regular language. In this context, we prove that the quantum descriptional complexity is computable in exponential time.

A language L is unary if $L \subseteq \{a\}^*$. Every language L accepted with isolated cut point by a 1qfa can be recognized by a deterministic automaton whose next state function is a permutation for every symbol [6,12]. It follows that the class of unary languages recognized with isolated cut point by 1qfa's is the class of periodic languages, where a language $L \subseteq \{a\}^*$ is called n-periodic if and only if $a^k \in L \Leftrightarrow a^{k+n} \in L$, for all $k \geqslant 0$.

The minimum period of L coincides with its classical descriptional complexity $D_{\mathrm{C}}(L)$. So, we can use a result in [23] to give an upper bound for its quantum descriptional complexity in term of its classical descriptional complexity:

Theorem 7. $D_{\mathrm{Q}}(L) \leqslant 2\sqrt{6D_{\mathrm{C}}(L)} + 26$.

Hence, for a unary regular language L, we have the following situation: if L is not periodic, then it cannot be recognized with isolated cut point by 1qfa's (i.e., $D_{\mathrm{Q}}(L) = \infty$), while if L is periodic, quantum computing helps ($D_{\mathrm{Q}}(L) = \mathrm{O}(\sqrt{D_{\mathrm{C}}(L)})$. Observe that the bound of Theorem 7 is almost tight infinitely often; in fact, in [9] a lower bound $D_{\mathrm{Q}}(L) = \Omega(\sqrt{D_{\mathrm{C}}(L)/\log D_{\mathrm{C}}(L)})$ is proved for infinitely many periodic languages.

We are now going to show that the quantum descriptional complexity $D_{\mathrm{Q}}(L)$ is a computable function; unfortunately, the time complexity of the algorithm is exponential.

Theorem 8. *For unary periodic languages L, the quantum descriptional complexity $D_{\mathrm{Q}}(L)$ is computable in time $T(D_{\mathrm{C}}^2(L))$, where T is the time for proving existential formulas in L_{OF}.*

Proof. Consider a n-periodic language L represented by a vector $v_L \in \{0,1\}^n$, where $v_L(k) = 1 \Leftrightarrow a^{k \bmod n} \in L$, and a 1qfa (π, U, P) recognizing L with isolated cut point. Because of periodicity, we can restrict ourselves to consider unitary evolution matrices U with eigenvalues of the form $\mathrm{e}^{\mathrm{i}(2\pi/n)k}$, with integer k.

Fixed an integer F, to specify a 1qfa with F states, consider the following set of complex variables (as usual, a complex variable should be interpreted as a pair of real variables, see Section 4):

(i) $x = \{x_i \mid 1 \leqslant i \leqslant F\}$ denoting the amplitudes of the initial superposition;
(ii) $X = \{X_{i,j} \mid 1 \leqslant i, j \leqslant F\}$ denoting the unitary matrix;
(iii) $Y = \{Y_{i,j} \mid 1 \leqslant i, j \leqslant F\}$ denoting the projector (measure operator).

1qfa's with F states and eigenvalues of U of the form $\mathrm{e}^{\mathrm{i}(2\pi/n)k}$ are exactly the zero set of the following set of polynomials:

$$\mathcal{P}_F = \{\| x \|^2 = 1, XX^\dagger = I, X^n = I, Y = Y^\dagger, Y^2 = Y\}.$$

Thus, we observe that the n-periodic language L, specified by $v_L \in \{0,1\}^n$, it is recognized with isolated cut point by an F-state 1qfa if and only if the following sentence $\Psi_{F,L}$ holds in L_{OF}:

$$\Psi_{F,L} \equiv \exists x, X, Y, \lambda \left(\bigwedge_{p \in \mathcal{P}_F} p \wedge \bigwedge_{k \in \{1,\ldots,n\}} (-1)^{v_L(k)} \| xX^kY \|^2 < (-1)^{v_L(k)} \lambda \right).$$

