*International Journal of Theoretical Physics, Vol. 41, No. 4, April 2002 (© 2002)*

# Properties of Quantum Languages

**S. Gudder[1,2] and R. Ball[1]**

*Received May 21, 2001*

The class of quantum languages $Q(\Sigma)$ over an alphabet $\Sigma$ is the class of languages accepted by quantum automata. We study properties of $Q(\Sigma)$ and compare $Q(\Sigma)$ with the class of regular languages $R(\Sigma)$. It is shown that $Q(\Sigma)$ is closed under union, intersection, and reversal but is not closed under complementation, concatenation, or Kleene star. It is also shown that $Q(\Sigma)$ and $R(\Sigma)$ are incomparable. Finally, we prove that $L \in Q(\Sigma)$ if and only if $L$ admits a transition amplitude function satisfying a certain property and a similar characterization is given for $R(\Sigma)$.

**KEY WORDS:** quantum languages; quantum automata; regular languages.

## 1. INTRODUCTION

Although theoretical quantum computers were first studied in the 1980s (Benioff, 1982a,b; Deutsch, 1989; Feynman, 1982, 1986), it has only been recently that they have been considered with intense interest. One reason for this renewed interest is that quantum algorithms have been discovered, which show that quantum computers are capable of executing programs such as integer factorization and discrete logarithms exponentially faster than classical computers (Deutsch and Jozsa, 1992; Grover, 1996; Shor, 1997; Simon, 1997; Williams, 1999). Another reason is that prototypical quantum computers employing nuclear magnetic resonance or nonlinear optics technologies have actually been constructed (Williams, 1999).

A fundamental, yet particularly simple, type of quantum computer is a quantum automaton. Such machines have an input but no output and the languages that they accept are called quantum languages (Gudder, 1999, 2000, 2000a; Kondacs and Watrous, 1997; Moore and Crutchfield, in press). This paper discusses properties of quantum languages and compares them with the classical languages accepted by deterministic automata. The main classical languages are the regular languages and their properties are well-known. As we shall see, the quantum languages share some of the properties of regular languages and do not share others.

[1] Department of Mathematics and Computer Science, University of Denver, Denver, Colorado.

[2] To whom correspondence should be addressed at Department of Mathematics and Computer Science, University of Denver, Denver, Colorado 80208; e-mail: sgudder@du.edu.

0020-7748/02/0400-0569/0 © 2002 Plenum Publishing Corporation

We denote the class of regular languages over an alphabet $\Sigma$ by $R(\Sigma)$ and the quantum languages by $Q(\Sigma)$. It is well known that $R(\Sigma)$ is closed under the set-theoretic operations of union, intersection, and complementation. Moreover, $R(\Sigma)$ is closed under the monoid operations of concatenation, Kleene star, and reversal. The set-theoretic and monoid closure properties of $Q(\Sigma)$ will be some of the main concerns of this paper. There are various characterizations of $R(\Sigma)$ and our other main concern will be to develop a characterization of $Q(\Sigma)$.

For the benefit of readers who are not familiar with classical automata and regular languages, we present a brief review in Sections 2 and 3. Section 3 also gives a reformulation of the concept of a deterministic automaton that should aid the understanding of the operation of a quantum automaton. Section 4 introduces a class of languages $\mathrm{Rev}(\Sigma)$ called the reversible languages. These languages are common to $R(\Sigma)$ and $Q(\Sigma)$ and they are useful for comparing their properties. The languages $\mathrm{Rev}(\Sigma)$ are precisely those that are accepted by reversible deterministic automata. We show that $\mathrm{Rev}(\Sigma)$ is closed under union, intersection, complementation, and reversal but is not closed under concatenation or Kleene star.

Section 5 first describes the operation of $q$-automata and the languages $Q(\Sigma)$ that they accept. We show that $Q(\Sigma)$ contains $\mathrm{Rev}(\Sigma)$ and the set of finite languages. It is demonstrated that $Q(\Sigma)$ is closed under union, intersection, and reversal but is not closed under complementation, concatenation, or Kleene star. Moreover, we show that $R(\Sigma)$ and $Q(\Sigma)$ are incomparable; that is, neither is contained in the other. Finally, we briefly mention another class of quantum languages denoted by $Q_\eta(\Sigma)$. Although it is known that $R(\Sigma)$, $Q(\Sigma)$, and $Q_\eta(\Sigma)$ are mutually incomparable, most of the properties of $Q_\eta(\Sigma)$ are still unknown.

The paper concludes with a characterization of $Q(\Sigma)$ in Section 6. This result shows that $L \in Q(\Sigma)$ if and only if $L$ admits a transition amplitude function that satisfies a certain condition. For comparison purposes, we also present similar characterizations for $R(\Sigma)$ and $\mathrm{Rev}(\Sigma)$. Some of the material of this paper is a continuation of our work in Gudder (2000), and we refer to this work for needed results.

## 2. FORMAL LANGUAGES

An **alphabet** is a finite nonempty set of **symbols**. A **string** over an alphabet $\Sigma$ is a finite sequence of symbols from $\Sigma$. Instead of writing strings as $(a_1, a_2, \ldots, a_n)$, we simply juxtapose the symbols $a_1a_2 \cdots a_n$. We use the notation $aa \cdots a = a^n$ when there are $n$ $a$'s. A string may have no symbols in which case it is the **empty string** and is denoted by $e$. The set of all strings including $e$ over $\Sigma$ is denoted by $\Sigma^*$. Then $\Sigma^*$ becomes a monoid in which the product is juxtaposition and the identity is $e$. The length of a string $w$ is the number of symbols in $w$ and is denoted by $|w|$. If $w$ is a string, we write $w(i)$ for the symbol in the $i$th position for $i \leq |w|$. A string $x$ is a **prefix (suffix)** of a string $w$ if $w = xy$ $(w = yx)$ for some $y \in \Sigma^*$.

Any set of strings over $\Sigma$, that is any subset of $\Sigma^*$, is called a **language** over $\Sigma$. For example, $\Sigma^*$, $\emptyset$, and $\Sigma$ are languages over $\Sigma$. Since languages over $\Sigma$ are sets, they can be combined by the set operations of union, intersection, and difference. We can also use the fact that $\Sigma^*$ is a monoid to define other operations on languages. If $L_1, L_2 \subseteq \Sigma^*$, their **concatenation** is the language $L = L_1 L_2$ given by

$$L = \{w \in \Sigma^* : w = xy, x \in L_1, y \in L_2\}$$

The **Kleene star** of a language $L$, denoted by $L^*$, is the set of all strings obtained by concatenating zero or more strings from $L$. By convention, the concatenation of zero strings is $e$ and the concatenation of one string is the string itself. Thus,

$$L^* = \{w \in \Sigma^* : w = w_1 w_2 \cdots w_n, n \geq 0, w_1, \ldots, w_n \in L\}$$

For example, $\Sigma^*$ is the Kleene star of the language $\Sigma$ and $\emptyset^* = \{e\}$. Notice that if $L \neq \emptyset$, then $L^*$ is infinite. If $w = w_1 w_2 \cdots w_n \in \Sigma^*$, the **reversal** $w^R$ of $w$ is defined as $w^R = w_n \cdots w_2 w_1$. It is clear that $w^{RR} = w$ and that $(xy)^R = y^R x^R$ for every $w, x, y \in \Sigma^*$. The **reversal** $L^R$ of a language $L$ is defined as $L^R = \{w^R : w \in L\}$.

In this paper we shall discuss the properties of various classes of languages. For a simple example, let $F(\Sigma)$ be the class of all finite languages over $\Sigma$. It is clear that $F(\Sigma)$ is closed under union, intersection, and difference. However, it is not closed under complementation and so $F(\Sigma)$ is not a Boolean algebra. It is also evident that $F(\Sigma)$ is closed under concatenation and reversal but is not closed under Kleene star. We next discuss a less trivial and very important class of languages called the regular languages.

The **regular languages** over $\Sigma$ are the smallest collection $R(\Sigma)$ of languages over $\Sigma$ that contain $\{\{\sigma\} : \sigma \in \Sigma\} \cup \{\emptyset\}$ and is closed under union, concatenation, and Kleene star. Thus, $R(\Sigma)$ contains $\emptyset$ and the singleton strings $\{\sigma\}$, $\sigma \in \Sigma$; the union, concatenation, and Kleene star of languages in $R(\Sigma)$ are again in $R(\Sigma)$; and $R(\Sigma)$ is the smallest set of languages over $\Sigma$ with these properties. In the next section we shall see that $R(\Sigma)$ is also closed under intersection and differences. In particular, if $L \in R(\Sigma)$, then $\Sigma^* \smallsetminus L \in R(\Sigma)$ so $R(\Sigma)$ is a Boolean algebra. Moreover, in the next section we shall see that $R(\Sigma)$ is closed under reversal and shall give the connection between regular languages and deterministic automata. Finally, it is clear that $F(\Sigma) \subseteq R(\Sigma)$.

We now discuss a useful characterization of $R(\Sigma)$. Let $L \subseteq \Sigma^*$ be a language and let $x, y \in \Sigma^*$. Then we write $x \approx_L y$ if for every $z \in \Sigma^*$ we have $xz \in L$ if and only if $yz \in L$. Notice that $\approx_L$ is an equivalence relation on $\Sigma^*$. We use $[x]_L$ to denote the equivalence class of $x$ with respect to $\approx_L$ and write

$$\Sigma^*/L = \{[x]_L : x \in \Sigma^*\}$$

The following result is called the Myhill-Nerode theorem (Lewis and Papadimitriou, 1998).

