On One-Dimensional Quantum Cellular Automata

John Watrous*
Computer Sciences Department
University of Wisconsin
Madison, Wisconsin 53706

Abstract

Since Richard Feynman introduced the notion of quantum computation in 1982, various models of "quantum computers" have been proposed. These models include quantum Turing machines and quantum circuits. In this paper we define another quantum computational model, one-dimensional quantum cellular automata, and demonstrate that any quantum Turing machine can be efficiently simulated by a one-dimensional quantum cellular automaton with constant slowdown. This can be accomplished by consideration of a restricted class of one-dimensional quantum cellular automata called one-dimensional partitioned quantum cellular automata. We also show that any one-dimensional partitioned quantum cellular automaton can be simulated by a quantum Turing machine with linear slowdown, but the problem of efficiently simulating an arbitrary one-dimensional quantum cellular automaton with a quantum Turing machine is left open. From this discussion, some interesting facts concerning these models are easily deduced.

1 Introduction

The idea that certain principles of quantum mechanics might be powerful computational tools has led to the study of various theoretical models of quantum computers. The archetypal quantum computer, as introduced by Richard Feynman in [1], is a computer which can simulate quantum physical processes, and which operates in accordance with quantum physical laws. Feynman noted that the problem of simulating quantum physics with a computer based on classical physics appears to be intractable, thereby suggesting that quantum computers may be inherently more powerful than classical computers. David Deutsch later formalized the notion of quantum computation by defining what has become known as the quantum Turing machine (QTM) in [2], and in [3] Ethan Bernstein and Umesh Vazirani, expanding on Deutsch's work, showed that there exists a universal QTM which can simulate any QTM to any required accuracy with at most polynomial slowdown. Another quantum computational model, the quantum circuit, was introduced by Andrew Yao in [4] and shown to be equivalent to the quantum Turing machine.

It is not known whether or not these models are more powerful than their classical analogues. However, there is evidence to suggest that this is the case; most notably Peter Shor has shown in [5] that the integer factoring and discrete log problems can be solved in polynomial time using a QTM. (These problems are believed not to be solvable in polynomial time using a probabilistic Turing machine.)

It is natural to extend the idea of quantum computation to other computational models; in this paper we discuss *one-dimensional quantum cellular automata*. Given any well-formed QTM, we give a construction of a one-dimensional quantum cellular automaton (1d-QCA) which will efficiently simulate this QTM. This is accomplished by defining a restricted class of 1d-QCA called *one-dimensional partitioned quantum cellular automata* (1d-PQCA). A 1d-PQCA is a 1d-QCA in which each cell is partitioned into three subcells (left, middle, and right), and where the next states of any given cell depend only on the contents of the right subcell of its left neighbor, the middle subcell of itself, and the left subcell of its right neighbor. This is the quantum analogue of the partitioned cellular automaton discussed by Kenichi Morita and Masateru Harao in [6]. The advantage of the 1d-PQCA class is that it is a simple matter to determine whether or not a given 1d-PQCA is well-formed, while this is not a trivial matter for an arbitrary 1d-QCA.

It is not clear that an arbitrary 1d-QCA can be efficiently simulated by a QTM. However, it is shown that any given 1d-PQCA can be simulated by a QTM with linear slowdown. It is interesting to note that given any 1d-PQCA, the QTM which results from this con-

*Supported in part by NSF Grant CCR-9208639.

struction will simulate the given 1d-PQCA with deterministic head position, i.e. if this QTM is observed at any time during its computation, the probability that the tape head will be observed in any given location will be either 0 or 1. This allows for the construction of a QTM which will simulate, with deterministic head position, any given QTM with linear slowdown. Thus, for example, the position of the tape head of any such QTM could be observed at every time step without affecting its computation. (This is generally not the case for an arbitrary QTM.)

The remainder of this paper will be organized as follows. In section 2, the one-dimensional quantum cellular automata model is defined. In section 3, the class of one-dimensional partitioned quantum cellular automata is defined, and necessary and sufficient conditions for the well-formedness of a 1d-PQCA are discussed. In section 4, the quantum Turing machine model is reviewed and in section 5, the equivalence of the quantum Turing machine model and the partitioned quantum cellular automata model is demonstrated. Finally, in section 6, some facts resulting from this discussion are mentioned.

2 One-Dimensional Quantum Cellular Automata

A *one-dimensional quantum cellular automaton* M is a quadruple (Q, δ, k, A) where Q is a finite set of *states* (including a distinguished *quiescent state* denoted by ϵ), δ is a *local transition function* (described below), k is an integer denoting the *acceptance cell*, and $A \subseteq Q$ is a set of *accepting states*. M is assumed to have a two-way infinite sequence of *cells* indexed by the integers (hereafter denoted by $\mathbb{Z}$.) The *neighborhood* of each cell is defined to be that cell itself along with its closest neighbor on each side.

A *configuration* of a 1d-QCA M is a map

$$a : \mathbb{Z} \to Q$$

where, for each integer n, $a(n)$ denotes the state of the cell indexed by n. For any configuration a, it is assumed that there are only finitely many values of n for which $a(n)$ is a non-quiescent state. Denote by $\mathcal{C} = \mathcal{C}(M)$ the set of all configurations of M, so that $\mathcal{C}$ is countable for any given 1d-QCA M. For any $a \in \mathcal{C}$, define $|a|$ (the *length* of a) to be the maximum number of consecutive cells such that the first and last cells are non-quiescent. Any configuration of M in which the cell indexed by k contains an element of A is said to be an *accepting configuration* and all other configurations are *non-accepting configurations*.

