ELSEVIER

Theoretical Computer Science 262 (2001) 69–81

Theoretical Computer Science

www.elsevier.com/locate/tcs

Analogies and differences between quantum and stochastic automata

Alberto Bertoni[a,*], Marco Carpentieri[a]

[a] *Dipartimento di Scienze dell'Informazione, Università di Milano, Via Comelico 39, 20135 Milano (MI), Italy*

Received 10 February 1999; revised 29 February 2000

Abstract

We analyze some features of the behaviour of quantum automata, providing analogies and differences with the corresponding stochastic models. In particular, we prove:

- there is a quantum automaton where the change of state depends on unitary transformations defined by matrices with nonnull amplitudes that accepts a non regular language with cut point zero and inverse error polynomially bounded,
- stochastic automata with matrices having nonnull elements and with polynomial bounds on the inverse error recognize only regular languages,
- the class of stochastic languages contains the class of quantum languages,
- quantum languages are empty or contain an infinite number of words,
- the class of quantum languages is not closed under complementation.

Keywords: Automata; Formal power series; Quantum computing

1. Introductions

Even if the present technology does consent to realize only very simple devices based on the principles of quantum mechanics, many authors considered it to be worth asking whether a theoretical model of quantum computation could offer any substantial benefits over the correspondent theoretical model based on the assumptions of classical physics. Recently, this question has received considerable attention because of the growing belief that quantum mechanical processes might be able to perform computation that traditional computing machines can only perform inefficiently. For

* Corresponding author.
E-mail address: bertoni@dsi.unimi.it (A. Bertoni).

0304-3975/01/$ - see front matter © 2001 Published by Elsevier Science B.V.
PII: S0304-3975(00)00154-7

an extensive bibliography and illustration of the main results in the area the reader is referred to [4, 6, 16, 18, 33, 34, 37].

In 1982 Benioff [2] first considered that devices computing according to the principles of quantum mechanics could be at least as powerful as classical computers. The question whether the computational power of quantum mechanical processes might be beyond that of traditional computation models was raised by Feynmann [19] who gave arguments as to why quantum mechanics might be computationally expensive to simulate on a classical computer. In 1985 Deutsch [13], re-examined the Church Turing Principle, on which the current computational complexity theory is founded, and he proposed a precise model of a quantum physical computer, so, defining *quantum Turing machines.* Then, Deutsch [14] defined quantum networks and investigated some of their properties. Bernstein and Vazirani [6] gave the foundations of the quantum theory of computational complexity and described an efficient universal quantum computer that simulates a large class of Quantum Turing Machines. Yao [37] introduced the quantum complexity theory in terms of quantum networks and showed the existence of an efficient quantum simulator for each Quantum Turing Machine.

Several authors offered evidence that the quantum model of computation may have significantly more complexity theoretic power than the traditional Turing Machines [6–8, 15, 19, 20, 33, 34]. Berthiaume and Brassard [7, 8] and Deutsch and Jozsa [15] introduced problems that quantum computers can quickly solve exactly, while classical ones can only solve quickly with a bounded probability of error. Bernstein and Vazirani [6], proposed an oracle problem that can be solved in polynomial time by quantum computation, but requires super-polynomial time on a classical machine. This result was improved by Simon [34], who gave a simpler construction of an oracle problem that takes polynomial time by quantum computation, but exponential time on a classical computer. Simon's algorithm inspired the work of Shor [33] that presented quantum polynomial time algorithms for the discrete logarithm and integer factoring problems that, as it is well known, are unlikely to be solvable in polynomial time by classical computation. Indeed, the integer factoring is so widely believed to be hard that the *RSA* public cryptosystem [30] is based on the assumption of its hardness.

Although some suggestions have been made to design quantum computers [36, 25, 26, 11, 17, 35, 10], there are substantial difficulties in building any of these because of the destabilizing effects of the environmental interaction that is a major experimental (and theoretical) obstacle. Such difficulties become very serious as the computation time and the size of the computer grow so that it is conceivable to build only small or very simple quantum machines.

The problems of the destabilizing effects of interaction with an environment suggest the study of quantum devices, simpler than quantum machines, such as those corresponding to classical automata, that can be experimentally useful to understand better and possibly control quantum phenomena. A finite control state Quantum Automaton (QA) can be viewed as a particular quantum Turing machine, where the head moves