**Theorem 2.1.** *$L \in R(\Sigma)$ if and only if $\Sigma^*/L$ is finite.*

We next present a useful method for showing that a language is not regular (Lewis and Papadimitriou, 1998).

**Theorem 2.2.** *Let $L$ be a regular language. Then there exists $n \in \mathbb{N}$ such that any string $w \in L$ with $|w| \geq n$ can be written as $w = xyz$ such that $y \neq e$, $|xy| \leq n$ and $xy^iz \in L$ for every $i \geq 0$.*

This last result is called a **pumping theorem** because we can pump in (insert) $y$ any number of times without effecting the membership of $w$ in $L$. A simple exercise employing Theorem 2.2 shows that if $\Sigma = \{a, b\}$ and $L_1 = \{a^ib^i : i \geq 0\}$, then $L_1 \notin R(\Sigma)$. In a similar way

$$L_2 = \{w \in \Sigma^* : w \text{ has an equal number of } a\text{'s and } b\text{'s}\} \notin R(\Sigma)$$

Although $L_1, L_2 \notin R(\Sigma)$ they belong to a larger class called the context-free languages. Although we shall not discuss this class in detail, we will mention that the context-free languages are those that can be constructed from the rules of a formal grammar. Two examples of languages that are not context-free over $\Sigma = \{a, b, c\}$ are $\{a^ib^ic^i : i \geq 0\}$ and

$$L_3 = \{w \in \Sigma^* : w \text{ has the same number of } a\text{'s, } b\text{'s, and } c\text{'s}\}$$

## 3. CLASSICAL AUTOMATA AND LANGUAGES

We motivate the precise definition of a deterministic automaton by first describing how such devices operate. Strings are fed into the machine by means of an **input tape** which is divided into cells with one symbol in each cell. The main part of the machine is the **finite control** which at a specified moment is in one of a finite number of internal **states**. The finite control can sense what symbol is written in any cell of the tape by means of a movable **reading head**. Initially the reading head is placed at the leftmost cell of the tape and the control is set in a designated **initial** state. At regular intervals the automaton reads one symbol from the input tape and then enters a new state that depends only on the current state and the symbol just read. After reading an input symbol, the reading head moves one cell to the right on the input tape so that on the next move it will read the symbol in the next cell. This process is continued until the reading head reaches the end of the input string. If the control ends up in one of a set of **final states**, the input is considered to be **accepted**. The language accepted by the machine is the set of all strings it accepts. This is an example of a language recognizer.

We now present the precise definition. A **deterministic automaton** (abbreviated DA) is a quintuple $M = (S, \Sigma, \delta, s_0, F)$ where $S$ is a finite set of states,

$\Sigma$ is an alphabet, $s_0 \in S$ is the **initial state**, $F \subseteq S$ is the set of **final states**, and $\delta : S \times \Sigma \to S$ is the **transition function**. If $M$ is in state $s \in S$ and the symbol read from the input tape is $a \in \Sigma$, then $\delta(s, a) \in S$ is the uniquely determined state to which $M$ passes. It is because of the uniqueness of $\delta(s, a)$ that $M$ is called deterministic. We call $(s, a, s') \in S \times \Sigma \times S$ a **transition** if $\delta(s, a) = s'$. For example, if $M$ is fed the string *aba*, then $M$ starts in state $s_0$ and proceeds along the sequence of states $s_0$, $\delta(s_0, a)$, $\delta(\delta(s_0, a), b)$, $\delta(\delta(\delta(s_0, a), b), a)$. A **configuration** of $M$ is an element of $S \times \Sigma^*$. A configuration $(s, w)$ represents the current state $s$ of $M$ and the unread part $w$ of the string being processed. A **computation** of $M$ on an input string is the sequence of configurations of $M$ that represent the status of $M$ at successive moments. Thus, the computation for the input string *aba* becomes $(s_0, aba)$, $(\delta(s_0, a), ba)$, $(\delta(\delta(s_0, a), b), a)$, $(\delta(\delta(\delta(s_0, a), b), a), e)$.

The binary relation $\vdash_M$ holds between two configurations of $M$ if and only if $M$ can pass from one to the other as a result of a single move. Thus, $(s, w) \vdash_M (s', w')$ if and only if $w = aw'$ for some $a \in \Sigma$ and $\delta(s, a) = s'$. We then say that $(s, w)$ **yields** $(s', w')$ **in one step**. We denote the reflexive, transitive closure of $\vdash_M$ by $\vdash_M^*$. Then $(s, w) \vdash_M^* (s', w')$ is read $(s, w)$ yields $(s', w')$ (after some number, possibly zero, of steps). A string $w \in \Sigma^*$ is **accepted** by $M$ if there exists an $s \in F$ such that $(s_0, w) \vdash_M^* (s, e)$. We can extend $\delta$ to $S \times \Sigma^*$ by defining $\delta(s, w) = s' \in S$ where $s'$ is the unique state that satisfies $(s, w) \mapsto_M^* (s', e)$. Then $w$ is accepted by $M$ if and only if $\delta(s_0, w) \in F$. The **language accepted** by $M$, denoted $L(M)$, is the set of all strings accepted by $M$. The following theorem is the most important result in the theory of deterministic automata (Lewis and Papadimitriou, 1998).

**Theorem 3.1.** *A language $L$ is accepted by a DA if and only if $L$ is regular.*

Theorem 3.1 is useful in many ways. For example, a simple application of Theorem 3.1 shows that $R(\Sigma)$ is closed under complementation and hence $R(\Sigma)$ is a Boolean algebra. Also, Theorem 3.1 can be employed to show that $R(\Sigma)$ is closed under reversal. Applying Theorem 2.1 one can construct the minimal DA, denoted by $M_L$, that accepts $L \in R(\Sigma)$. The DA $M_L$ is minimal in the sense that $M_L$ has the least number of states. We can define $M_L$ by

$$M_L = (\Sigma^*/L, \Sigma, \delta_L, [e]_L, \{[x]_L : x \in L\})$$

where $\delta_L([x]_L, a) = [xa]_L$.

Another type of classical automaton is the nondeterministic automaton (NA). For a NA the next state for a given current state and input symbol may not be unique. Although a DA is a special case of a NA, it can be shown that the set of languages accepted by NA is still the set of regular languages (Lewis and Papadimitriou, 1998). Thus, NA are no more powerful than DA.

There is a result similar to Theorem 3.1 for context-free languages. This theorem says that $L$ is context-free if and only if $L$ is accepted by a push-down automaton. Roughly speaking, a push-down automaton is like a NA except it possesses an unlimited memory stack.

It is convenient to describe the operation of a DA in terms of certain operators on a Hilbert space. This is unnecessary for a DA but it will be essential when we discuss quantum automata. Let $M = (S, \Sigma, \delta, s_0, F)$ be a DA and suppose the cardinality $|S| = n$. Let $H$ be an $n$-dimensional complex Hilbert space and let $s \mapsto \hat{s}$ be a bijection from $S$ to an orthonormal basis $\hat{S}$ of $H$. We call $\hat{S}$ a **computational basis** for $M$ and we call $\hat{F} = \text{span}\,\{\hat{s} : s \in F\}$ the **final subspace** for $M$. For $a \in \Sigma$ define the linear operator $U(a) : H \to H$ by $U(a)\hat{s} = \hat{t}$ if $\delta(s, a) = t$ and extend $U(a)$ to $H$ by linearity. Relative to $\hat{S}$, $U(a)$ is represented by a 0–1 matrix in which each column contains precisely one 1. Of course, there may be more than one 1 in a row. We call such a matrix a 0–1 **stochastic matrix**. If $w = a_1a_2 \cdots a_k$ is a string in $\Sigma^*$, we define

$$U(w) = U(a_k) \cdots U(a_2)U(a_1)$$

if $w \neq e$ and otherwise $U(e) = I$. It is clear that $U(w)$ is again a 0–1 stochastic matrix. We call $U(w)$ the **evolution operator** for $w$ because it describes the evolution of $M$ when fed the string $w$. We then have that $w \in L(M)$ if and only if $U(w)\hat{s}_0 \in \hat{F}$. We say that $M$ is **reversible** if $U(a)$ is invertible for every $a \in \Sigma$. Equivalently, $M$ is reversible if and only if for every $a \in \Sigma$ the map $\delta(\cdot, a) \colon S \to S$ is injective (and hence, bijective). A DA is reversible precisely when it does not dissipate heat and this is an important factor in the design of modern computers. The proof of the following lemma is clear.

**Lemma 3.2.** *A DA is reversible if and only if $U(a)$ is unitary for every $a \in \Sigma$.*

We now consider probabilistic automata (PA) and, as we shall see, this type of classical automata is similar to quantum automata. A PA is a quintuple $M = (S, \Sigma, \delta, s_0, F)$ where $S, \Sigma, s_0, F$ are the same as for a DA and $\delta \colon S \times \Sigma \times S \to [0, 1]$ is a transition probability function satisfying

$$\sum_{t \in S} \delta(s, a, t) = 1 \tag{3.1}$$

for every $s \in S, a \in \Sigma$. We interpret $\delta(s, a, t)$ as the probability that $M$ enters state $t$ after scanning $a$ in its current state $s$. Then Eq. (3.1) says that $M$ must enter some state with probability 1. As with a DA, the action of $M$ can be conveniently described by an evolution operator. Let $\hat{S}$ be a computational basis for $M$ in the Hilbert space $H$. For $a \in \Sigma$, define the linear operator $U(a)$ on $H$ by

$$U(a)\hat{s} = \sum_{t \in S} \delta(s, a, t)\hat{t} \tag{3.2}$$

and extend by linearity. Then $U(a)$ is represented by a matrix whose entries are in [0, 1] and whose column sums are 1. Thus, we may consider $U(a)$ to be a stochastic matrix. For $w \in \Sigma^*$ we define the operator $U(w) : H \to H$ as before and call $U(w)$ the **evolution operator** for $w$. Notice from Eq. (3.2) that $U(a)\hat{s}$ is a convex combination of elements of $\hat{S}$. We call such vectors **probability vectors**. It follows from the next well-known lemma that $U(w)$ is a stochastic matrix and thus the evolution of $M$ under $w$ gives a Markov chain.