The local transition function δ is a map

$$\delta : Q^4 \longrightarrow \mathbb{C}$$

with

$$\delta(\epsilon, \epsilon, \epsilon, q) = \begin{cases} 1 & \text{if } q = \epsilon \\ 0 & \text{if } q \neq \epsilon \end{cases} \tag{1}$$

which describes the evolution of M. (Here $\mathbb{C}$ denotes the field of complex numbers.) Suppose that at some given time t, three consecutive cells of M are in states q_1, q_2 and q_3 respectively. Then for every state $q \in Q$, the cell which contained q_2 at time t will, at time $t+1$, update to the state q with *amplitude* $\delta(q_1, q_2, q_3, q)$. Every cell updates simultaneously in this manner, so that globally, if M is in some configuration $a \in \mathcal{C}$ at time t, then the amplitude with which M transforms to any configuration $b \in \mathcal{C}$ at time $t+1$ is defined to be the product of the amplitudes with which each cell of a transforms to the corresponding cell of b, i.e.

$$\prod_{n \in \mathbb{Z}} \delta(a(n-1), a(n), a(n+1), b(n)).$$

(This product is guaranteed to exist by (1).)

Thus, any configuration of M will transform into multiple "next configurations", where the transformation to each individual configuration has an associated amplitude. The evolution behaves as if all of these transformations occur simultaneously, so that after some number of steps, M will have evolved along many computation paths simultaneously. Each path has an associated amplitude which is defined to be the product of the amplitudes of the transformations along that path.

Multiple paths with differing amplitudes may lead from one given configuration to another. This effect is known as *interference*. If M is assumed to be in some configuration a and is allowed to evolve for, say l steps, then M will be in a *linear superposition* of configurations. For each configuration b in such a superposition, we associate with it an amplitude which is the sum of the amplitudes of all paths of length l from a to b. It may therefore be the case, for example, that a configuration will have amplitude zero in some superposition, despite the fact that multiple paths of nonzero amplitude lead to it.

If a 1d-QCA M is *observed* while in some superposition of configurations, the observer will not see this superposition. Rather, the act of observation forces the machine to choose one of the configurations in the given superposition randomly, so that exactly one configuration will be observed. The probability that any

given configuration is observed is the *absolute square* of the amplitude associated with that configuration, i.e. the absolute square of the sum of the amplitudes of all paths which lead to that configuration. The act of observation has the effect of altering the machine, so that immediately after the observation occurs the machine will be in a single configuration, and no longer a superposition of configurations. (More general types of observations are possible, but will be ignored for the purposes of this paper.)

For any 1d-QCA M and input configuration a, we are interested in whether or not an accepting configuration will be observed after some number of steps. The *probability that M accepts a after l steps* is simply the probability of observing any accepting configuration after l steps, assuming that M is initially placed in configuration a and is not observed before l steps have passed.

Since each configuration in a given superposition is observed with a certain probability, it is necessary that the sum of the probabilities be exactly one. Thus, allowed local transition functions δ must be restricted to those that guarantee this condition for any superposition resulting from any given input. A machine with such a local transition function is said to be *well-formed*. This will be formalized presently.

Given any 1d-QCA M, let $\ell_2(\mathcal{C})$ denote the space of all complex valued functions with domain $\mathcal{C} = \mathcal{C}(M)$ and bounded ℓ_2-norm, i.e.

$$\ell_2(\mathcal{C}) = \left\{ x : \mathcal{C} \to \mathbb{C} \;\middle|\; \left(\sum_{a \in \mathcal{C}} x(a)\overline{x(a)} \right)^{1/2} < \infty \right\}.$$

Then $\ell_2(\mathcal{C})$ is a *Hilbert space* with respect to the inner product $\langle \cdot, \cdot \rangle : \ell_2(\mathcal{C}) \times \ell_2(\mathcal{C}) \to \mathbb{C}$ defined by

$$\langle x_1, x_2 \rangle = \sum_{a \in \mathcal{C}} x_1(a)\overline{x_2(a)}.$$

Any superposition of M can now be identified with an element $x \in \ell_2(\mathcal{C})$, where $x(a) \in \mathbb{C}$ denotes the amplitude associated with configuration a in this superposition. Thus, the probability of observing a from this superposition is $|x(a)|^2$ for any $a \in \mathcal{C}$. We must therefore have

$$\sum_{a \in \mathcal{C}} |x(a)|^2 = 1 \tag{2}$$

for any superposition x. The sum in (2) is exactly $\|x\|^2$ by definition, so we define

$$\mathcal{S} = \{x \in \ell_2(\mathcal{C}) \mid \|x\| = 1\}$$

to be the set of all possible superpositions of M.

Each superposition of a given 1d-QCA M will, in one time-step, evolve into a new superposition according to the local transition function of M. We can associate with any M a function E which will map any given superposition to this next superposition; if x is some superposition of M at time t, then M will be in the superposition Ex at time $t+1$. In general, after l steps, M will be in the superposition $E^l x$. E is the *time-evolution operator* of M, and can be explicitly defined as follows. For all $a, b \in \mathcal{C}$ let $\alpha(a, b)$ denote the amplitude with which configuration a transforms into configuration b, i.e.

$$\alpha(a, b) = \prod_{n \in \mathbb{Z}} \delta(a(n-1), a(n), a(n+1), b(n)),$$

and for each $x \in \ell_2(\mathcal{C})$ and $b \in \mathcal{C}$ define

$$Ex(b) = \sum_{a \in \mathcal{C}} \alpha(a, b)x(a).$$

Thus, we say that $M = (Q, \delta, k, A)$ is a *well formed one-dimensional quantum cellular automaton* (write $M \in$ 1d-QCA) if and only if the corresponding time-evolution operator E preserves ℓ_2-norm, i.e.

$$x \in \mathcal{S} \iff Ex \in \mathcal{S}.$$

3 Partitioned Quantum Cellular Automata

In general, given an arbitrary $M = (Q, \delta, k, A)$, it is not a trivial matter to determine whether or not M is well formed. For this reason we now define a restricted class of 1d-QCA called *partitioned quantum cellular automata* for which this can easily be determined. This is a generalization of (deterministic) partitioned cellular automata discussed by Morita and Harao in [6].