only to the right reading and writing the same symbol. The states of a QA with m control states $\{1,\ldots,m\}$ can be described as unit length m-dimensional complex vectors whose kth component represents the *amplitude* of the control state k $(1 \leqslant k \leqslant m)$. We recall that an observation of the state $\upsilon = (v_1,\ldots,v_m) \in \mathbf{C}^m$ produces the control state k with probability $|v_k|^2$. The possible input messages are words over a finite alphabet Σ; the input symbol $\sigma \in \Sigma$ causes a change of state according to a unitary transformation $M(\sigma) : \mathbf{C}^m \to \mathbf{C}^m$ such that $M(\sigma)(\upsilon) = \upsilon M(\sigma)$. Fixed an initial state α, a word $\sigma_1 \ldots \sigma_n \in \Sigma^*$ determines a new state $\upsilon' = \alpha M(\sigma_1)\ldots M(\sigma_n)$. The probabilistic event realized by QA is defined by the probability $P_{\mathrm{QA}}(\sigma_1 \ldots \sigma_n)$ that the control state observed from υ' belongs to a preassigned set F of final control states. Given a cut point $\lambda \in [0,1)$, the behaviour of the quantum automaton QA can be defined by the language $L_{\mathrm{QA},\lambda}$ containing the input words $\sigma_1 \ldots \sigma_n$ for which $p(\sigma_1 \ldots \sigma_n) > \lambda$. An important notion associated to the automaton QA with cut point λ is the error function $\varepsilon_{\mathrm{QA},\lambda} : \mathbf{N} \to [0,1]$, that represents the minimum absolute value of the difference between the probability of a word of length at most n and the cut point λ. The inverse error $\varepsilon^{-1}_{\mathrm{QA},\lambda}(n)$, for $\varepsilon_{\mathrm{QA},\lambda}(n) \neq 0$, is an estimation of the number of repetitions of an experiment to decide the correct membership to $L_{\mathrm{QA},\lambda}$ of a word of length at most n with high confidence. If there is $\varepsilon > 0$ for which $\varepsilon_{\mathrm{QA},\lambda}(n) \geqslant \varepsilon$, we say that the cut point λ is isolated. The notion of quantum automaton has strong analogies with that of stochastic automaton. Nevertheless, in this paper we emphasize some differences between the behaviours of the two computational models. Roughly speaking, the use of amplitudes, instead of probabilities, increases the computational power of the quantum automata with respect to the stochastic automata. Conversely, the reversibility constraints limit the computational capabilities of the quantum automata. To be more precise, we show that stochastic automata with matrices having nonnull elements and with polynomial bounds on the inverse error recognize only regular languages. On the other hand, we exhibit a quantum automaton, where the change of state depends on unitary transformations defined by matrices with nonnull amplitudes and that recognizes a non regular language with cut point 0 and inverse error polynomially bounded. Notice that it is well known that stochastic automata accept with cut point 0 only regular languages. We prove that the class of stochastic languages, that is, those accepted by stochastic automata with cut point, contains the class of quantum languages (accepted by quantum automata with cut point). A property to check whether a language is not accepted by a quantum automaton is given. Then, the property is used to prove that quantum languages are empty or contain infinite words and that the class of quantum languages is not closed under complementation.

2. Preliminaries

In this section we review the basic concepts used in the rest of the paper. To a more exhaustive illustration of the topics presented here the reader is referred to [9, 12, 21, 23, 24, 27, 31].

2.1. Formal power series

Let $\langle \Sigma^*, \cdot, \mathbf{1} \rangle$ be the free monoid generated by a finite alphabet Σ consisting of the words over Σ along with concatenation product $\cdot$ and the empty word $\mathbf{1}$. Given a field $\mathbf{K}$, the class $\mathbf{K}\langle\langle \Sigma \rangle\rangle$ of formal power series in non commuting variables in Σ and coefficients in $\mathbf{K}$ is the set of functions of the type $s : \Sigma^* \to \mathbf{K}$. Typically, the value $s(w)$ of the function s on $w \in \Sigma^*$ is denoted by (s, w) and referred as the coefficient of the series. The power series is written as a formal sum

$$s = \sum_{w \in \Sigma^*} (s, w)w.$$

The usual operations defined on two power series $s : \Sigma^* \to \mathbf{K}$ and $t : \Sigma^* \to \mathbf{K}$ are the sum

$$\sum_{w \in \Sigma^*} (s + t, w)w = \sum_{w \in \Sigma^*} [(s, w) + (t, w)]w$$

and the Cauchy product

$$\sum_{w \in \Sigma^*} (st, w) = \sum_{w = uv} (s, u)(t, v)w.$$

Moreover, the Hadamard product $s \circ t$ of s and t is the function $s \circ t : \Sigma^* \to \mathbf{R}$ defined by $s \circ t(w) = s(w)t(w)$. The support of s is the language $supp(s) = \{w \in \Sigma^* : (s, w) \neq 0\}$. A polynomial is a series of finite support. The family $\mathbf{K}^{\mathrm{Rat}}\langle\langle \Sigma \rangle\rangle$ of $\mathbf{K}-$ rational power series over Σ is the smallest subdomain of $\mathbf{K}\langle\langle \Sigma \rangle\rangle$ containing the polynomials and closed under the operations of sum, Cauchy product and star, where star of a power series s, such that $(s, \mathbf{1}) = 0$, is defined by

$$s^* = \sum_{n \geqslant 0} s^n.$$

It is well known that the class of rational power series is closed under the operation of Hadamard product. A linear representation of a power series s is a triple $\langle \mathbf{p}, \{A(\sigma) : \sigma \in \Sigma\}, \eta \rangle$ with $\mathbf{p} \in \mathbf{K}^{1 \times m}$, $A(\sigma) \in \mathbf{K}^{m \times m}$ for each $\sigma \in \Sigma$, $\eta \in \mathbf{K}^{m \times 1}$ and such that for $w = \sigma_1 \ldots \sigma_k \in \Sigma^*$ it results

$$(s, w) = \mathbf{p} \prod_{j=1}^{k} A(\sigma_j)\eta.$$

The following result [32, 9, 31] characterizes the rational power series, extending Kleene's Theorem [23] to the power series.