**Lemma 3.3.** (a) *If A and B are stochastic matrices, then AB is a stochastic matrix.* (b) $U(w)\psi$ *is a probability vector for any probability vector* $\psi$.

Of course, a DA is a special case of a PA in which the transition probability function has values 0 and 1. Now the set of stochastic matrices form a convex set so in a sense we can consider the evolution operators of PA as forming a convex set. The next result shows that the evolution operators of DA are the extreme points of this convex set.

**Lemma 3.4.** *If $\mathcal{S}$ is the set of stochastic $n \times n$ matrices, then the set of 0–1 stochastic $n \times n$ matrices is the set of extreme points of $\mathcal{S}$.*

We say that a PA is **reversible** if $U(a)^{-1}$ exists and is a stochastic matrix for every $a \in \Sigma$. The next result shows that a PA is reversible if and only if it is a reversible DA (Gudder, 2000).

**Lemma 3.5.** *If A and B are stochastic $n \times n$ matrices with $AB = I$, then A and B are 0–1 unitary matrices.*

Putting the previous results together, we have the following theorem.

**Theorem 3.6.** *If M is a PA then the following statements are equivalent.* (a) *M is reversible.* (b) *M is a reversible DA.* (c) *The evolution operators $U(a)$ for M are unitary.*

Let $M = (S, \Sigma, \delta, s_0, F)$ be a PA and let $w \in \Sigma^*$. Lemma 3.3 shows that

$$U(w)\hat{s}_0 = \sum_{t \in S} \lambda_t^w \hat{t}$$

is a probability vector so that $\sum_{t \in S} \lambda_t^w = 1$, $\lambda_t^w \geq 0$. We write

$$p(F \mid w) = \sum_{t \in F} \lambda_t^w$$

and interpret $p(F \mid w)$ as the probability that $M$ ends up in a final state when fed the string $w$. We say that $w$ is **accepted with probability greater than** $\eta$ if $p(F \mid w) > \eta$. The set of all strings accepted by $M$ with probability greater than $\eta$ is the $\eta$-**language** for $M$. It can be shown that every regular language is an $\eta$-language for some PA for every $0 \leq \eta < 1$ (Paz, 1971). Moreover, there are $\eta$-languages for $0 < \eta < 1$ that are not regular (Paz, 1971). This shows that PA are more powerful than DA. However, unlike the quantum automata that will be considered next, PA are theoretical machines that cannot be efficiently implemented in general (Dwork and Stockmeyer, 1990).

## 4. REVERSIBLE LANGUAGES

A regular language over $\Sigma$ is **reversible** if for every $x \in \Sigma^*$ there exists a $y \in \Sigma^*$ such that $uv \in L$ if and only if $uxyv \in L$. In a certain sense any string $x$ has a **canceling** string $y$ relative to $L$. We denote the set of reversible languages over $\Sigma$ by Rev($\Sigma$).

**Lemma 4.1.** *If $\emptyset \neq L \in$ Rev($\Sigma$) then every $x \in \Sigma^*$ is a prefix of a string in $L$.*

**Proof:** Let $z \in L$ and let $y$ be a canceling string for $x$ relative to $L$. Then $xyz \in L$ because $z \in L$. □

It follows from Lemma 4.1 that every nonempty $L \in$ Rev($\Sigma$) is infinite. Thus, $F(\Sigma) \cap$ Rev$(\Sigma) = \{\emptyset\}$ and since $F(\Sigma) \subseteq R(\Sigma)$ we conclude that Rev($\Sigma$) is properly contained in $R(\Sigma)$. We now prove a result analogous to Theorem 3.1 which says that a language $L$ is accepted by a reversible DA if and only if $L \in$ Rev($\Sigma$).

**Lemma 4.2.** (a) *If $L$ is accepted by a reversible DA then for any $a \in \Sigma$ there exists $n(a) \in \mathbb{N}$ such that for every $x, y \in \Sigma^*$, $xa^{n(a)}y \in L$ if and only if $xy \in L$.* (b) *If $L$ is accepted by a reversible DA then for every $x, y, z \in \Sigma^*$, $xz \approx_L yz$ implies that $x \approx_L y$.* (c) *If $L \in R(\Sigma)$ then $L$ is accepted by a reversible DA if and only if $M_L$ is reversible.*

**Proof:** (a) Let $M = (S, \Sigma, \delta, s_0, F)$ be a reversible DA accepting $L$. Since for fixed $a \in \Sigma$, the map $s \mapsto \delta(s, a)$ is a bijection on $S$, it has finite order in the permutation group on $S$. Let $n(a)$ be the order of this permutation. Then

$$\delta\big(s_0, xa^{n(a)}y\big) = \delta(s_0, xy)$$

for every $x, y \in \Sigma^*$ so the result follows. (b) It is enough to show that $xa \approx_L ya$ implies that $x \approx_L y$ for every $a \in \Sigma$ and $x, y \in \Sigma^*$. Assume that $xa \approx_L ya$ and that $z \in \Sigma^*$. By Part (a) we have $xz \in L$ if and only if $xaa^{n(a)-1}z \in L$. Since $xa \approx_L ya$, the latter condition is equivalent to $yaa^{n(a)-1}z \in L$ which by Part (a) is equivalent to $yz \in L$ Hence, $x \approx_L y$. (c) If $M_L$ is reversible, then clearly $L$ is acepted by a reversible DA. Conversely, suppose $L$ is accepted by a reversible DA.

To show that $M_L$ is reversible suppose that $\delta_L([x]_L, a) = \delta_L([y]_L, a)$ for some $x, y \in \Sigma^*$, $a \in \Sigma$. But then $[xa]_L = [ya]_L$ so that $xa \approx_L ya$. Applying Part (b) we have $x \approx_L y$ and hence, $[x]_L = [y]_L$. □

**Theorem 4.3.** *If $L \in R(\Sigma)$, then the following statements are equivalent.*

(a) *$L$ is accepted by a reversible DA.*
(b) *$M_L$ is reversible.*
(c) *For every $a \in \Sigma$ there exists $n(a) \in \mathbb{N}$ such that for every $x, y \in \Sigma^*$, $xa^{n(a)}y \in L$ if and only if $xy \in L$.*
(d) *For every $x, y, z \in \Sigma^*$, $xz \approx_L yz$ implies that $x \approx_L y$.*
(e) *$L \in \mathrm{Rev}(\Sigma)$.*

**Proof:** That (a)–(d) are equivalent follows from Lemma 4.2 and its proof. Now (c) implies (e) because if $x = a_1 a_2 \cdots a_k$ then we can take a canceling string for $x$ relative to $L$ to be

$$y = a_k^{n(a_k)-1} \cdots a_2^{n(a_2)-1} a_1^{n(a_1)-1}$$

We now show that (e) implies (d). Suppose that $L \in \mathrm{Rev}(\Sigma)$ and that $xz \approx_L yz$ for some $x, y, z \in \Sigma^*$. Let $v$ be a canceling string for $z$ relative to $L$. Since $xz \approx_L yz$ we have $xzvw \in L$ if and only if $yzvw \in L$ for every $w \in \Sigma^*$. It follows that $xw \in L$ if and only if $yw \in L$ for every $w \in \Sigma^*$. Hence, $x \approx_L y$. □

Since $\mathrm{Rev}(\Sigma)$ is properly contained in $R(\Sigma)$, we conclude from Theorem 4.3 that DA are more powerful than reversible DA. For example, if $\emptyset \neq L \in F(\Sigma)$, then $L$ is accepted by a DA but not by a reversible DA.

**Corollary 4.4.** (a) *If $L \in \mathrm{Rev}(\Sigma)$, then $L^R \in \mathrm{Rev}(\Sigma)$.* (b) *If $\emptyset \neq L \in \mathrm{Rev}(\Sigma)$, then every $x \in \Sigma^*$ is a suffix of a string in $L$.*

**Proof:** (a) If $L \in \mathrm{Rev}(\Sigma)$, then $L \in R(\Sigma)$ so $L^R \in R(\Sigma)$. For $a \in \Sigma$ there exists $n(a) \in \mathbb{N}$ satisfying Theorem 4.3(c). Now $xy \in L^R$ if and only if $y^R x^R \in L$. By Theorem 4.3(c) this latter condition is equivalent to $y^R a^{n(a)} x^R \in L$ which is equivalent to $xa^{n(a)}y \in L^R$. The result follows from Theorem 4.3(c). (b) Since $L^R \in \mathrm{Rev}(\Sigma)$, by Lemma 4.1 there exists $y \in \Sigma^*$ such that $x^R y \in L^R$. But then $y^R x \in L$. □

Corollary 4.4 shows that $\mathrm{Rev}(\Sigma)$ is closed under reversal. It is shown in Gudder (2000) that $\mathrm{Rev}(\Sigma)$ is closed under union, intersection, and complementation. We now investigate whether $\mathrm{Rev}(\Sigma)$ is closed under concatenation and Kleene star.