A one-dimensional partitioned quantum cellular automaton is a 1d-QCA in which each cell is partitioned into three *subcells*: a *left subcell*, a *middle subcell* and a *right subcell*. (The set of states Q is decomposed accordingly.) The next state(s) of any cell may now only depend upon the states of the left subcell of the right neighbor, the middle subcell of the cell itself, and the right subcell of the left neighbor.

More formally, let $M = (Q, \delta, k, A)$ as in the 1d-QCA case, where Q and δ are restricted as follows. Let

$$Q = Q_l \times Q_m \times Q_r$$

for finite sets Q_l, Q_m and Q_r, (and again let ϵ denote the distinguished quiescent element of Q.) Let Λ be an $|Q| \times |Q|$ matrix over $\mathbb{C}$ having the form

$$\Lambda = \begin{pmatrix} \lambda(q_1,q_1) & \lambda(q_1,q_2) & \dots & \lambda(q_1,q_{|Q|}) \\ \lambda(q_2,q_1) & \lambda(q_2,q_2) & \dots & \lambda(q_2,q_{|Q|}) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(q_{|Q|},q_1) & \lambda(q_{|Q|},q_2) & \dots & \lambda(q_{|Q|},q_{|Q|}) \end{pmatrix}$$

where $\lambda : Q \times Q \longrightarrow \mathbb{C}$ must satisfy

$$\lambda(\epsilon,q) = \lambda(q,\epsilon) = \begin{cases} 1 & \text{if } q = \epsilon \\ 0 & \text{if } q \neq \epsilon. \end{cases} \tag{3}$$

For any state $q = (q_l, q_m, q_r)$ define

$$l(q) = q_l, \quad m(q) = q_m, \quad r(q) = q_r,$$

and define δ as

$$\delta(q_1,q_2,q_3,q) = \lambda(\,(l(q_3), m(q_2), r(q_1)),\, q)$$

for all $q_1, q_2, q_3, q \in Q$. Since a given matrix Λ completely determines δ in this manner, we may write $M = (Q, \Lambda, k, A)$ rather than $M = (Q, \delta, k, A)$ for a 1d-PQCA M whenever convenient.

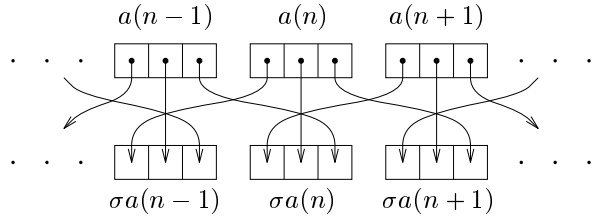
The behavior of a partitioned quantum cellular automaton M is, in general, simpler than that of an arbitrary 1d-QCA. Suppose that M is in configuration a. Then after one time step, for any given $n \in \mathbb{Z}$, the state of the cell indexed by n will be transformed to each state q with amplitude

$$\begin{aligned} &\delta(a(n-1), a(n), a(n+1), q) \\ &\quad = \lambda(\,(l(a(n+1)), m(a(n)), r(a(n-1))),\, q). \end{aligned} \tag{4}$$

In order to simplify this, we will define a permutation $\sigma : \mathcal{C} \longrightarrow \mathcal{C}$ as

$$\sigma a(n) = (l(a(n+1)), m(a(n)), r(a(n-1)))$$

for all $n \in \mathbb{Z}$. The action of the permutation σ on any configuration a can be illustrated as follows:



Now, (4) is equivalent to

$$\delta(a(n-1), a(n), a(n+1), q) = \lambda(\sigma a(n), q),$$

so that applying δ to each neighborhood of some configuration a is equivalent to first applying σ to a and then applying λ to each individual cell of σa, i.e. $\sigma a(n)$ is transformed into each state q with amplitude $\lambda(\sigma a(n), q)$ for every $n \in \mathbb{Z}$.

If, for such an M, we have $M \in$ 1d-QCA we will say that M is a *well formed one-dimensional partitioned quantum cellular automaton* (write $M \in$ 1d-PQCA.) The following theorem allows us to characterize one-dimensional partitioned cellular automata in terms of the matrix Λ.

Theorem 3.1 *Let $M = (Q, \Lambda, k, A)$ with Λ as above. Then $M \in$ 1d-PQCA if and only if Λ is unitary.*

The remainder of this section will be devoted to proving this theorem.

For each $a, b \in \mathcal{C}$ define

$$u_b(a) = \overline{\alpha(a,b)},$$

and

$$v_b(a) = \alpha(b,a).$$

Lemma 3.1 *Let $M = (Q, \Lambda, k, A)$, where Λ satisfies* (3)*. Then we have*

$$\#\{a \in \mathcal{C} \mid u_b(a) \neq 0\} < \infty \tag{5}$$

and

$$\#\{a \in \mathcal{C} \mid v_b(a) \neq 0\} < \infty \tag{6}$$

for any $b \in \mathcal{C}$.

Proof. Given $b \in \mathcal{C}$, assume that $u_b(a) \neq 0$. By definition

$$u_b(a) = \prod_{n \in \mathbb{Z}} \overline{\lambda(\sigma a(n), b(n))}.$$

Since $b \in \mathcal{C}$ and $\lambda(q, \epsilon) = 0$ for $q \neq \epsilon$, a must be such that $\sigma a(n) = b(n) = \epsilon$ for all but finitely many n. There are finitely many such $a \in \mathcal{C}$.

(6) follows similarly. ■

By Lemma 3.1, the sums

$$\sum_{a \in \mathcal{C}} u_b(a)\overline{u_b(a)}$$

and

$$\sum_{a \in \mathcal{C}} v_b(a)\overline{v_b(a)}$$

contain only finitely many nonzero terms and therefore converge, so we have that u_b and v_b are elements of $\ell_2(\mathcal{C})$ for each $b \in \mathcal{C}$.