Theorem 1 (Scutzenberger [32]). *A power series is rational if and only if it has a linear representation of finite dimension.*

2.2. Stochastic automata

Let $\langle \Sigma^*, \cdot, \mathbf{1} \rangle$ be the free monoid generated by a finite alphabet Σ consisting of the words over Σ along with concatenation product and the empty word $\mathbf{1}$. We denote the

length of the word $w \in \Sigma^*$ by $|w|$, while by $\Sigma^{\leqslant n}$ we mean the set of the words in Σ^* of length at most n.

Definition 1. A Stochastic Automaton SA over Σ and with m control states is a system

$$\mathrm{SA} = \langle \mathbf{p}, \{A(\sigma), \sigma \in \Sigma\}, F \rangle,$$

where $\mathbf{p} \in \mathbf{R}^m$ is a stochastic vector, $A(\sigma) \in \mathbf{R}^{m \times m}$ is a stochastic matrix $m \times m$ ($\sigma \in \Sigma$), and $F \subseteq \{1, \ldots, m\}$.

The function $A : \Sigma \to \mathbf{R}^{m \times m}$ can be extended to Σ^* in such a way that for any word $\sigma_1 \ldots \sigma_l \in \Sigma^*$ we have

$$A(\sigma_1 \ldots \sigma_l) = \prod_{j=1}^{l} A(\sigma_j).$$

The probability distribution $\mathbf{p}A(w)$, for $w \in \Sigma^*$, is obtained processing the system, initialized in control state j with probability $\mathbf{p}_j$ ($1 \leqslant j \leqslant m$), on the input words in Σ^*. The stochastic event generated by SA is the function

$$P_{\mathrm{SA}} : \Sigma^* \to [0, 1],$$

defined by

$$P_{\mathrm{SA}}(w) = \sum_{k \in F} (\mathbf{p}A(w))_k.$$

The stochastic event P_{SA} defined by the stochastic automaton SA is, indeed, a rational power series by the theorem enunciated in the previous subsection. Given a stochastic automaton SA and $\lambda \in [0, 1)$, the language $L_{\mathrm{SA},\lambda}$ accepted by SA with cut point λ is

$$L_{\mathrm{SA},\lambda} = \{w\colon\ P_{\mathrm{SA}}(w) > \lambda\}.$$

The class of languages accepted with a cut point by stochastic automata is the class of stochastic languages. The error function $\varepsilon_{\mathrm{SA},\lambda} : \mathbf{N} \to [0, 1]$ is defined by

$$\varepsilon_{\mathrm{SA},\lambda}(n) = \min_{w:|w| \leqslant n} |P_{\mathrm{SA}}(w) - \lambda|.$$

When there exists $\varepsilon > 0$ such that $\varepsilon_{\mathrm{SA},\lambda}(n) \geqslant \varepsilon$ for every $n \in \mathbf{N}$, then λ is said to be isolated with respect to SA. Notice that $\lceil \varepsilon^{-1}_{\mathrm{SA},\lambda}(n) \rceil$, for $\varepsilon_{\mathrm{QA},\lambda}(n) \neq 0$, is the number of occurrences of the experiment required to know whether word $w \in \Sigma^{\leqslant n}$ is in the language $L_{\mathrm{SA},\lambda}$ with suitable confidence.

The following are the well-known results in the literature.

Fact 1. *For each stochastic automaton* SA $L_{\mathrm{SA},0}$ *is a regular language.*

Theorem 2 (Rabin [29]). *If* λ *is isolated with respect to* SA, *then* $L_{\mathrm{SA},\lambda}$ *is regular.*

Theorem 3 (Saloma and Soittola [31] Turakainen). *A language L is stochastic if and only if there exists a rational power series $\phi : \Sigma^* \to \mathbf{R}$ and a nonnegative real λ such that*

$$L = \{w : \phi(w) > \lambda\}.$$

2.3. Quantum automata

Definition 2. A quantum automaton (QA) with m control states over Σ is a system

$$\mathrm{QA} = \langle \alpha, \{M(\sigma), \sigma \in \Sigma\}, F \rangle,$$

where α is a vector in $\mathbf{C}^m$ such that $\|\alpha\| = 1$, $M(\sigma)$ defines a unitary transformation $M(\sigma) : \mathbf{C}^m \to \mathbf{C}^m$ and $F \subseteq \{1, \ldots, m\}$.