*Example 4.1.* Let $\Sigma = \{a, b\}$ and let $L_1 \subseteq \Sigma^*$ be the language given by

$$L_1 = \{w \in \Sigma^* : w \text{ has an odd number of } a\text{'s}\}$$

We will now show that $L_1 \in \text{Rev}(\Sigma)$. We accomplish this by producing a reversible DA $M_1$ that accepts $L_1$. This DA is given by $M_1 = (S, \Sigma, \delta, s_0, F)$ where $S = \{s_0, s_1\}$, $F = \{s_1\}$ and $\delta(s_0, a) = s_1$, $\delta(s_0, b) = s_0$, $\delta(s_1, a) = s_0$, $\delta(s_1, b) = s_1$. Another way to show that $L_1 \in \text{Rev}(\Sigma)$ is to employ Theorem 4.3(c). First, $L_1 \in R(\Sigma)$ because $L_1 = b^*ab^*(b^*ab^*ab^*)^*$. Let $n(a) = 2$, $n(b) = 1$. Since $xa^2y \in L$ if and only if $xy \in L$ and $xby \in L$ if and only if $xy \in L$ we conclude that $L_1 \in \text{Rev}(\Sigma)$.

An argument similar to that in Example 4.1 shows that $L_2 \in \text{Rev}(\Sigma)$ where

$$L_2 = \{w \in \Sigma^* : |w| \text{ to even}\}$$

In this case $n(a) = n(b) = 2$. Similarly, $L_3 \in \text{Rev}(\Sigma)$ where

$$L_3 = \{w \in \Sigma^* : w \text{ has an even number of } a\text{'s}\}$$

The next result shows that, in general, $\text{Rev}(\Sigma)$ is not closed under concatenation and Kleene star.

**Theorem 4.5.** *If $L_1$ is the language of Example 4.1, then*

$$\text{(a) } L_1L_1 \notin \text{Rev}(\Sigma), \quad \text{(b) } L_1^* \notin \text{Rev}(\Sigma).$$

**Proof:** (a) Suppose that $L_1L_1 \in \text{Rev}(\Sigma)$. Applying Theorem 4.3(c), there exists $n(a) \in \mathbb{N}$ such that $xa^{n(a)}y \in L_1L_1$ if and only if $xy \in L_1L_1$. Now $aa \in L_1L_1$ so $aa^{n(a)}a \in L_1L_1$. Now $n(a)$ must be even because $aa^{n(a)}a$ must contain an even number of $a$'s. But then $ba^{n(a)}b \in L_1L_1$ so that $bb \in L_1L_1$ and this is a contradiction. (b) It is easy to check that

$$\begin{aligned} L_1^* &= \{w \in \Sigma^* : w = e \text{ or } w(i) = a \text{ for some } i \in \mathbb{N}\} \\ &= \{e\} \cup \Sigma^* a \Sigma^* \end{aligned}$$

Suppose $L_1^* \in \text{Rev}(\Sigma)$. Since $ba^{n(a)}b \in L_1^*$, by Theorem 4.3(c) we have $bb \in L_1^*$. But this is a contradiction. □

## 5. QUANTUM LANGUAGES

In the sequel, $H$ will denote a finite-dimensional complex Hilbert space with unit sphere $\hat{H}$. We denote the set of unitary operators on $H$ by $\mathcal{U}(H)$. A $q$-**automaton** is a quintuple $M = (H, \Sigma, U, s_0, F)$ where $\Sigma$ is an alphabet, $U : \Sigma \to \mathcal{U}(H)$, $s_0 \in \hat{H}$, and $F$ is a subspace of $H$. We extend $U$ to a map from

$\Sigma^*$ into $\mathcal{U}(H)$ as follows. If $w = a_1 a_2 \cdots a_n \in \Sigma^*$ we define

$$U(w) = U(a_n) \cdots U(a_2)U(a_1)$$

and $U(e) = I$. Of course, this makes sense because the product of unitary operators is unitary.

We interpret $\hat{H}$ as the state space for $M$, $s_0 \in \hat{H}$ is the **start state** (or **initial state**) of $M$ and $F$ is the **final subspace** for $M$. We call $U(w)$ the **evolution operator** of $M$ for $w \in \Sigma^*$ and interpret $U(w)s_0$ as the state in which $M$ finds itself after being fed the string $w$. The **probability that** $M$ **reaches** $s \in \hat{H}$ when fed $w \in \Sigma^*$ is

$$p_M(s \mid w) = |\langle U(w)s_0, s\rangle|^2$$

Denoting the orthogonal projection onto $F$ by $P(F)$ the **probability that** $M$ **reaches** the final subspace $F$ when fed $w \in \Sigma^*$ is given by

$$p_M(F \mid w) = \|P(F)U(w)s_0\|^2$$

We say that $w \in \Sigma^*$ is **accepted** by $M$ if $p_M(F \mid w) = 1$ and define

$$L(M) = \{w \in \Sigma^* : p_M(F \mid w) = 1\}$$

A language $L$ is a **quantum language** if $L = L(M)$ for some $q$-automaton $M$. We denote the set of all quantum languages over $\Sigma$ by $Q(\Sigma)$.

It is shown in Gudder (2000) that if $L_1, L_2 \in Q(\Sigma)$, then $L_1 \cup L_2 \in Q(\Sigma)$ and $L_1 \cap L_2 \in Q(\Sigma)$ so that $Q(\Sigma)$ is closed under union and intersection. The next result shows that $Q(\Sigma)$ is closed under reversal.

**Theorem 5.1.** *If $L \in Q(\Sigma)$, then $L^R \in Q(\Sigma)$.*

**Proof:** Let $L = L(M)$ for a $q$-automaton $M = (H, \Sigma, U, s_0, F)$ where $F \neq \{0\}$. Let $\dim F = n$ and let $\mathcal{P}$ be the set of all projections on $H$ of dimension $n$. Let $H'$ be the set of all complex linear combinations of elements of $\mathcal{P}$. Then $H'$ is a finite-dimensional linear space because $H'$ is a subspace of the finite-dimensional linear space of all operators on $H$. Define an inner product on $H'$ by $\langle A, B\rangle_1 = \operatorname{tr}(AB^*)$. For every $a \in \Sigma$ define $U'(a) : H' \to H'$ by $U'(a)A = U(a)^* AU(a)$. Then $U'(a)$ is unitary because

$$\begin{aligned}\|U'(a)A\|_1^2 &= \operatorname{tr}(U(a)^* AU(a)U(a)^* A^* U(a)) = \operatorname{tr}(U(a)^* AA^* U(a))\\ &= \operatorname{tr}(AA^*) = \|A\|_1^2\end{aligned}$$

We extend $U'$ to a map from $\Sigma^*$ into $\mathcal{U}(H')$ as before. Note that $U'(w^R)A = U(w)^* AU(w)$. Indeed, if $w = a_1 a_2 \cdots a_k$ we have

$$\begin{aligned}U'(w^R)A &= U'(a_1) \cdots U'(a_k)\, A = U(a_1)^* \cdots U(a_k)^* AU(a_k) \cdots U(a_1)\\ &= U(w)^* AU(w)\end{aligned}$$

Form the $q$-automaton $M' = (H', \Sigma, U', s_0', F')$ where $s_0' = P(F)/\sqrt{n}$ and

$$F' = \operatorname{span}\{P \in \mathcal{P} : Ps_0 = s_0\}$$

Suppose that $w \in L$. We then have $P(F)U(w)s_0 = U(w)s_0$. Now

$$U'(w^R)s_0' = \frac{1}{\sqrt{n}}U(w)^*P(F)U(w)$$

and $U(w)^*P(F)U(w) \in \mathcal{P}$ with $U(w)^*P(F)U(w)s_0 = s_0$. Hence, $U'(w^R)s_0' \in F'$ so that $w^R \in L(M')$. Conversely, suppose that $w \in L(M')$. Then $U'(w)s_0' = 1/\sqrt{n}P$ where $P \in \mathcal{P}$ with $Ps_0 = s_0$. Since

$$\sqrt{n}U'(w)s_0' = U(w^R)^*P(F)U(w^R)$$

we have

$$U(w^R)^*P(F)U(w^R)s_0 = s_0$$

Hence, $P(F)U(w^R)s_0 = U(w^R)s_0$ so that $w^R \in L$. Thus, $w = (w^R)^R$ where $w^R \in L$ so that $L(M') = L^R$. $\square$

We now compare $Q(\Sigma)$ with the classical languages $R(\Sigma)$ and $\operatorname{Rev}(\Sigma) \subseteq R(\Sigma)$. First, if $L \in \operatorname{Rev}(\Sigma)$ then by Theorem 4.3, $L$ is accepted by a reversible DA $M$. By Lemma 3.2 the corresponding operators $U(a)$ are unitary for every $a \in \Sigma$. It follows that $M$ can be considered to be a $q$-automaton whose final subspace is the span of $F$. Hence, $L \in Q(\Sigma)$ and we conclude that $\operatorname{Rev}(\Sigma) \subseteq Q(\Sigma)$. To compare $Q(\Sigma)$ and $R(\Sigma)$, we first give some examples of quantum languages. Our initial example shows that singleton strings are quantum languages.