Lemma 3.2 *Λ unitary $\Longrightarrow$ $\{u_b\}_{b\in\mathcal{C}}$ and $\{v_b\}_{b\in\mathcal{C}}$ are orthonormal sequences in $\ell_2(\mathcal{C})$.*

Proof. Given $a, b \in \mathcal{C}$ we will show

$$\langle u_a, u_b\rangle = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b. \end{cases} \tag{7}$$

For each $m \in \mathbb{Z}$, $q \in Q$, define $S_m^q : \mathcal{C} \longrightarrow \mathcal{C}$ as

$$S_m^q(c)(n) = \begin{cases} c(n) & \text{if } n > m \\ q & \text{if } n = m \\ c(n+1) & \text{if } n < m \end{cases}$$

for all $n \in \mathbb{Z}$, and also define $R_m^q : \mathcal{C} \longrightarrow \mathcal{C}$ as

$$R_m^q(c)(n) = \begin{cases} c(n) & \text{if } n \neq m \\ q & \text{if } n = m \end{cases}$$

for all $n \in \mathbb{Z}$.

Since σ is one-to-one and onto, we have

$$\begin{aligned} \langle u_a, u_b\rangle &= \sum_{c\in\mathcal{C}} u_a(\sigma^{-1}c)\overline{u_b(\sigma^{-1}c)} \\ &= \sum_{c\in\mathcal{C}} \prod_{n\in\mathbb{Z}} \overline{\lambda(c(n), a(n))}\lambda(c(n), b(n)). \end{aligned} \tag{8}$$

By Lemma 3.1 there are only finitely many values of c for which the summand is nonzero, so we are free to change the order of summation in (8) as follows

$$\langle u_a, u_b\rangle = \sum_{c\in\mathcal{C}} \sum_{q\in Q} P\,\overline{\lambda(q, a(m))}\lambda(q, b(m))$$

where

$$P = \prod_{n\neq m} \overline{\lambda(S_m^q(c)(n), a(n))}\lambda(S_m^q(c)(n), b(n))$$

and m is any integer. P is independent of q, so we have

$$\langle u_a, u_b\rangle = \sum_{c\in\mathcal{C}} P \sum_{q\in Q} \overline{\lambda(q, a(m))}\lambda(q, b(m)). \tag{9}$$

Suppose that $a \neq b$. Then there must exist $m \in \mathbb{Z}$ such that $a(m) \neq b(m)$. Λ is unitary, so that

$$\sum_{q\in Q} \overline{\lambda(q, a(m))}\lambda(q, b(m)) = 0$$

and therefore by (9) we have $\langle u_a, u_b\rangle = 0$.

Now consider $\langle u_a, u_a\rangle$. From (9)

$$\langle u_a, u_a\rangle = \sum_{c\in\mathcal{C}} P \sum_{q\in Q} |\lambda(q, a(m))|^2$$

for

$$P = \prod_{n\neq m} |\lambda(S_m^q(c)(n), a(n))|^2.$$

For any $p \in Q$ we have $\sum_{q\in Q} |\lambda(p, q)|^2 = 1$, since Λ is unitary. Thus

$$\begin{aligned} \langle u_a, u_a\rangle &= \sum_{c\in\mathcal{C}} \prod_{n\neq m} |\lambda(S_m^q(c)(n), a(n))|^2 \\ &= \sum_{c\in\mathcal{C}} \prod_{n\neq m} |\lambda(S_m^\epsilon(c)(n), a(n))|^2 \\ &= \sum_{c\in\mathcal{C}} \prod_{n\in\mathbb{Z}} |\lambda(c(n), R_m^\epsilon(a)(n))|^2 \\ &= \langle u_{a_1}, u_{a_1}\rangle \end{aligned} \tag{10}$$

for $a_1 = R_m^\epsilon(a)$.

Now $a \in \mathcal{C}$, and therefore there exists a finite set $\{m_1, \ldots, m_k\}$ for which

$$n \notin \{m_1, \ldots, m_k\} \Longrightarrow a(n) = \epsilon.$$

If we repeat the process resulting in (10) for each $m = m_1, m_2, \ldots, m_k$, we get $\langle u_a, u_a\rangle = \langle u_{a_k}, u_{a_k}\rangle$ for $a_k = R_{m_1}^\epsilon(R_{m_2}^\epsilon(\cdots(R_{m_k}^\epsilon(a))\cdots))$. Since $a_k(n) = \epsilon$ for all $n \in \mathbb{Z}$ we have

$$\begin{aligned} \langle u_a, u_a\rangle &= \langle u_{a_k}, u_{a_k}\rangle \\ &= \sum_{c\in\mathcal{C}} \prod_{n\in\mathbb{Z}} |\lambda(c(n), \epsilon)|^2 = 1, \end{aligned}$$

and so we have shown (7).

A slight modification of the above argument shows that $\{v_b\}_{b\in\mathcal{C}}$ is also an orthonormal sequence. ■

Proof of Theorem 3.1. Assume that we are given $M = (Q, \Lambda, k, A)$ with Λ unitary. We will show that E, the time-evolution operator of M, is unitary.

By definition, we have

$$Ex(b) = \sum_{a\in\mathcal{C}} x(a)\overline{u_b(a)}.$$

so that

$$Ex(b) = \langle x, u_b\rangle$$

for every $x \in \ell_2(\mathcal{C})$ and $b \in \mathcal{C}$. Also define F as

$$Fx(b) = \sum_{a\in\mathcal{C}} x(a)\overline{v_b(a)},$$

so that

$$Fx(b) = \langle x, v_b\rangle$$

for every $x \in \ell_2(\mathcal{C})$ and $b \in \mathcal{C}$.