By $M(\sigma_1 \ldots \sigma_l) : \mathbf{C}^m \to \mathbf{C}^m$ $(\sigma_1 \ldots \sigma_j \in \Sigma^*)$ we mean the transformation

$$M(\sigma_1 \ldots \sigma_l) = \prod_{j=1}^{l} M(\sigma_j).$$

The stochastic event generated by QA is the function

$$P_{\mathrm{QA}} : \Sigma^* \to [0, 1],$$

defined by

$$P_{\mathrm{QA}}(w) = \sum_{k \in F} |(\alpha M(w))_k|^2.$$

The language $L_{\mathrm{QA},\lambda}$ accepted by QA with cut point $\lambda \in [0, 1)$ is

$$L_{\mathrm{QA},\lambda} = \{w : P_{\mathrm{QA}}(w) > \lambda\}.$$

Given a quantum automaton QA and $\lambda \in [0, 1)$, the error function $\varepsilon_{\mathrm{QA},\lambda} : \mathbf{N} \to [0, 1]$ is defined by

$$\varepsilon_{\mathrm{QA},\lambda}(n) = \min_{w : |w| \leqslant n} |P_{\mathrm{QA}}(w) - \lambda|$$

Moreover, when there exists $\varepsilon > 0$ such that $\varepsilon_{\mathrm{QA},\lambda}(n) \geqslant \varepsilon$ for every $n \in \mathbf{N}$, then λ is said to be isolated with respect to QA.

3. A non regular language accepted with cut point zero and inverse error polynomial

In this section, we exhibit a quantum automaton with two control states that accepts a non regular language with cut point 0 and it has inverse error polynomial in the length of the input. First, we prove the following lemma.

Lemma 1. *If* $\theta=(\sqrt{5}-1)/2$, *then* $\sin^2(k\pi\theta)\geqslant(\frac{2}{27})^2 1/k^2$ *for all integers* $k\neq 0$.

Proof. By (Hardy and Wright [22]), it is known that if θ is a quadratic irrational, then

$$\inf_{p\in\mathbf{Z}}|k\theta-p|\geqslant\frac{1}{(M+2)^3|k|},$$

where M is any upper bound of the nth quotient of the continued fraction converging to θ. If $\theta=(\sqrt{5}-1)/2$, then each quotient is 1, from which it follows that

$$\inf_{p\in\mathbf{Z}}|k\theta-p|\geqslant\frac{1}{27|k|}. \tag{1}$$

Thus, we have

$$\begin{aligned}\sin^2(\pi k\theta)&=\sin^2\left(\pi\inf_{p\in\mathbb{Z}}|k\theta-p|\right)\quad(\text{since }\sin^2\pi x=\sin^2\pi(x\pm p))\\&\geqslant 4\inf_{p\in\mathbb{Z}}|k\theta-p|^2\quad(\text{since }\sin^2\pi x\geqslant 4x^2\text{ for }0\leqslant x\leqslant\tfrac{1}{2}\\&\qquad\qquad\text{and }0\leqslant\inf_{p\in\mathbb{Z}}|k\theta-p|\leqslant\tfrac{1}{2})\\&\geqslant\left(\frac{2}{27}\right)^2\frac{1}{k^2}\quad(\text{by (1)})\qquad\square\end{aligned}$$

Theorem 4. *There exists a quantum automaton* QA *such that*
1. *the language* $L_{\mathrm{QA},0}$ *accepted by* QA *with cut point* 0 *is not regular*,
2. $\varepsilon_{\mathrm{QA},0}(n)\geqslant(\frac{2}{27})^2 1/n^2$.

Proof. Consider the following QA with two control states and over $\Sigma=\{\sigma,\sigma'\}$:

$$\mathrm{QA}=\left\langle\alpha=(1,0),M(\sigma)=\begin{pmatrix}\cos\pi\theta & -\sin\pi\theta\\ \sin\pi\theta & \cos\pi\theta\end{pmatrix},\right.$$
$$\left.M(\sigma')=\begin{pmatrix}\cos\pi\theta & \sin\pi\theta\\ -\sin\pi\theta & \cos\pi\theta\end{pmatrix},F=\{2\}\right\rangle,$$

where $\theta=(\sqrt{5}-1)/2$. Note that $M(\sigma')$ is the inverse of $M(\sigma)$ and represents the rotation of the angle $\pi\theta$. If $\#_\sigma(w)$, $\#_{\sigma'}(w)$ denote the number of σ and σ' in a word $w\in\Sigma^*$, respectively, it is straightforward to check that $P_{\mathrm{QA}}(w)=\sin^2(\pi k\theta)$, where $k=\#_\sigma(w)-\#_{\sigma'}(w)$. Since θ is irrational, it follows that the language accepted with cut point $\lambda=0$ by QA is

$$L_{\mathrm{QA},0}=\{w:\ \#_\sigma(w)\neq\#_{\sigma'}(w)\}.$$

The language $L_{\mathrm{QA},0}$ is not regular; moreover, if $w \in L_{\mathrm{QA},0}$ by the previous lemma we have that

$$P_{\mathrm{QA}}(w) \geqslant \left(\frac{2}{27}\right)^2 1/(\#_\sigma(w) - \#_{\sigma'}(w))^2$$
$$\geqslant \left(\frac{2}{27}\right)^2 \frac{1}{|w|^2}. \qquad \square$$