*Example 5.1.* If $\Sigma = \{a_1, \ldots, a_n\}$, then $\{a_i\} \in Q(\Sigma)$, $i = 1, \ldots, n$.

**Proof:** Form the $q$-automaton $M = (H, \Sigma, U, s_0, F)$ with $H = \mathbb{C}^{2n}$

$$s_0 = (2n)^{-1/2}(1, 1, \ldots, 1)$$

$s_1 = U(a_1)s_0$, $F = \operatorname{span}\{s_1\}$, $\theta = \sqrt{2}\pi$ and

$$U(a_1) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 & \cdots & 0 \\ \sin\theta & \cos\theta & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$\vdots$$

$$U(a_n) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & \\ 0 & 1 & 0 & \cdots & 0 & \\ & \vdots & & & & \\ 0 & 0 & 0 & \cdots & \cos\theta & -\sin\theta \\ 0 & 0 & 0 & \cdots & \sin\theta & \cos\theta \end{bmatrix}$$

It is easy to check that $L(M) = \{a_1\}$ so that $\{a_1\} \in Q(\Sigma)$. A similar construction shows that $\{a_i\} \in Q(\Sigma)$, $i = 1, \ldots, n$. □

If we take $F = \text{span}\{s_0\}$ in Example 5.1, we conclude that $\{e\} \in Q(\Sigma)$. The next example shows that a string of length two is a quantum language.

*Example 5.2.* If $\Sigma = \{a, b\}$, then $\{ab\} \in Q(\Sigma)$.

**Proof:** Form the $q$-automaton $M = (H, \Sigma, U, s_0, F)$ with $H = \mathbb{C}^3$, $s_0 = (1, 0, 0)$, $s_1 = U(b)U(a)s_0$, $F = \text{span}\{s_1\}$, $\theta = \sqrt{2}\pi$ and

$$U(a) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$U(b) = \begin{bmatrix} \cos\theta & 0 & -\sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & \cos\theta \end{bmatrix}$$

It is easy to check that $L(M) = \{ab\}$. □

A straightforward extension of Example 5.2 shows that any string is a quantum language. Since $Q(\Sigma)$ is closed under union, we conclude that $F(\Sigma) \subseteq Q(\Sigma)$. It is shown in Gudder (2000) that the nonregular languages $L_2$ and $L_3$ of Section 2 are quantum languages so that $Q(\Sigma) \nsubseteq R(\Sigma)$.

The proof of the following lemma appears in Moore and Crutchfield (in press). We now give a different proof.

**Lemma 5.2.** *If $U \in \mathcal{U}(H)$ and $\varepsilon > 0$ then there exists $k \in \mathbb{N}$ such that $\|U^k - I\| < \varepsilon$.*

**Proof:** Since $H$ is finite dimensional, the unit sphere $B(H)^\wedge$ in the set of (bounded) operators $B(H)$ on $H$ is compact and $\{U^j : j \in \mathbb{N}\} \subseteq B(H)^\wedge$. Hence, there exists a subsequence $U^{j'}$ that converges in $B(H)^\wedge$. Since $U^{j'}$ is Cauchy, there exist $j, k \in \mathbb{N}$, $j \neq k$ such that $\|U^j - U^k\| < \varepsilon$. Now for every $U \in \mathcal{U}(H)$

we have $\|UA\| = \|A\|$ for every $A \in B(H)$. Indeed,

$$\|UA\| = \sup_{\|\psi\|=1} \|UA\psi\| = \sup_{\|\psi\|=1} \langle UA\psi, UA\psi\rangle^{1/2}$$
$$= \sup_{\|\psi\|=1} \langle A\psi, A\psi\rangle^{1/2} = \sup_{\|\psi\|=1} \|A\psi\| = \|A\|$$

Thus, if $j < k$ we have

$$\|U^{k-j} - I\| = \|U^j(U^{k-j} - I)\| = \|U^k - U^j\| < \varepsilon \qquad \square$$

**Corollary 5.3.** *Let $M = (H, \Sigma, U, s_0, F)$ be a $q$-automaton. For any $\varepsilon > 0$ and $w \in \Sigma^*$ there exists $k \in \mathbb{N}$ such that*

$$\|U(uw^kv) - U(uv)\| < \varepsilon \tag{5.1}$$

*for every $u, v \in \Sigma^*$.*

**Proof:** Applying Lemma 5.2 there exists $k \in \mathbb{N}$ such that $\|U(w)^k - I\| < \varepsilon$. Hence,

$$\begin{aligned}\|U(uw^kv) - U(uv)\| &= \|U(v)U(w)^kU(u) - U(v)U(u)\|\\ &= \|U(v)[U(w)^k - I]U(u)\|\\ &\leq \|U(w)^k - I\| < \varepsilon \qquad \square\end{aligned}$$

The next result is called the quantum pumping theorem [14].

**Theorem 5.4.** *Let $L \in Q(\Sigma)$ and let $u, v, w \in \Sigma^*$. If $uv \notin L$, then there exists $k \in \mathbb{N}$ such that $uw^kv \notin L$.*

**Proof:** Suppose that $L = L(M)$ for a $q$-automaton $M = (H, \Sigma, U, s_0, F)$. Since $\|P(F)U(uv)s_0\| < 1$ there exists $\varepsilon > 0$ such that $\|P(F)U(uv)s_0\| < 1 - \varepsilon$. By Corollary 5.3 there exists $k \in \mathbb{N}$ such that Eq. (5.1) holds. We then have

$$\begin{aligned}\|P(F)U(uw^kv)s_0\| &\leq \|P(F)U(wv)s_0\| + \|P(F)U(uw^kv)s_0 - P(F)U(uv)s_0\|\\ &\leq 1 - \varepsilon + \|U(uw^kv)s_0 - U(uv)s_0\| < 1 - \varepsilon + \varepsilon = 1\end{aligned}$$

Hence, $uw^kv \notin L$. $\square$

*Example 5.3.* For $\Sigma = \{a\}$, the regular language

$$L_1 = \{a^n \in \Sigma^* : n = 0, 2, 3, \ldots\} \notin Q(\Sigma)$$

**Proof:** Since $\{a\} \subseteq \Sigma^*$ is regular and $R(\Sigma)$ is closed under complementation, $L_1 = \Sigma^* \smallsetminus \{a\} \in R(\Sigma)$. Now suppose that $L_1 \in Q(\Sigma)$. Since $a \notin L_1$, by Theorem 5.4 there exists $k \in \mathbb{N}$ such that $aa^k \notin L_1$. This is a contradiction. □

It follows from Example 5.3 that $R(\Sigma) \not\subseteq Q(\Sigma)$. Also $\{a\} \in Q(\Sigma)$ but $L_1 = \Sigma^* \smallsetminus \{a\} \notin Q(\Sigma)$ so $Q(\Sigma)$ is not closed under complementation. Moreover, $\{a^2, a^3\} \in Q(\Sigma)$ but $\{a^2, a^3\}^* = L_1 \notin Q(\Sigma)$ so $Q(\Sigma)$ is not closed under Kleene star. Finally, we have seen in Section 4 that

$$L_2 = \{e, a^2, a^4, \ldots\} \in \mathrm{Rev}(\Sigma)$$

so that $L_2 \in Q(\Sigma)$. Now $L_3 = \{e, a^3\} \in Q(\Sigma)$ but $L_2 L_3 = L_1 \notin Q(\Sigma)$. Hence, $Q(\Sigma)$ is not closed under concatenation. We summarize our findings in the following theorem.

**Theorem 5.5.** (a) $F(\Sigma) \cup \mathrm{Rev}(\Sigma) \subseteq R(\Sigma) \cap Q(\Sigma)$. (b) $R(\Sigma) \not\subseteq Q(\Sigma)$ *and* $Q(\Sigma) \not\subseteq R(\Sigma)$. (c) $Q(\Sigma)$ *is closed under union, intersection and reversal but is not closed under complementation, concatenation, or Kleene star.*

For a string $w$ to be accepted by a $q$-automaton $M$, we must have $p_M(F \mid w) = 1$. This requirement is sometimes relaxed and we say that $w \in \Sigma^*$ is $\eta$-**accepted** by $M$, where $0 \leq \eta < 1$ if $p_M(F \mid w) > \eta$. The set of all strings $L_\eta(M)$ that are $\eta$-accepted by $M$ is the **language** $\eta$-**accepted** by $M$. A language $L$ is $\eta$-**quantum** if $L = L_n(M)$ for some $q$-automaton $M$ and we denote the set of $\eta$-quantum languages over $\Sigma$ by $Q_\eta(\Sigma)$, $0 \leq \eta < 1$. The following result is proved in Gudder (2000, 2000a).

**Theorem 5.6.** (a) $Q_0(\Sigma) \subseteq Q_\eta(\Sigma)$ *for* $0 \leq \eta < 1$. (b) $Q_\eta(\Sigma) = Q_{\eta'}(\Sigma)$ *for all* $0 < \eta, \eta' < 1$.