By Lemma 3.1, $\{u_b\}_{b\in\mathcal{C}}$ is an orthonormal sequence. So, by Bessel's inequality

$$\begin{aligned}\|Ex\|^2 &= \sum_{b\in\mathcal{C}} Ex(b)\overline{Ex(b)} \\ &= \sum_{b\in\mathcal{C}} |\langle x, u_b\rangle|^2 \\ &\leq \|x\|^2,\end{aligned}$$

for any $x \in \ell_2(\mathcal{C})$. Thus E is a bounded linear operator, and hence we have that

$$\langle Ex, y\rangle = \sum_{b\in\mathcal{C}}\sum_{a\in\mathcal{C}} x(a)\overline{u_b(a)y(b)} \qquad (11)$$

is a bounded bilinear form. This allows us (see [7], for example) to change the order of summation in (11) to get

$$\begin{aligned}\langle Ex, y\rangle &= \sum_{a\in\mathcal{C}}\sum_{b\in\mathcal{C}} x(a)\overline{u_b(a)y(b)} \\ &= \sum_{a\in\mathcal{C}} x(a)\sum_{b\in\mathcal{C}}\overline{y(b)}v_a(b) \\ &= \langle x, Fy\rangle\end{aligned}$$

for any $x, y \in \ell_2(\mathcal{C})$, so that $E^* = F$.

Now, for any $x \in \ell_2(\mathcal{C})$ and $b \in \mathcal{C}$ we have, by applying Lemma 3.1 and Lemma 3.2,

$$\begin{aligned}E^*Ex(b) &= \sum_{a\in\mathcal{C}} Ex(a)\overline{v_b(a)} \\ &= \sum_{a\in\mathcal{C}}\sum_{c\in\mathcal{C}} x(c)\overline{u_a(c)v_b(a)} \\ &= \sum_{c\in\mathcal{C}}\sum_{a\in\mathcal{C}} x(c)v_c(a)\overline{v_b(a)} \\ &= \sum_{c\in\mathcal{C}} x(c)\langle v_c, v_b\rangle \\ &= x(b)\end{aligned}$$

so that $E^*E = I$. Similarly

$$EE^*x(b) = \sum_{c\in\mathcal{C}} x(c)\langle u_c, u_b\rangle = x(b)$$

for any $x \in \ell_2(\mathcal{C})$, $b \in \mathcal{C}$, so that $EE^* = I$.

Thus, E is unitary and hence preserves ℓ_2-norm. We therefore have that $M \in$ 1d-PQCA.

The converse is straightforward. ■

Corollary 3.1 *For any $M \in$ 1d-PQCA, the associated time-evolution operator E is unitary.*

4 Quantum Turing Machines

In this section we will review the quantum Turing machine model as defined in [3]. A quantum Turing machine M is a quintuple (K, Σ, μ, k, A) where K is a finite set of *states*, Σ is a finite *tape alphabet* (including a distinguished *blank* symbol, denoted by b), μ is a *local transition function* (described below), k is an integer denoting the distinguished *acceptance tape square*, and $A \subseteq \Sigma$ is a set of *accepting symbols*. M is assumed to have a single read-write tape head and a single two-way infinite tape with tape squares indexed by $\mathbb{Z}$.

A *configuration* of a QTM M is a triple (s, h, c), where $s \in K$ denotes the current *state* of M, $h \in \mathbb{Z}$ denotes the index of the tape square over which the tape head is currently located, and c is a map from $\mathbb{Z}$ to Σ which describes the contents of the tape. For any configuration of M it is assumed that the number of tape squares containing non-blank symbols is finite. Any configuration of M in which the tape cell indexed by k contains an element of A is said to be an *accepting configuration* and all other configurations are *non-accepting configurations*.

The local transition function μ is a map

$$\mu : K \times \Sigma \times \Sigma \times K \times \{L, R\} \longrightarrow \mathbb{C}$$

which describes the evolution of M. Suppose that, at some particular time, the current state of M is s and the tape head of M is located above a tape square which contains the symbol τ. Then for every triple $(\tau', s', d) \in \Sigma \times K \times \{L, R\}$, M will write the symbol τ' in the currently scanned tape square, change internal state to s' and move the tape head in direction d with amplitude $\mu(s, \tau, \tau', s', d)$.

As in the 1d-QCA case, the computation behaves as if all of these transitions occur simultaneously, so that after some number of steps M will have traversed many different computation paths simultaneously, each with an associated amplitude. The amplitude associated with each path is defined to be the product of the amplitudes of the transitions along that path. After l steps, say, M will be in a linear superposition of configurations, and the amplitude associated with each configuration will be the sum of the amplitudes along all paths of length l to that configuration.

If observed while in a superposition of configurations, M will randomly choose a single configuration which will be seen; again the probability that a given configuration will be observed is the absolute square of the amplitude associated with that configuration. Allowed local transition functions μ must be restricted

to those that guarantee that the sum of these probabilities will be one for any given superposition. Such a QTM is said to be well-formed. (Write $M \in$ QTM whenever M is a well-formed quantum Turing machine.) We state, without proof, the following theorem, due to Bernstein and Vazirani, which allows us to characterize well-formed quantum Turing machines in terms of their local transition functions:

Theorem 4.1 (Bernstein & Vazirani) *Given any $M = (K, \Sigma, \mu, k, A)$ as above, $M \in QTM$ if and only if* (i) $\forall\, (s_1, \tau_1), (s_2, \tau_2) \in K \times \Sigma$:

$$\sum_{\xi, s, d} \mu(s_1, \tau_1, \xi, s, d)\overline{\mu(s_2, \tau_2, \xi, s, d)} = \begin{cases} 1 & \text{if } (s_1, \tau_1) = (s_2, \tau_2) \\ 0 & \text{if } (s_1, \tau_1) \neq (s_2, \tau_2) \end{cases}$$

and (ii) $\forall\, (s_1, \tau_1, \xi_1), (s_2, \tau_2, \xi_2) \in K \times \Sigma \times \Sigma$:

$$\sum_{s} \mu(s_1, \tau_1, \xi_1, s, L)\overline{\mu(s_2, \tau_2, \xi_2, s, R)} = 0.$$

5 Equivalence of QTM and 1d-PQCA Models

We now show that for any $M_{tm} \in$ QTM, there is an $M_{ca} \in$ 1d-PQCA which simulates M_{tm} with constant slowdown, and similarly for any $M_{ca} \in$ 1d-PQCA there is an $M_{tm} \in$ QTM which simulates M_{ca} with linear slowdown.