4. Quantum and stochastic languages

Denote by e_1 the m-dimensional vector $e_1 = (1, 0, \ldots, 0)$ and by P the cyclic permutation matrix

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

Given the function $\phi : \Sigma^* \to \mathbf{C}$, let $\mathrm{Re}\,\phi : \Sigma^* \to \mathbf{R}$ and $Co\,\phi : \Sigma^* \to \mathbf{R}$ be such that $\phi(w) = \mathrm{Re}\,\phi(w) + \mathrm{i}Co\,\phi(w)$ for each $w \in \Sigma^*$.

Lemma 2. *If $\phi : \Sigma^* \to \mathbf{C}$ is a rational power series represented by*

$$\langle \alpha = \alpha_1 + \mathrm{i}\alpha_2, \{M(\sigma) = M_1(\sigma) + \mathrm{i}M_2(\sigma):\ \sigma \in \Sigma\}, \eta \rangle,$$

then $\mathrm{Re}\,\phi : \Sigma^* \to \mathbf{R}$ is the rational power series represented by

$$\langle \hat{\alpha} = \alpha_1 \otimes e_1 I + \alpha_2 \otimes e_1 P, \{\hat{M}(\sigma) = M_1(\sigma) \otimes I + M_2(\sigma) \otimes P:\ \sigma \in \Sigma\},$$
$$\hat{\eta}_1 = \eta \otimes (1, 0, -1, 0)^{\mathrm{T}} \rangle.$$

and $Co\,\phi : \Sigma^* \to \mathbf{R}$ is the rational power series represented by

$$\langle \hat{\alpha}, \{\hat{M}(\sigma):\ \sigma \in \Sigma\}, \hat{\eta}_2 = \eta \otimes (0, 1, 0, -1)^{\mathrm{T}} \rangle.$$

Proof. By induction on the length n of the words we can show that if

$$\alpha M(\sigma_1) \cdots M(\sigma_n) = a_1 + \mathrm{i}a_2$$

and

$$\hat{\alpha}\hat{M}(\sigma_1) \cdots \hat{M}(\sigma_n) = b_1 \otimes e_1 I + b_2 \otimes e_1 P + b_3 \otimes e_1 P^2 + b_4 \otimes e_1 P^3,$$

then it holds $a_1 = b_1 - b_3$ and $a_2 = b_2 - b_4$. Consequently, we have

$$\hat{\alpha}\hat{M}(\sigma_1) \cdots \hat{M}(\sigma_n)\hat{\eta}_1 = (b_1, b_2, b_3, b_4)(\eta, 0, -\eta, 0)^{\mathrm{T}}$$
$$= (b_1 - b_3)\eta = a_1\eta$$

and

$$\hat{\alpha}\hat{M}(\sigma_1)\cdots\hat{M}(\sigma_n)\hat{\eta}_2 = a_2\eta,$$

where

$$\alpha M(\sigma_1)\cdots M(\sigma_n)\eta = a_1\eta + \mathrm{i}a_2\eta. \qquad \square$$

Theorem 5. *The language*

$$L_{\mathrm{QA},\lambda} = \{w\colon\ P_{\mathrm{QA},\lambda} > \lambda\}$$

accepted by a quantum automaton QA *with cut point* λ *is a stochastic language.*

Proof. The stochastic event

$$P_{\mathrm{QA}} : \Sigma^* \to [0,1],$$

is defined by

$$\begin{aligned} P_{\mathrm{QA}}(w) &= \sum_{k\in F} |(\alpha M(w))_k|^2 \\ &= \sum_{k\in F} \{\mathrm{Re}^2[(\alpha M(w))_k] + Co^2[(\alpha M(w))_k]\}, \end{aligned}$$

where $\mathrm{Re}[(\alpha M(w))_k] + \mathrm{i}Co[(\alpha M(w))_k] = (\alpha M(w))_k$ $(w \in \Sigma^*)$. Since $\phi_k : \Sigma^* \to \mathbf{C}$ such that $\phi_k(w) = (\alpha M(w))_k$ is a rational power series, then by Lemma 2 both $\mathrm{Re}\,\phi_k : \Sigma^* \to \mathbf{R}$ and $Co\,\phi_k : \sigma^* \to \mathbf{R}$ are rational power series. The class of power series is closed under the sum and the Hadamard product. Therefore, the proof follows by Theorem 3. $\square$