Since the languages $Q_\eta(\Sigma)$ $0 < \eta < 1$ are all the same we now have three types of quantum languages: $Q_0(\Sigma)$, $Q_\eta(\Sigma)$, and $Q(\Sigma)$. The author does not know whether the inclusion $Q_0(\Sigma) \subseteq Q_\eta(\Sigma)$, $0 < \eta < 1$, is proper. It is clear that $\mathrm{Rev}(\Sigma)$ is contained in all of these languages. It can be shown that $Q_0(\Sigma)$ is closed under union and intersection (Gudder, 2000) but we do not know whether $Q_\eta(\Sigma)$ is closed under these operations for $0 < \eta < 1$. It can also be shown that $Q_\eta(\Sigma)$ is not closed under complementation (Gudder, 2000) but we do not know whether $Q_\eta(\Sigma)$ is closed under concatenation, Kleene star, or reversal, $0 \leq \eta < 1$. The next theorem summarizes other known properties of $Q_\eta(\Sigma)$, $0 < \eta < 1$ (Gudder, 2000).

**Theorem 5.7.** (a) $Q_\eta(\Sigma) \cap F(\Sigma) = \{\emptyset\}$. (b) $L \in Q(\Sigma)$ *if and only if* $\Sigma^* \smallsetminus L \in Q_0(\Sigma)$. (c) $Q(\Sigma)$, $Q_\eta(\Sigma)$ *and* $R(\Sigma)$ *are mutually incomparable (none is contained in any of the others).*

## 6. CHARACTERIZATION OF QUANTUM LANGUAGES

We have defined $Q(\Sigma)$ to be the set of languages accepted by $q$-automaton over the alphabet $\Sigma$. We now present an internal characterization of this class of languages. Our result shows that $L \in Q(\Sigma)$ if and only if $L$ admits a transition amplitude function satisfying a certain condition.

Let $S = \{x_1, \ldots, x_n\}$ be a finite nonempty set. A map $\phi : S \times S \to \mathbb{C}$ is **positive-definite** if for every $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ we have

$$\sum_{i,j=1}^{n} \alpha_i \alpha_j^* \phi(x_i, x_j) \geq 0 \tag{6.1}$$

and if equality holds in Eq. (6.1) then $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

**Lemma 6.1.** *Let $\phi : S \times S \to \mathbb{C}$ be positive-definite.* (a) $\phi(x_i, x_j) = \phi(x_j, x_i)^*$ *for every $i$, $j$.* (b) *If*

$$\sum_{i=1}^{n} \alpha_i \phi(x_i, x_j) = \sum_{i=1}^{n} \beta_i \phi(x_i, x_j)$$

*for every $j$, then $\alpha_i = \beta_i$ for every $i$.*

**Proof:** (a) It follows from Eq. (6.1) that $\phi(x_i, x_i) \geq 0$ so the result holds for $i = j$. For $i \neq j$ we prove the result for $\phi(x_1, x_2)$ and the other cases are similar. Letting $\alpha_1 = \alpha_2 = 1$, $\alpha_i = 0$, $i \neq 1, 2$, we have by Eq. (6.1) that

$$\phi(x_1, x_1) + \phi(x_2, x_2) + \phi(x_1, x_2) + \phi(x_2, x_1) \geq 0$$

Hence, $\phi(x_1, x_2) + \phi(x_2, x_1) \in \mathbb{R}$ so that $\operatorname{Im} \phi(x_1, x_2) = -\operatorname{Im} \phi(x_2, x_1)$. Letting $\alpha_1 = 1$, $\alpha_2 = i$, $\alpha_i = 0$, $i \neq 1, 2$, we have by Eq. (6.1) that

$$\phi(x_1, x_1) + \phi(x_2, x_2) - i\phi(x_1, x_2) + i\phi(x_2, x_1) \geq 0$$

Hence, $-i\phi(x_1, x_2) + i\phi(x_2, x_1) \in \mathbb{R}$ so that $\operatorname{Re} \phi(x_1, x_2) = \operatorname{Re}(x_2, x_1)$ and the result follows. (b) By assumption we have

$$\sum_{i=1}^{n} (\alpha_i - \beta_i) \phi(x_i, x_j) = 0$$

for every $j$. Hence,

$$\sum_{i,j=1}^{n} (\alpha_i - \beta_i)(\alpha_j - \beta_j)^* \phi(x_i, x_j) = 0$$

Since $\phi$ is positive-definite, we have $\alpha_i = \beta_i$ for every $i$. □

We say that $\phi : \Sigma^* \times \Sigma^* \to \mathbb{C}$ is a **transition amplitude** on $\Sigma^*$ if there exists a finite subset $B = \{x_1, \ldots, x_n\} \subseteq \Sigma^*$ with $x_1 = e$ such that the following conditions hold.

(A1) $\phi : B \times B \to \mathbb{C}$ is positive-definite.

(A2) For every $a \in \Sigma$, $\phi(x_i a, x_j a) = \phi(x_i, x_j)$ for every $i, j$.

(A3) For every $x \in \Sigma^*$ there exists $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that

$$\phi(xa, y) = \sum_{i=1}^{n} \alpha_i \phi(y, x_i a)^*$$

for every $y \in \Sigma^*$ and $a \in \Sigma \cup \{e\}$.

We say that $L \subseteq \Sigma^*$ is an **amplitude language** over $\Sigma$ if there exists a transition amplitude $\phi$ on $\Sigma^*$ such that

(A4) If $\phi(w, x_j) = \sum_{i=1}^{m} \alpha_i \phi(y_i, x_j)$ for every $j$ where $y_1, \ldots, y_m \in L$, then $w \in L$.

**Theorem 6.2.** *$L \in Q(\Sigma)$ if and only if $L$ is an amplitude language over $\Sigma$.*

**Proof:** Suppose that $L \in Q(\Sigma)$. Then $L = L(M)$ for some $q$-automaton $M = (H, \Sigma, U, s, F)$. Define $\phi : \Sigma^* \times \Sigma^* \to \mathbb{C}$ by $\phi(x, y) = \langle U(x)s, U(y)s\rangle$. Let

$$H' = \operatorname{span}\{U(x)s : x \in \Sigma^*\}$$

and let $U(x_i)s$ be a basis for $H'$, $i = 1, \ldots, n$ with $x_1 = e$. Define $B = \{x_1, \ldots, x_n\} \subseteq \Sigma^*$. To show that $\phi : B \times B \to \mathbb{C}$ is positive-definite we have for every $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ that

$$\begin{aligned}\sum_{i,j=1}^{n} \alpha_i \alpha_j^* \phi(x_i, x_j) &= \sum_{i,j=1}^{n} \alpha_i \alpha_j^* \langle U(x_i)s, U(x_j)s\rangle \\ &= \left\langle \sum \alpha_i U(x_i)s, \sum \alpha_j U(x_j)s \right\rangle \\ &= \left\| \sum \alpha_j U(x_i)s \right\|^2 \geq 0\end{aligned}$$

Moreover, if equality holds, then $\sum \alpha_i U(x_i)s = 0$ and since the $U(x_i)s$ are linearly independent, we have $\alpha_1 = \cdots = \alpha_n = 0$. For (A2) we have

$$\begin{aligned}\phi(x_i a, x_j a) &= \langle U(x_i a)s, U(x_j a)s\rangle = \langle U(a)U(x_i)s, U(a)U(x_j)s\rangle \\ &= \langle U(x_i)s, U(x_j)s\rangle = \phi(x_i, x_j)\end{aligned}$$

To prove (A3), let $x \in \Sigma^*$. Since $U(x_i)s$ is a basis for $H'$, there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that $U(x)s = \sum \alpha_i U(x_i)s$. Hence, for every $y \in \Sigma^*$, $a \in \Sigma \cup \{e\}$

we have

$$\begin{aligned}\phi(xa, y) &= \langle U(xa)s, U(y)s\rangle = \sum \alpha_i \langle U(a)U(x_i)s, U(y)s\rangle \\ &= \sum \alpha_i \langle U(y)s, U(x_i a)s\rangle^* = \sum \alpha_i \phi(y, x_i a)^*\end{aligned}$$

To prove (A4), suppose that $\phi(w, x_j) = \sum \alpha_i \phi(y_i, x_j)$ for every $j$ where $y_i, \dots, y_m \in L$. We then have

$$\begin{aligned}\langle U(w)s, U(x_j)s\rangle &= \sum \alpha_i \langle U(y_i)s, U(x_j)s\rangle \\ &= \left\langle \sum \alpha_i U(y_i)s, U(s_j)s\right\rangle\end{aligned}$$

for every $j$. Since $U(x_j)s$ is a basis for $H'$, we conclude that $U(w)s = \sum \alpha_i U(y_i)s \in F$ and hence $w \in L$.