5.1 1d-PQCA Simulation of a QTM

Let $M_{tm} = (K, \Sigma, \mu, k_{tm}, A_{tm}) \in$ QTM and let $M_{ca} = (Q, \Lambda, k_{ca}, A_{ca}) \in$ 1d-PQCA. We will say that M_{ca} *simulates* M_{tm} if and only if there exists a linear-time computable function $T : \mathcal{C}(M_{tm}) \to \mathcal{C}(M_{ca})$ and a function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ such that for any given configuration $a \in \mathcal{C}(M_{tm})$, the probability that M_{tm} accepts a after t steps is equal to the probability that M_{ca} accepts $T(a)$ after $f(t, |T(a)|)$ steps.

Without loss of generality, we can assume that the QTM which is to be simulated has the property that any given state is only entered while the tape head is moving in one direction, due to the following lemma of Bernstein and Vazirani.

Lemma 5.1 (Bernstein & Vazirani) *Given any $M \in QTM$, there exists an $M' \in QTM$ which simulates M with constant slowdown, and which satisfies the following property:*

(P1) M' enters each state while moving in exactly one direction, i.e. if $\mu'(s_1, \tau_1, \xi_1, s_1', d_1)$ and $\mu'(s_2, \tau_2, \xi_2, s_2', d_2)$ are both nonzero, then $d_1 = d_2$.

Thus, given $M_{tm} = (K, \Sigma, \mu, k_{tm}, A_{tm})$ satisfying $(P1)$, K can be partitioned into two sets: K_l and K_r, such that M enters states in K_l only when moving left, and enters states in K_r only when moving right.

We now define a 1d-PQCA $M_{ca} = (Q, \Lambda, k_{ca}, A_{ca})$ which will simulate M_{tm}. Define $Q = Q_l \times Q_m \times Q_r$ with

$$Q_l = K_l \cup \{\#\}, \quad Q_m = \Sigma, \quad Q_r = K_r \cup \{\#\}.$$

The quiescent element of Q is defined to be $(\#, b, \#)$, where b is the blank symbol of M_{tm}. Define Λ as follows:

(i) for each $(s_1, \tau_1), (s_2, \tau_2) \in K_l \times \Sigma$ let

$$\lambda((s_1, \tau_1, \#), (s_2, \tau_2, \#)) = \mu(s_1, \tau_1, \tau_2, s_2, L),$$

(ii) for each $(s_1, \tau_1) \in K_l \times \Sigma$, $(s_2, \tau_2) \in K_r \times \Sigma$ let

$$\lambda((s_1, \tau_1, \#), (\#, \tau_2, s_2)) = \mu(s_1, \tau_1, \tau_2, s_2, R),$$
$$\lambda((\#, \tau_2, s_2), (s_1, \tau_1, \#)) = \mu(s_2, \tau_2, \tau_1, s_1, L),$$

(iii) for each $(s_1, \tau_1), (s_2, \tau_2) \in K_r \times \Sigma$ let

$$\lambda((\#, \tau_1, s_1), (\#, \tau_2, s_2)) = \mu(s_1, \tau_1, \tau_2, s_2, R),$$

(iv) for any $q_1, q_2 \in Q$ for which $\lambda(q_1, q_2)$ has not already been defined in (i) – (iii), let

$$\lambda(q_1, q_2) = \begin{cases} 1 & \text{if } q_1 = q_2 \\ 0 & \text{otherwise.} \end{cases}$$

Let $k_{ca} = k_{tm}$ and define

$$A_{ca} = \{(q_l, q_m, q_r) \in Q \mid q_m \in A_{tm}\}.$$

A straightforward application of Theorem 3.1 and Theorem 4.1 yields the following

Lemma 5.2 *If $M_{tm} \in QTM$ then $M_{ca} \in$ 1d-PQCA.*

For $(s, h, c) \in \mathcal{C}(M_{tm})$, define $T((s, h, c)) \in \mathcal{C}(M_{ca})$ as follows. For each $n \in \mathbb{Z}$ let

$$T((s, h, c))(n) = \begin{cases} (\#, c(n), \#) & \text{if } s \in K_l \text{ and } n \neq h + 1 \\ (s, c(n), \#) & \text{if } s \in K_l \text{ and } n = h + 1 \\ (\#, c(n), \#) & \text{if } s \in K_r \text{ and } n \neq h - 1 \\ (\#, c(n), s) & \text{if } s \in K_r \text{ and } n = h - 1. \end{cases}$$

Lemma 5.3 *For any $n \in \mathbb{Z}^+$, the probability that M_{tm} accepts (s,h,c) after n steps is equal to the probability that M_{ca} accepts $T((s,h,c))$ after n steps.*

Proof. [Sketch] For any configuration a of M_{tm}, the symbol contained in the tape square indexed by n is equal to the contents of the middle subcell of the cell indexed by n in $T(a)$. Recall that the evolution of a 1d-PQCA may be decomposed into two steps: applying the permutation σ to the current configuration, then transforming each cell according to λ. Now, for each n, $\sigma T((s,h,c))(n)$ will have have a non-# state in its left or right subcell exactly when $h = n$, thereby simulating the presence of the tape head at this location. By inspection of the definition of λ, it is clear that M_{ca} will evolve in accordance with M_{tm}. ■

Together, Lemma 5.1, Lemma 5.2 and Lemma 5.3 give us

Theorem 5.1 *Given any $M_{tm} \in QTM$ there is an $M_{ca} \in$ 1d-PQCA which simulates M_{tm} with constant slowdown.*

5.2 QTM Simulation of a 1d-PQCA

Again, let $M_{tm} = (K, \Sigma, \mu, k_{tm}, A_{tm}) \in$ QTM and let $M_{ca} = (Q, \Lambda, k_{ca}, A_{ca}) \in$ 1d-PQCA. Then M_{tm} *simulates* M_{ca} if and only if there exists a linear-time computable function $T : \mathcal{C}(M_{ca}) \to \mathcal{C}(M_{tm})$ and a function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ such that for any given configuration $a \in \mathcal{C}(M_{ca})$, the probability that M_{ca} accepts a after t steps is equal to the probability that M_{tm} accepts $T(a)$ after $f(t, |T(a)|)$ steps.