Lemma 3. *If* M *is any unitary matrix of order* m *over the complex field and* I_m *is the identity matrix over* $\mathbf{C}^m$, *then for any* $\varepsilon > 0$ *there exists* $v \in \mathbf{N}$ *such that it holds*

$$\|M^v - I_m\| \leqslant \varepsilon.$$

Proof. Consider the linear space of matrices of order m over the complex field with norm $\|M\| = \sup_{v\in \mathrm{US}_m} \|vM\|$. Each unitary matrix M is such that $\|M\| = 1$; moreover, the set of unitary matrices along with the distance $d(M,M') = \|M - M'\|$ is a compact metric space. Then, from the sequence $\{M^n\}_{n\in\mathbf{N}}$ we can extract a Cauchy sequence $\{M^{n_k}\}_{k\in\mathbf{N}}$, i.e. for each $\varepsilon > 0$ there exists $v_\varepsilon \in \mathbf{N}$ such that $n_{k_1}, n_{k_2} > v_\varepsilon$ implies $\|M^{n_{k_2}} - M^{n_{k_1}}\| \leqslant \varepsilon$. Fix $n_{k_2} > n_{k_1} > v_\varepsilon$ and set $v = n_{k_2} - n_{k_1}$. We have

$$\begin{aligned} \|M^v - I_m\| &= \|M^{-n_{k_1}} M^{n_{k_1}+v} - M^{-n_{k_1}} M^{n_{k_1}}\| \\ &= \|M^{-n_{k_1}}(M^{n_{k_1}+v} - M^{n_{k_1}})\| \\ &= \|M^{n_{k_1}+v} - M^{n_{k_1}}\| \quad (\text{since } M^{-n_{k_1}} \text{ preserves length}) \\ &\leqslant \varepsilon \qquad \square \end{aligned}$$

The following lemma states a useful property to check whether a language is not accepted by any quantum automaton.

Lemma 4. *If $L_{\mathrm{QA},\lambda}$ is a language accepted by a quantum automaton* QA, *then for each $x \in \Sigma^*$ and for every $w \in L_{\mathrm{QA},\lambda}$ there exists a positive integer $\bar{v}$ such that $wx^{\bar{v}} \in L_{\mathrm{QA},\lambda}$.*

Proof. For any $v \in \mathbf{N}$ it results

$$\begin{aligned}
|P_{\mathrm{QA}}(w) - P_{\mathrm{QA}}(wx^v)| &= \left| \sum_{k\in F} (|(\alpha M(w))_k|^2 - |(\alpha M(wx^v))_k|^2) \right| \\
&\leqslant 2 \sum_{k\in F} \| |(\alpha M(w))_k| - |(\alpha M(wx^v))_k| \| \\
&\leqslant 2 \sum_{k\in F} |(\alpha M(w))_k - (\alpha M(wx^v))_k| \\
&= 2 \sum_{k\in F} |\alpha M(w)(I - M^v(x))e_k| \\
&\leqslant 2 \sum_{k\in F} \|I - M^v(x)\| \\
&= 2|F|\|I - M^v(x)\|.
\end{aligned}$$

Since $w \in L_{\mathrm{QA},\lambda}$, then $P_{\mathrm{QA}}(w) > \lambda$ and we can set $P_{\mathrm{QA}}(w) - \lambda = \delta > 0$. By Lemma 3, there exists $\bar{v}$ such that

$$\|I - M^{\bar{v}}(x)\| \leqslant \frac{\delta}{4|F|}$$

and, consequently,

$$\left|P_{\mathrm{QA}}(w) - P_{\mathrm{QA}}(wx^{\bar{v}})\right| \leqslant \frac{\delta}{2}.$$

We can conclude that $wx^{\bar{v}} \in L_{\mathrm{QA},\lambda}$ since

$$P_{\mathrm{QA}}(wx^v) - \lambda \geqslant P_{\mathrm{QA}}(w) - \frac{\delta}{2} - \lambda \geqslant \frac{\delta}{2} > 0. \qquad \square$$

The next two theorems are consequences of Lemma 4.

Theorem 6. *Quantum automata accept languages empty or containing an infinite number of words.*

Theorem 7. *The class of the quantum languages is not closed under complementation.*

Proof. Consider the language $L \subseteq \{\sigma, \sigma'\}^*$ such that

$$L = \{w : \#_\sigma(w) \neq \#_{\sigma'}(w)\}.$$

By Theorem 4 there exists a QA accepting L. Moreover, the complement L^c of L is

$$L^c = \{w:\ \#_\sigma(w) = \#_{\sigma'}(w)\}.$$

Note that if $w = \sigma\sigma' \in L^c$ and $x = \sigma^2\sigma'$, then for each $v > 0$ $\#_\sigma(wx^v) > \#_{\sigma'}(wx^v)$ and therefore $wx^v \notin L^c$. The proof follows since by Lemma 4 does not exist a QA accepting L^c. □