Conversely, suppose that $L$ is an amplitude language over $\Sigma$ with transition amplitude $\phi' : \Sigma^* \times \Sigma^* \to \mathbb{C}$ and $B = \{x_1, \dots, x_n\} \subseteq \Sigma^*$. Since $\phi'$ is positive-definite, we have $\phi'(e, e) > 0$. Hence, $\phi(x, y) = \phi'(x, y)/\phi'(e, e)$ satisfies (A1)–(A4). If $x, y \in \Sigma^*$, then it follows from (A3) that there exist $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ and $\beta_1, \dots, \beta_n \in \mathbb{C}$ such that $\phi(x, y) = \sum \alpha_i \phi(y, x_i)^*$ and for every $i$ we have $\phi(y, x_i) = \sum \beta_j \phi(x_i, x_j)^*$. Hence,

$$\phi(x, y) = \sum_{i,j=1}^{n} \alpha_i \beta_j^* \phi(x_i, x_j) \tag{6.2}$$

Applying Lemma 6.1 we have $\phi(y, x) = \sum \beta_j \phi(x, x_j)^*$. Since $\phi(x, x_j)^* = \sum \alpha_i^* \phi(x_j, x_i)$ we conclude that

$$\phi(y, x) = \sum_{i,j=1}^{n} \beta_j \alpha_i^* \phi(x_j, x_i) = \phi(x, y)^*$$

Define $f : \Sigma^* \to \mathbb{C}^n$ by $f(x) = (\alpha_1, \dots, \alpha_n)$ where $\alpha_i$ are the unique scalars satisfying (A3). For $x, y \in \Sigma^*$ define $x \sim y$ if $\phi(x, x_i) = \phi(y, x_i)$ for every $i \in \{1, \dots, n\}$. Then $\sim$ is an equivalence relation and we denote the equivalence class containing $x$ by $[x]$. If $x \sim y$ and $f(x) = (\alpha_1, \dots, \alpha_n)$, $f(y) = (\beta_1, \dots, \beta_n)$ we have by (A3) that

$$\sum \alpha_i \phi(x_i, x_j) = \phi(x, x_j) = \phi(y, x_j) = \sum \beta_i \phi(x_i, x_j)$$

for every $j$. Applying Lemma 6.1(b) we conclude that $\alpha_i = \beta_i$, $i = 1, \dots, n$, so that $f(x) = f(y)$. Conversely, if $f(x) = f(y)$ then $x \sim y$. It follows that the function $g : \Sigma^*/\sim \to \mathbb{C}^n$ given by $g([x]) = f(x)$ is well-defined and is injective.

Let $H$ be the free complex linear space with generators $[x], \dots, [x_n]$. If $g([x]) = (\alpha_1, \dots, \alpha_n)$ we identify $[x]$ with $\sum \alpha_i [x_i]$ and write $[x] = \sum \alpha_i [x_i]$.

If $\psi = \sum \alpha_i [x_i]$ and $\psi' = \sum \beta_i [x_i]$ we define

$$\langle \psi, \psi' \rangle = \sum_{i,j=1}^{n} \alpha_i \beta_j^* \phi(x_i, x_j)$$

It follows from the positive definiteness of $\phi$ that $\langle \psi, \psi \rangle \geq 0$ for every $\psi \in H$ and that $\langle \psi, \psi \rangle = 0$ implies that $\psi = 0$. Hence, $\langle \cdot, \cdot \rangle$ is positive-definite. Moreover, from Eq. (6.2) we have that $\langle [x], [y] \rangle = \phi(x, y)$ for every $x, y \in \Sigma^*$. For any $c \in \mathbb{C}$ we have

$$\langle c\psi, \psi' \rangle = \sum_{i,j} c\alpha_i \beta_j^* \phi(x_i, x_j) = c \sum_{i,j} \alpha_i \beta_j^* \phi(x_i, x_j) = c\langle \psi, \psi' \rangle$$

In a similar way, for every $\psi_1, \psi_2 \in H$ we have

$$\langle \psi_1 + \psi_2, \psi \rangle = \langle \psi_1, \psi \rangle + \langle \psi_2, \psi \rangle$$

Finally, by Lemma 6.1 we have

$$\langle \psi, \psi' \rangle = \left( \sum_{i,j} \beta_j \alpha_i^* \phi(x_j, x_i) \right)^* = \langle \psi', \psi \rangle^*$$

so $\langle \cdot, \cdot \rangle$ is an inner product on $H$ making $H$ a Hilbert space of dimension $n$.

For $a \in \Sigma$, define $U(a)[x_i] = [x_i a]$ and extend $U(a)$ to $H$ by linearity. To show that $U(a)$ is well-defined, suppose that $x \sim y$. Applying (A3) we have

$$\phi(xa, x_j) = \sum \alpha_i \phi(x_i a, x_j) = \phi(yz, x_j)$$

for every $j$ and hence $xa \sim ya$. We now show that $U(a)[x] = [xa]$ for every $x \in \Sigma^*$, $a \in \Sigma$. Applying (A3), for every $j \in \{1, \ldots, n\}$ we have

$$\begin{aligned} \langle [xa], [x_j] \rangle = \phi(xa, x_j) &= \sum \alpha_i \phi(x_i a, x_j) = \sum \alpha_i \langle [x_i a], [x_j] \rangle \\ &= \sum \alpha_i \langle U(a)[x_i], [x_j] \rangle = \langle U(a)[x], [x_j] \rangle \end{aligned}$$

and the result follows. We also conclude that $U(y)[x] = [xy]$ for every $y \in \Sigma^*$. Now $U(a) \in \mathcal{U}(H)$ because by (A2) we have

$$\begin{aligned} \langle U(a)[x_i], U(a)[x_j] \rangle &= \langle [x_i a], [x_j a] \rangle = \phi(x_i a, x_j a) \\ &= \phi(x_i, x_j) = \langle [x_i], [x_j] \rangle \end{aligned}$$

It follows that $\langle U(a)\psi, U(a)\psi' \rangle = \langle \psi, \psi' \rangle$ for every $\psi, \psi' \in H$.

To complete the proof, we let $s = [e]$ and $F = \text{span}\{[y] : y \in L\}$. To show that $F$ is well-defined, suppose that $y \in L$ and $x \sim y$. Then for every $j \in \{1, \ldots, n\}$ we have $\phi(x, x_j) = \phi(y, x_j)$ and it follows from (A4) that $x \in L$. Since $\|e\|^2 = \phi(e, e) = 1$, we conclude that $M = (H, \Sigma, U, s, F)$ is a $q$-automaton. Finally, the following statements are equivalent: $w \in L(M)$, $U(w)s \in F$, $[w] \in F$, $[w] = \sum \alpha_i [y_i]$ where $y_i \in L$, $i = 1, \ldots, m$. But the last equation holds if and only if for every $j \in \{1, \ldots, n\}$ we have

$$\phi(w, x_j) = \langle [w], [x_j] \rangle = \sum \alpha_i \langle [y_i], [x_j] \rangle = \sum \alpha_i \phi(y_i, x_j)$$

Applying (A4), we conclude that $w \in L(M)$ if and only if $w \in L$. Hence, $L = L(M) \in Q(\Sigma)$. □

We can also characterize $R(\Sigma)$ and $\mathrm{Rev}(\Sigma)$ in terms of transition amplitudes. To accomplish this, we need the following definitions. We call $\phi : \Sigma^* \times \Sigma^* \to \mathbb{C}$ a **weak transition amplitude** on $\Sigma^*$ if there exists a finite set $B = \{x_1, \ldots, x_n\} \subseteq \Sigma^*$ with $x_1 = e$ such that (A1) and (A3) hold. We call $L \subseteq \Sigma^*$ a **weak amplitude language** over $\Sigma$ if there exists a weak transition amplitude $\phi$ on $\Sigma^*$ such that (A4) holds. If $\phi : \Sigma^* \times \Sigma^* \to \{0, 1\}$ is a (weak) transition amplitude we call $\phi$ a 0–1 (weak) transition amplitude.

**Theorem 6.3.** (a) $L \in R(\Sigma)$ *if and only if* $L$ *is a weak amplitude language over* $\Sigma$ *with a 0–1 weak transition amplitude* $\phi$ *such that* $\phi(x, y) = 1$ *implies* $\phi(xz, yz) = 1$ *for every* $z \in \Sigma^*$. (b) $L \in \mathrm{Rev}(\Sigma)$ *if and only if* $L$ *is an amplitude language over* $\Sigma$ *with 0–1 transition amplitude.*

**Proof:** (a) Suppose that $L \in R(\Sigma)$ and $M = (S, \Sigma, \delta, s, F)$ is a DA that accepts $L$. Let $S' = \{s_1, \ldots, s_n\}$ be the set of states in $S$ that are reachable with strings in $\Sigma^*$. Then for every $s_i \in S'$ there exists $x_i \in \Sigma^*$ such that $\delta(s, x_i) = s_i$. Of course, $s \in S'$ and we let $s_1 = s$, $x_1 = e$ and $B = \{x_1, \ldots, x_n\}$. Define $\phi : \Sigma^* \times \Sigma^* \to \{0, 1\}$ by $\phi(x, y) = 1$ if $\delta(s, x) = \delta(s, y) \in S'$ and otherwise $\phi(x, y) = 0$. Then $\delta(x_i, x_j) = \delta_{ij}$ for $i, j = 1, \ldots, n$. To prove (A1), let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then

$$\sum_{i,j} \alpha_i \alpha_j^* \phi(x_i, x_j) = \sum_{i,j} \alpha_i \alpha_j^* \delta_{ij} = \sum_i |\alpha_i|^2 \geq 0$$

and if equality holds, we have $\alpha_1 = \cdots = \alpha_n = 0$. Notice that in general (A2) need not hold because we may have $\delta(x_i a, x_j a) = 1$ for $i \neq j$. To prove (A3), for every $x \in \Sigma^*$ there exists $s_i \in S'$ such that $\delta(s, x) = s_i$ so that $\delta(x, x_i) = 1$. But then for every $y \in \Sigma^*$, $a \in \Sigma \cup \{e\}$ we have

$$\phi(xa, y) = \phi(x_i a, y) = \phi(y, x_i a)^*$$

To prove (A4) suppose that for every $j \in \{1, \ldots, n\}$ we have

$$\phi(w, x_j) = \sum_{i=1}^{m} \alpha_i \phi(y_i, x_j) \tag{6.3}$$

where $y_1, \ldots, y_m \in L$. Now there exists $x_j \in B$ such that $\phi(w, x_j) = 1$. Then Eq. (6.3) implies that $\phi(y_i, x_j) = 1$ for some $i \in \{1, 2, \ldots, n\}$. Hence, $s_j \in F$ and $\delta(s, w) = s_j$ so that $w \in L$. Finally, it is clear that if $\phi(x, y) = 1$ then $\phi(xz, yz) = 1$ for every $z \in \Sigma^*$.