Given $M_{ca} = (Q, \Lambda, k_{ca}, A_{ca}) \in$ 1d-PQCA we will now define $M_{tm} = (K, \Sigma, \mu, k_{tm}, A_{tm}) \in$ QTM which will simulate M_{ca}.

Each tape square of M_{tm} will represent the cell of M_{ca} with the same index. Define

$$\Sigma = (Q_l \times Q_m \times Q_r) \cup (Q_l \times Q_m \times Q_r)^\star$$

where $(Q_l \times Q_m \times Q_r)^\star$ is a copy of $(Q_l \times Q_m \times Q_r)$, so that $(p_l, p_m, p_r)^\star \in (Q_l \times Q_m \times Q_r)^\star$ whenever $(p_l, p_m, p_r) \in (Q_l \times Q_m \times Q_r)$. ($M_{tm}$ will need to simulate only a finite portion of M_{ca}, since we are only concerned with finite configurations of M_{ca}, so tape squares containing a symbol in $(Q_l \times Q_m \times Q_r)^\star$ will be used to mark the leftmost and rightmost cells of M_{ca} being simulated at that time.) Let ϵ be the blank symbol of M_{tm}.

Define

$$K = Q_l \times \{s_0, s_1, s_1^\star, s_2, s_2^\star, s_3\} \times Q_r.$$

Each state of M_{tm} will consist of one element from Q_l and one element from Q_r (in order to "move" states from one tape square to another when performing the permutation σ, as described in section 3) and one element from $\{s_0, s_1, s_1^\star, s_2, s_2^\star, s_3\}$.

The simulation of each step of M_{ca} takes place in three stages. The first stage reversibly performs the permutation σ on the configuration of M_{ca} currently represented by the contents of the tape. In order to do this, let μ take the following values: for each $(l,r) \in Q_l \times Q_r$, $(p_l, p_m, p_r), (q_l, q_m, q_r) \in Q_l \times Q_m \times Q_r$, define

$$\begin{aligned}
&\mu((l, s_0, r), (p_l, p_m, p_r)^\star, (p_l, p_m, r)^\star, (l, s_1, p_r), R) = 1\\
&\mu((l, s_1, r), (p_l, p_m, p_r), (p_l, p_m, r), (l, s_1, p_r), R) = 1\\
&\mu((l, s_1, r), (p_l, p_m, p_r)^\star, (p_l, p_m, r), (l, s_1^\star, p_r), R) = 1\\
&\mu((l, s_1^\star, r), (p_l, p_m, p_r)^\star, (p_l, p_m, r)^\star, (l, s_1^\star, p_r), R) = 1
\end{aligned}$$

$$\begin{aligned}
&\mu((l, s_1^\star, r), (p_l, p_m, p_r), (l, p_m, r)^\star, (p_l, s_2, p_r), L) = 1\\
&\mu((l, s_2, r), (p_l, p_m, p_r), (l, p_m, p_r), (p_l, s_2, r), L) = 1\\
&\mu((l, s_2, r), (p_l, p_m, p_r)^\star, (l, p_m, p_r), (p_l, s_2^\star, r), L) = 1\\
&\mu((l, s_2^\star, r), (p_l, p_m, p_r)^\star, (l, p_m, p_r)^\star, (p_l, s_2^\star, r), L) = 1
\end{aligned}$$

(Note that not all of these transitions will be used given proper input, but are added to guarantee well-formedness.) In the second stage of the simulation, the state contained in each tape square of M_{tm} is transformed in accordance with λ, so for each $(l,r) \in Q_l \times Q_r$, $(p_l, p_m, p_r), (q_l, q_m, q_r) \in Q_l \times Q_m \times Q_r$, define

$$\begin{aligned}
&\mu((l, s_2^\star, r), (p_l, p_m, p_r), (q_l, q_m, q_r)^\star, (p_l, s_3, r), R)\\
&\qquad = \lambda((l, p_m, p_r), (q_l, q_m, q_r))\\
&\mu((l, s_3, r), (p_l, p_m, p_r), (q_l, q_m, q_r), (l, s_3, r), R)\\
&\qquad = \lambda((p_l, p_m, p_r), (q_l, q_m, q_r))\\
&\mu((l, s_3, r), (p_l, p_m, p_r)^\star, (q_l, q_m, q_r)^\star, (l, s_0, r), L)\\
&\qquad = \lambda((p_l, p_m, p_r), (q_l, q_m, q_r))
\end{aligned}$$

The third stage of the simulation simply returns the tape head to the tape square representing the (new) leftmost cell of M_{ca} being simulated. For each $(l,r) \in Q_l \times Q_r$, $(p_l, p_m, p_r), (q_l, q_m, q_r) \in Q_l \times Q_m \times Q_r$, define

$$\mu((l, s_0, r), (p_l, p_m, p_r), (p_l, p_m, p_r), (l, s_0, r), L) = 1$$

Finally, let μ take the value 0 everywhere not defined above.

Let $k_{tm} = k_{ca}$ and define

$$A_{tm} = \{q \mid q \in A_{ca}\} \cup \{q^\star \mid q \in A_{ca}\}.$$

The following lemma follows from Theorem 3.1 and Theorem 4.1.