Lemma 5 (Paz, [27]). *For any $m \times m$ stochastic matrix A and m-dimensional stochastic vectors $\mathbf{p} = (p_1, \ldots, p_m)$, $\mathbf{p}' = (p'_1, \ldots, p'_m)$ there exists δ $(0 \leqslant \delta \leqslant 1)$ such that*

$$\|(\mathbf{p} - \mathbf{p}')A\| \leqslant (1 - \delta)\|\mathbf{p} - \mathbf{p}'\|,$$

where $\|\mathbf{p} - \mathbf{p}'\| = \sum_{k=1}^{m} |p_k - p'_k|$. □

A straightforward consequence of the previous lemma is the following.

Lemma 6. *There exists $\bar{\delta}$, where $0 \leqslant \bar{\delta} \leqslant 1$, such that for any words $x, y \in \Sigma^*$ it holds that*

$$\|P_{\mathrm{SA}}(yx) - P_{\mathrm{SA}}(x)\| \leqslant 2(1 - \bar{\delta})^{|x|}.$$ □

Lemma 7. *If the stochastic automaton* SA *has stochastic matrices $A(\sigma)$ such that $A_{j,r}(\sigma) > 0$, for $j, r = 1, \ldots, m$ and $\sigma \in \Sigma$, then only one of the properties holds*
1. *there is $w \in \Sigma^*$ such that $P_{\mathrm{SA}}(w) = \lambda$;*
2. *the cut point is isolated with respect to* SA *(in Rabin's sense);*
3. *there exists a nonnegative real $\rho < 1$ such that $\varepsilon_{\mathrm{SA},\lambda}(n) \leqslant \rho^n$ for each $n \in \mathbf{N}$.*

Proof. Set

$$x_n = \min_{x:|x|=n} |P_{\mathrm{SA}}(x) - \lambda|.$$

Suppose that $P_{\mathrm{SA}}(w) \neq \lambda$ for each $w \in \Sigma^*$. Let $\bar{\delta}$ be the positive integer such that Lemma 6 holds. If for every n $|P_{\mathrm{SA}}(x_n) - \lambda| \leqslant 3(1 - \bar{\delta})^n$, then Property 3 holds. Conversely, suppose that there exists $\bar{n}$ such that

$$|P_{\mathrm{SA}}(x_n) - \lambda| > 3(1 - \bar{\delta})^{\bar{n}}. \tag{2}$$

Then, for any word $z = ya_{\bar{n}} \in \Sigma^*$ with suffix $a_{\bar{n}}$ of length $\bar{n}$ it holds that

$$\begin{aligned}
|P_{\mathrm{SA}}(z) - \lambda| &= |P_{\mathrm{SA}}(ya_{\bar{n}}) - P_{\mathrm{SA}}(a_{\bar{n}}) + P_{\mathrm{SA}}(a_{\bar{n}}) - \lambda| \\
&\geqslant \|P_{\mathrm{SA}}(a_{\bar{n}}) - \lambda| - |P_{\mathrm{SA}}(ya_{\bar{n}}) - P_{\mathrm{SA}}(a_{\bar{n}})\| \\
&\geqslant \|P_{\mathrm{SA}}(x_n) - \lambda| - |P_{\mathrm{SA}}(ya_{\bar{n}}) - P_{\mathrm{SA}}(a_{\bar{n}})\| \\
&\geqslant (1 - \bar{\delta})^{\bar{n}} \text{ (by 2 and Lemma 6)}
\end{aligned}$$

Therefore, we have

$$\inf_{z\in\Sigma^*}|P_{\mathrm{SA}}(z)-\lambda| = \min\left\{\min_{z:|z|<\bar{n}}|P_{\mathrm{SA}}(z)-\lambda|, \inf_{z:|z|\geqslant\bar{n}}|P_{\mathrm{SA}}(z)-\lambda|\right\}$$
$$\geqslant \min\left\{\min_{z:|z|<\bar{n}}|P_{\mathrm{SA}}(z)-\lambda|, (1-\bar{\delta})^{\bar{n}}\right\} > 0 \text{ (since } p(z)\neq\lambda). \quad \square$$

The next theorem is a simple corollary of Lemma 7.