Conversely, suppose that $L$ is a weak amplitude language over $\Sigma$ with a 0–1 weak transition amplitude $\phi$ such that $\phi(x, y) = 1$ implies that $\phi(xz, yz) = 1$ for every $z \in \Sigma^*$ and let $B = \{x_1, \ldots, x_n\} \subseteq \Sigma^*$ with $x_1 = e$ be the corresponding finite set. Since $\phi(x_i, x_i) > 0$ we have $\phi(x_i, x_i) = 1$ for every $i$. Also, from the proof of Theorem 6.2 we have that $\phi(x, y) = \phi(y, x)$ for every $x, y \in \Sigma^*$. Letting $\alpha_1 = 1, \alpha_2 = -1$, we have

$$\begin{aligned} 0 < \sum_{i,j=1}^{2} \alpha_i \alpha_j^* \phi(x_i, x_j) &= \phi(x_1, x_1) + \phi(x_2, x_2) - 2\phi(x_1, x_2) \\ &= 2[1 - \phi(x_1, x_2)] \end{aligned}$$

Hence, $\phi(x_1, x_2) = 0$ and in a similar way, $\phi(x_i, x_j) = \delta_{ij}$ for all $i, j$. Moreover, since $\phi(e, e) = 1$ we have

$$\phi(x, x) = \phi(ex, ey) = 1$$

for every $x \in \Sigma^*$. As in the proof of Theorem 6.2, define $f : \Sigma^* \to \mathbb{C}$ by $f(x) = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ when $\phi(x, y) = \sum \alpha_i \phi(x_i, y)$ for every $y \in \Sigma^*$. If $f(x) = (\alpha_1, \ldots, \alpha_n)$ and $f(y) = (\beta_1, \ldots, \beta_n)$ by Eq. (6.2) we have

$$\phi(x, y) = \sum_{i,j} \alpha_i \beta_j^* \phi(x_i, x_j) = \sum_{i,j} \alpha_i \beta_j^* \delta_{ij} = \sum_i \alpha_i \beta_i^* = \langle f(x), f(y) \rangle$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{C}^n$. It follows that $\phi$ is positive semidefinite on any finite subset of $\Sigma^*$. Indeed, suppose that $y_1, \ldots, y_n \in \Sigma^*$ and $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$. Then

$$\begin{aligned} \sum_{i,j} \alpha_i \alpha_j^* \phi(y_i, y_j) &= \sum_{i,j} \alpha_i \alpha_j^* \langle f(y_i), f(y_j) \rangle \\ &= \left\langle \sum \alpha_i f(y_i), \sum \alpha_j f(y_j) \right\rangle \geq 0 \end{aligned}$$

For $x, y \in \Sigma^*$ define $x \sim y$ if $\phi(x, y) = 1$. Then $\sim$ is clearly reflexive and symmetric. To show that $\sim$ is transitive, suppose that $y_1 \sim y_2$ and $y_2 \sim y_3$. Letting $\alpha_1 = \alpha_3 = 1, \alpha_2 = -1$, we have

$$\begin{aligned} 0 \leq \sum_{i,j=1}^{3} \alpha_i \alpha_j^* \phi(y_i, y_j) &= \phi(y_1, y_1) + \phi(y_2, y_2) + \phi(y_3, y_3) - 2\phi(y_1, y_2) \\ &\quad - 2\phi(y_2, y_3) + 2\phi(y_1, y_3) = 2\phi(y_1, y_3) - 1 \end{aligned}$$

Hence, $\phi(y_1, y_3) = 1$ so that $y_1 \sim y_3$. Thus, $\sim$ is an equivalence relation on $\Sigma^*$. Since $\phi(x, y) = 1$ implies $\phi(xz, yz) = 1$, we conclude that $x \sim y$ implies $xz \sim yz$ for every $z \in \Sigma^*$. If $f(x) = (\alpha_1, \ldots, \alpha_n)$ we have

$$1 = \phi(x, x) = \sum \alpha_i \phi(x_i, x)$$

It follows that $\phi(x_i, x) = 1$ for some $i$ and hence $x \sim x_i$. From the transitivity of $\sim$ we conclude that $x \sim x_i$ for a unique $i \in \{1, \ldots, n\}$. Thus, there are precisely $n$ equivalence classes in $\Sigma^*/\sim$. Suppose that $w \sim y$ where $y \in L$. Now there exists a unique $x_i$ such that $y \sim x_i$. Hence, $w \sim x_i$ and

$$\phi(w, x_i) = \phi(y, x_i) = 1$$

It follows from the uniqueness of $x_i$ that

$$\phi(w, x_j) = \phi(y, x_j) = 0$$

for every $j \neq i$. Applying (A4) we have that $w \in L$. We conclude that $L$ is a union of equivalence classes in $\Sigma^*/\sim$ and it follows from the proof of the Myhill-Nerode theorem that $L \in R(\Sigma)$.

(b) Suppose that $L \in \mathrm{Rev}(\Sigma)$ and $M = (S, \Sigma, \delta, s, F)$ is a reversible DA that accepts $L$. Define $\phi$ and $B$ as in the proof of Part (a). Since $L \in R(\Sigma)$, (A1), (A3), (A4) hold and $\phi(x, y) = 1$ implies $\phi(xz, yz) = 1$ for every $z \in \Sigma^*$. It now suffices to show that (A2) holds. If $\phi(x_i a, x_j a) = 0$ then we have that $\phi(x_i, x_j) = 0$. If $\phi(x_i a, x_j a) = 1$ then $\delta(s, x_i a) = \delta(s, x_j a)$. But since $\delta(\cdot, a)$ is injective, we have that $\delta(s, x_i) = \delta(s, x_j)$. Hence, $\phi(x_i, x_j) = 1$.

Conversely, suppose that $L$ is an amplitude language over $\Sigma$ with a 0–1 transition amplitude $\phi$. By the proof of Theorem 6.2 we have $\phi(xz, yz) = \phi(x, y)$ for every $x, y, z \in \Sigma^*$. Hence, $\phi(x, y) = 1$ implies that $\phi(xz, yz) = 1$ so all the conditions of Part (a) are satisfied. Moreover, we have $xa \sim ya$ implies $x \sim y$. As in Part (a) it follows from the proof of the Myhill-Nerode theorem that $L \in \mathrm{Rev}(\Sigma)$. □

We close with a final remark. In quantum computation, superpositions of states are frequently important and this is one of the reasons that quantum computers are more powerful than their classical counterparts. This leads to the question of whether there is a concept of superposition of symbols in the alphabet $\Sigma$ of a $q$-automaton $M$. More generally, we may ask about superposition of strings from an alphabet $\Sigma$. Such a concept exists in a certain sense and is one of the main ideas in the proof of Theorem 6.2. For example, the space $H'$ at the beginning of the proof of Theorem 6.2 can be viewed as a set of superpositions of strings in $\Sigma^*$ that are implemented by unitary operators $U(x)$, $x \in \Sigma^*$. Moreover, such superpositions are employed in the converse proof of Theorem 6.2 to construct the Hilbert space $H$.

## REFERENCES

Benioff, P. (1982a). Quantum Hamiltonian models of Turing machines. *International Journal of Statistical Physics* **29**, 515–546.

Benioff, P. (1982b). Quantum mechanical Hamiltonian models of Turing machines that dissipate no energy. *Physical Reviews Letters* **48**, 1581–1585.

Deutsch, D. (1989). Quantum computational networks. *Proceedings of the Royal Society of London, Series A* **425**, 73–90.

Deutsch, D. and Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London, Series A* **439**, 553–558.

Dwork, C. and Stockmeyer, L. (1990). A time-complexity gap for two-way probabilistic finite state automata. *SIAM Journal of Computing* **19**, 1011–1023.

Feynman, R. (1982). Simulating physics with computers. *International Journal of Theoretical Physics* **21**, 467–488.

Feynman, R. (1986). Quantum mechanical computers. *Foundations of Physics* **16**, 507–531.

Grover, L. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, pp. 212–219.

Gudder, S. (1999). Quantum automata: An overview. *International Journal of Theoretical Physics* **38**, 2259–2280.

Gudder, S. (2000). Quantum languages. In *Current Research in Operational Quantum Logic*, B. Coecke, D. J. Moore, and A. Wilce, eds., Kluwer, The Netherlands, pp. 289–310.

Gudder, S. (2000a). Basic properties of quantum automata. *Foundations of Physics* **30**, 301–319.

Kondacs, A. and Watrous, J. (1997). On the power of quantum finite state automata. In *Proceedings of the 38th IEEE Conference on Foundations of computer Science*, pp. 66–75.

Lewis, H. and Papadimitriou, C. (1998). *Elements of the Theory of Computation*, Prentice Hall, Englewood Cliffs, NJ.

Moore, C. and Crutchfield, J. (in press). Quantum automata and quantum grammars. *Theoretical Computer Science*.

Paz, A. (1971). *Introduction to Probabilistic Automata*, Academic Press, New York.

Shor, P. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing* **26**, 1484–1509.

Simon, D. (1997). On the power of quantum computation. *SIAM Journal of Computing* **26**, 1474–1483.

Williams, C. (1999). *Quantum Computing and Quantum Communication*, Springer, New York.