With minor modifications, $\Psi_{F,L}$ can be easily transformed into an equivalent sentence $\hat{\Psi}_{F,L}$ of length $\mathrm{O}(nF^2)$. Then, the function $D_{\mathrm{Q}}(L)$ can be computed by the following algorithm:

INPUT: $v_L \in \{0,1\}^n$
  $F := 1$;
  `while (`$\hat{\Psi}_{F,L}$ `is false) do` $F := F + 1$;
  `output(`F`)`

If $T(g)$ is the time required to prove existential sentences of length g in L_{OF}, we conclude that the computational complexity of the previous algorithm is $T(nD_{\mathrm{Q}}^2(L))$. By Theorem 7, we know that $D_{\mathrm{Q}}(L) = \mathrm{O}(\sqrt{n})$, obtaining the bound $T(\mathrm{O}(D_{\mathrm{C}}^2(L)))$. Since exponential algorithms for deciding existential formulas in L_{OF} are known [29], D_{Q} can be computed in exponential time. □

5.1. About the family $\{L_n\}_{n>0}$

We now present a method that, in some cases, allows to exhibit 1qfa's exponentially more succinct then their classical counterpart. In particular, we show the existence of a Monte Carlo 1qfa recognizing the language $L_n = \{a^{kn} \mid k \in \mathbf{N}\}$ with bounded error ε and $O((1/\varepsilon^3)\log n)$ states.

Consider a class $\mathcal{B} = \{\varphi_\alpha : \{a\}^* \to [0,1] \mid \alpha \in I\}$ of n-periodic events induced by M-state 1qfa's $(\pi_\alpha, U_\alpha(\sigma), P_\alpha)$ $(\alpha \in I)$ and call $\hat{\mathcal{B}}$ its convex closure. Every $\xi \in \hat{\mathcal{B}}$ is a convex linear combination $\xi = \sum_{\alpha\in I} b_\alpha \varphi_\alpha$, with $b_\alpha \geqslant 0$ and $\sum_\alpha b_\alpha = 1$. We can interpret $b = \{b_\alpha \mid \alpha \in I\}$ as a probability distribution on I; fixed $k \in \mathbf{N}$, $\varphi_\alpha(a^k)$ is a random variable on (I, b), whose expectation is $\sum_{\alpha\in I} b_\alpha \varphi_\alpha(a^k) = \xi(a^k)$. We can approximate the expectation $\xi(a^k)$ by an empirical average, by means of the following algorithm:

INPUT: `an integer` S `(number of samples)`
  `for` $t := 1$ `to` S `do`
    $\alpha[t] :=$ `α independently chosen in` I `with probability` b_α;
  `output the 1qfa` A `defined as`

$$A = \left(\oplus_{\alpha[t]}\sqrt{1/S}\pi_{\alpha[t]}, \oplus_{\alpha[t]} U_{\alpha[t]}(\sigma), \oplus_{\alpha[t]} P_{\alpha[t]}\right).$$

This 1qfa has SM states and realizes the empirical average

$$\psi_S(a^k) = \frac{1}{S}\sum_{t=1}^{S} \varphi_{\alpha[t]}(a^k),$$

for every $k \in \mathbf{N}$. To study how ψ_S approximates ξ, we need to recall Höffding's Inequality [22]: Let X_i's be i.i.d. random variables with values in [0, 1] and expectation μ. Then, for all S

$$\text{Prob}\left\{\left|\frac{1}{S}\sum_{i=1}^{S} X_i - \mu\right| \geqslant \delta\right\} \leqslant 2e^{-2\delta^2 S}. \tag{1}$$

Going back to our problem, since ψ_S and ξ are n-periodic events, we have:

$$\begin{aligned}\text{Prob}\left\{\sup_{k\in\mathbf{N}} |\psi_S(a^k) - \xi(a^k)| \geqslant \delta\right\} &= \text{Prob}\left\{\max_{0\leqslant k<n} |\psi_S(a^k) - \xi(a^k)| \geqslant \delta\right\} \\ &\leqslant n \cdot \max_{0\leqslant k<n} \text{Prob}\{|\psi_S(a^k) - \xi(a^k)| \geqslant \delta\} \quad \text{(by union bound)} \\ &\leqslant n \cdot 2e^{-2\delta^2 S} \quad \text{(by Höffding's Inequality (1))}.\end{aligned}$$