Theorem 8. *If for every $n\in\mathbf{N}$ there exists a polynomial $p(n)$ such that $\varepsilon_{\mathrm{SA},\lambda}(n)\geqslant(1/p(n))$, then $L_{\mathrm{SA},\lambda}$ is a regular language.*

Proof. Obviously, $P_{\mathrm{SA}}(w)\neq\lambda$ for each $w\in\Sigma^*$. If λ were not isolated with respect to SA, by Theorem 7, we would have

$$\frac{1}{p(n)}\leqslant\varepsilon_{\mathrm{SA},\lambda}\leqslant\rho^n,$$

for any $n\in\mathbf{N}$. Consequently, λ is isolated and $L_{\mathrm{SA},\lambda}$ is regular. $\square$

References

[1] A. Barenco, C.H. Bennet, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A 52 (1995) 3457–3467.
[2] P. Benioff, Quantum mechanical hamiltonian models of turing machines, J. Statist. Phys. 29 (1982) 515–546.
[3] C.H. Bennet, Logical reversibility of computation, IBM J. Res. Develop. 17 (1973) 525–532.
[4] C.H. Bennet, Quantum computation and information, Phys. Today 48 (10) (1995) 24–30.
[5] C.H. Bennet, E. Bernstein, G. Brassard, U. Vazirani, Strengths and weaknesses of quantum computing, SIAM J. Comput. 26 (5) (1997) 1510–1523.
[6] E. Bernstein, U. Vazirani, Quantum complexity theory, SIAM J. Comput. 26 (5) (1997) 1411–1473.
[7] A. Berthiaume, G. Brassard, The quantum challenge to structural complexity theory Proc. 7th IEEE Conf. Structure in Complexity Theory, 1992.
[8] A. Berthiaume, G. Brassard, Oracle quantum computing Proc. Physics of Computation, 1992.
[9] J. Berstel, C. Retenauer, Rational Series and their Languages, Springer, New York, 1988.
[10] L. Chuang, Y. Yamamoto, A simple quantum computer, Phys. Rev. A 52 (1995) 3489–3496.
[11] J.I. Cirach, P. Zoller, Quantum computation with cold trapped ions, Phys. Rev. Lett. 74 (1995) 4091–4094.
[12] D.W. Cohen, An Introduction to Hilbert Space and Quantum Logic, Springer, New York, 1989.
[13] D. Deutsch, Quantum theory, the church turing principle and the universal quantum computer, Proc. Roy. Soc. London A 400 (1985) 73–90.
[14] D. Deutsch, Quantum computational networks, Proc. Roy. Soc. London A 425 (1989) 73–90.
[15] D. Deutsch, R. Jozsa, Rapid solutions of problems by quantum computation, Proc. Roy. Soc. London A 439 (1992) 553–555.
[16] D.P. DiVincenzo, Quantum computation, Science 269 (1995) 256–261.
[17] D.P. DiVincenzo, Two-bit gates are universal for quantum computation, Phys. Rev. A 51 (1995) 1015–1022.
[18] A. Ekert, R. Jozsa, Quantum computation and Shor's factoring algorithm, Rev. Modern Phys. 68 (1996) 733–754.
[19] R. Feynman, Simulating physics with computers, Internat. J. Theoret. Phys. 21 (1982) 467–488.
[20] R. Feynman, Quantum mechanical computers, Found. Phys. 16 (1986) 507–531.

[21] S.V. Fomin, A.N. Kolmogorov, Introductory Real Analysis, Dover, New York, 1975.
[22] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Oxford Press, Oxford, 1979.
[23] J.E. Hopcroft, J.D. Ullman, Introduction to Automata Theory, Languages and Computation, Addison-Wesley, Reading, MA, 1979.
[24] H. Hughes, The Structure and Interpretation of Quantum Mechanics, Harward University Press, Cambridge, MA, 1989.
[25] S. Lloyd, A potentially realizable quantum computer, Science 261 (1993) 1659–1671.
[26] S. Lloyd, Envisioning a quantum supercomputer, Science 263 (1994) 695.
[27] A. Paz, Introduction to Probabilistic Automata, Academic Press, New York, 1971.
[28] J.E. Pin, On the languages recognized by finite reversible automata, 14th ICALP, Lecture Notes in Computer Science, Springer, Berlin, 1987, pp. 237–249.
[29] M.O. Rabin, Probabilistic Automata, Sequential Machines, Addison-Wesley, Reading, MA, 1964.
[30] R.L. Rivest, A. Shamir, L. Adelman, A method of obtaining digital signatures and public-key cryptosystems, Comm. *ACM* 21 (2) (1978) 120–126.
[31] A. Saloma, M. Soittola, Automata Aspects of Formal Power Series, Springer, Berlin, 1978.
[32] M.P. Scutzenberger, On the definition of a family of automata, Inform. and Control 4 (1961) 245–270.
[33] P. Shor, Algorithms for quantum computation: discrete log and factoring, SIAM J. Comput. 26 (5) (1997) 1484–1509.
[34] D. Simon, On the power of quantum computation, SIAM J. Comput. 26 (5) (1997) 1474–1483.
[35] T. Sleator, H. Weinfurther, Realizable quantum logic gates, Phys. Rev. Lett. 74 (1995) 4087–4090.
[36] G. Teich, K. Obermayer, G. Mahler, Structural basis of multistationary quantum systems II: effective few particle dynamics, Phys. Rev. B 37 (1988) 173–192.
[37] A. Yao, Quantum circuit complexity, Proc. 34th IEEE Symp. on Foundations of Computer Science (1993).