By requiring $n \cdot 2e^{-2\delta^2 S} < 1$, we obtain [10]:

Theorem 9. *Given a family $\mathcal{B}$ of n-periodic events induced by M-state 1qfa's, for any event ξ in the convex closure of $\mathcal{B}$ there is a 1qfa with $O((M/\delta^2)\log n)$ states inducing an event ψ, such that $\sup_{w\in\{a\}^*} |\psi(w) - \xi(w)| \leqslant \delta$.*

We specialize this result for the following family of n-periodic events:

$$\Psi_S = \left\{\varphi_{\alpha_1,\ldots,\alpha_s}(a^k) = \prod_{j=1}^{s} \cos^2\left(\frac{\pi\alpha_j k}{n}\right) \,\middle|\, \alpha_j \text{ integer}, \quad 0 \leqslant \alpha_j < n\right\}.$$

Any event in Ψ_S is induced by the 2^s-state 1qfa $A_{\alpha_1,\ldots,\alpha_s}$ obtained by Kronecker's product of the 2-state 1qfa's inducing events of type $\cos^2(\pi\alpha k/n)$ [8]. Let now consider the following convex linear combination of the events in Ψ_S:

$$\xi(a^k) = \frac{1}{n^s}\sum_{0\leqslant\alpha_1,\ldots,\alpha_s<n} \varphi_{\alpha_1,\ldots,\alpha_s}(a^k) = \left(\frac{1}{n}\sum_{\alpha=0}^{n-1} \cos^2\left(\frac{\pi\alpha k}{n}\right)\right)^s.$$

Then, we get

$$\xi(a^k) = \begin{cases} 1 & \text{for } k \bmod n = 0, \\ \dfrac{1}{2^s} & \text{otherwise.} \end{cases}$$

The event

$$\psi(a^k) \begin{cases} = 1 & \text{for } k \bmod n = 0, \\ \leqslant \dfrac{2}{2^s} & \text{otherwise.} \end{cases}$$

satisfies $\sup_{w\in\{a\}^*} |\psi(w) - \xi(w)| \leqslant 1/2^s$. Hence, by letting $\varepsilon = 1/2^{s-1}$ and by Theorem 9, ψ can be induced by a 1qfa with $O((1/\varepsilon^3)\log n)$ states.

Let us now apply such results to language recognition. Consider the unary language

$$L_n = \{a^{kn} \mid k \in \mathbf{N}\}.$$

In [2], the authors exhibit a Monte Carlo 1qfa accepting L_n, for prime n, with $O(\log n)$ states. Actually, a careful inspection of their construction algorithm reveals that their state upper bound exponentially depends on $1/\varepsilon$. Here, we improve this result as follows:

Theorem 10. *For any $n > 1$, there exists a 1qfa accepting L_n in Monte Carlo mode with bounded error ε and $O((1/\varepsilon^3)\log n)$ states.*

Proof. We can build a 1qfa with $O((1/\varepsilon^3)\log n)$ states inducing the n-periodic event

$$\psi(a^k) \begin{cases} = 1 & \text{for } k \bmod n = 0, \\ \leqslant \varepsilon & \text{otherwise.} \end{cases}$$

This clearly gives a Monte Carlo acceptance of L_n. □

References

[1] F.M. Ablayev, A. Gainutdinova, On the lower bounds for one-way quantum automata, in: Proc. 25th MFCS, Lecture Notes in Computer Science, Vol. 1893, 2000, pp. 132–140.

[2] A. Ambainis, R. Freivalds, 1-way quantum finite automata: strengths, weaknesses and generalizations, in: Proc. 39th FOCS, 1998, pp. 332–342.

[3] A. Ambainis, A. Kikusts, M. Valdats, On the class of languages recognizable by 1-way quantum finite automata, in: Proc. 18th STACS, Lecture Notes in Computer Science, Vol. 2010, 2001, pp. 305–316.

[4] T. Becker, V. Weispfenning, H. Kredel, Gröbner Bases, A Computational Approach to Commutative Algebra, Springer, Berlin, 1993.

[5] E. Bernstein, U. Vazirani, Quantum complexity theory, SIAM J. Comput. 26 (1997) 1411–1473.

[6] A. Bertoni, M. Carpentieri, Regular languages accepted by quantum automata, Inform. and Comput. 165 (2001) 174–182.

[7] A. Bertoni, G. Mauri, M. Torelli, Some recursive unsolvable problems relating to isolated cutpoints in probabilistic automata, in: Proc. Fourth ICALP, Lecture Notes in Computer Science, Vol. 52, 1977, pp. 87–94.

[8] A. Bertoni, C. Mereghetti, B. Palano, Quantum computing: 1-way quantum automata, in: Proc. Seventh DLT, Lecture Notes in Computer Science, Vol. 2710, 2003, pp. 1–20.

[9] A. Bertoni, C. Mereghetti, B. Palano, Lower bounds on the size of quantum automata accepting unary languages, in: Proc. Eighth Italian Conf. Theoretical Computer Science, Lecture Notes in Computer Science, Vol. 2841, 2003, pp. 86–95.

[10] A. Bertoni, C. Mereghetti, B. Palano, Small size quantum automata recognizing some regular languages, Theoret. Comput. Sci. 340 (2005) 394–407.

[11] V.D. Blondel, E. Jeandel, P. Koiran, N. Portier, Decidable and undecidable problems about quantum automata, Technical Report RR2003–24, LIP, ENS Lyon, 2003.

[12] A. Brodsky, N. Pippenger, Characterizations of 1-way quantum finite automata, SIAM J. Comput 31 (2001) 1456–1478.

[13] C. Chang, H. Keisler, Model Theory, North-Holland, Amsterdam, 1973.

[14] C. Choffrut, A short introduction to automatic group theory, Semigroups, algorithms, automata and languages, World Scientific, Singapore, 2002 pp. 133–154.

[15] C. Choffrut, K. Culik II, Properties of finite and pushdown transducers, SIAM J. Comput. 12 (1983) 300–315.

[16] C. Choffrut, J. Karhumäki, Some decision problems on integer matrices, Theoret. Informatics Appl. 39 (2005) 125–131.

[17] H. Derksen, E. Jeandel, P. Koiran, Quantum automata and algebraic groups, J. Symb. Comput. 39 (2005) 357–371.
[18] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, in: Proc. Roy. Soc. London Ser. A 400 (1985) 97–117.
[19] R. Feynman, Simulating physics with computers, Internat. J. Theoret. Phys. 21 (1982) 467–488.
[20] M. Golovkins, M. Kravtsev, Probabilistic reversible automata and quantum automata, in: Proc. Eighth ICCC, Lecture Notes in Computer Science, Vol. 2387, 2002, pp. 574–583.
[21] L. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th STOC, 1996, pp. 212–219.
[22] W. Höffding, Probability inequalities for sums of bounded random variables, J. Amer. Statist. Assoc. 58 (1963) 13–30.
[23] C. Mereghetti, B. Palano, On the size of one-way quantum finite automata with periodic behaviors, Theoret. Inf. Appl. 36 (2002) 277–291.
[24] C. Moore, J. Crutchfield, Quantum automata and quantum grammars, Theoret. Comput. Sci. 237 (2000) 275–306.
[25] J.E. Pin, On languages accepted by finite reversible automata, in: Proc. 14th ICALP, Lecture Notes in Computer Science, Vol. 267, 1987, pp. 237–249.
[26] M. Rabin, Probabilistic automata, Inform. and Control 6 (1963) 230–245.
[27] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997) 1484–1509.
[28] A. Tarski, A decision method for elementary algebra and geometry, University of California, Technical Report, 1948.
[29] V. Weispfenning, The complexity of linear problems in fields, J. Symbolic Comput 5 (1988) 3–27.