Lemma 5.4 *If $M_{ca} \in$ 1d-PQCA then $M_{tm} \in QTM$.*

Given $a \in \mathcal{C}(M_{ca})$ let n_l and n_r denote the indices of the leftmost and rightmost non-quiescent cells of a respectively. (If $n_l = n_r$ then set $n_r = n_l + 1$. If all

cells of a are quiescent, then choose n_l arbitrarily and set $n_r = n_l + 1$.) Define $(s, h, c) = T(a)$ as follows: let $s = (\epsilon, s_0, \epsilon)$, let $h = n_l$, and let $c : \mathbb{Z} \to \Sigma$ be defined as

$$c(n) = \begin{cases} a(n) & \text{if } n \neq n_l \text{ and } n \neq n_r \\ a(n)^\star & \text{if } n = n_l \text{ or } n = n_r. \end{cases}$$

Define

$$f(t, |c|) = 4t^2 + 4|c|t - t.$$

This is the number of steps required for M_{tm} to simulate t steps of M_{ca} on input c..

Lemma 5.5 *For any $t \in \mathbb{Z}^+$ and $c \in \mathcal{C}(M_{ca})$, the probability that M_{ca} accepts c after t steps is equal to the probability that M_{tm} accepts $T(c)$ after $f(t, |T(c)|)$ steps.*

Proof. [Sketch] Assume that we begin the simulation of each time step of M_{ca} with the tape head located over the leftmost cell of the finite section of M_{ca} being simulated, and with the current internal state of M_{tm} equal to $(\epsilon, s_0, \epsilon)$.

First, the permutation σ is performed reversibly in two passes of the tape contents, first moving to the far right then returning to the left. The finite section of M_{ca} being simulated will grow by one cell on each end during this stage, since the right and left starred symbols are shifted one cell to the right and left respectively. Next, in a single pass to the right, the state of each tape square is "quantumly" transformed in accordance with λ. When this has been completed, the tape head is returned to the tape square representing the (new) leftmost cell of M_{ca} being simulated. Since the tape squares outside of the region between the starred symbols are assumed to contain blanks (representing quiescent cells), the current internal state of M_{tm} will again be $(\epsilon, s_0, \epsilon)$.

Thus, after four passes of the current tape contents, M_{tm} will be in a linear superposition of configurations which corresponds to the superposition of M_{ca} after one time step, i.e. each configuration of M_{tm} will have the same amplitude as the configuration in the superposition of M_{ca} which it represents. The long-term evolution of M_{tm} will thus behave exactly as that of M_{ca}. ■

By Lemma 5.4 and Lemma 5.5 we have

Theorem 5.2 *Given any $M_{ca} \in$ 1d-PQCA, there exists $M_{tm} \in$ QTM which simulates M_{ca} with linear slowdown.*

6 Some Resulting Facts

From the preceeding discussion, we are immediately led to two straightforward results.

The first result is an observation concerning the construction in section 5.2. The QTM which results from this construction has the interesting property that the motion of its tape head is deterministic, formalized as follows. Let $M \in$ QTM and let a be an arbitrary configuration of M. If M is assumed to be in configuration a and is run (unobserved) for l steps and then observed, then for any integer h there is some probability that the tape head of M will be located over the tape square indexed by h. We say that M has *deterministic head position* if, for all $a \in \mathcal{C}(M)$, $l \in \mathbb{Z}^+$ and $h \in \mathbb{Z}$, we have that this probability is either zero or one.

By Theorem 5.1 and Theorem 5.2 we have

Corollary 6.1 *For any QTM M, there exists a QTM M' such that M' simulates M with linear slowdown, and such that M' has deterministic head position.*

In addition to being deterministic, the head position of the QTM resulting from the previously mentioned construction is also oblivious; for any input of a given length, the position of the tape head at a given time will depend only upon this length.

The second result regards the notion of acceptance and rejection by a 1d-PQCA. Consider

$$M = (Q, \Lambda, k, A) \in \text{1d-PQCA}.$$

Recall that for any $a \in \mathcal{C}$ and $l \in \mathbb{Z}^+$, M accepts a after l steps with probability equal to that of observing an element of A in the cell indexed by k after l steps. Of course, this probability may differ greatly with any change in l, so that if we are interested in whether or not M recognizes some language $\mathcal{L} \subseteq \mathcal{C}(M)$, we must pair some $l \in \mathbb{Z}^+$ with each input $a \in \mathcal{C}$ and observe M after *exactly* l steps have passed. This may seem unsatisfactory since it implies that the observer must carefully clock the machine and observe it at precisely the right moment, or else the computation may be invalid. However, we see that this is a reasonable definition of acceptance/rejection, due to the following

Theorem 6.1 *For any $M \in$ 1d-PQCA there exists an $M' \in$ 1d-PQCA so that for any $a \in \mathcal{C}(M)$ and $l \in \mathbb{Z}^+$ there exists an $a' \in \mathcal{C}(M')$ (computable in $\mathcal{O}(l + |a|)$ steps) such that the probability that M accepts a after l steps is equal to the probability that M' accepts a' after l' steps for any $l' \geq l$.*

Proof. Suppose that a 1d-PQCA $M = (Q, \Lambda, k, A)$, with quiescent state ϵ, is given.

First, define $M_t = (Q_t, \Lambda_t, k, A_t)$ as follows. Let

$$Q_t = \{0,1\} \times \{0,1\} \times \{0\}$$

(with $\epsilon_t = (0,0,0)$ as the quiescent state), let Λ_t be the identity matrix and let $A_t = \{(1,1,0)\}$. The action of M_t on any configuration is identical to the permutation σ.

For any given $l \in \mathbb{Z}^+$, if we define $a_t \in \mathcal{C}(M_t)$ as

$$a_t(n) = \begin{cases} (0,1,0) & \text{if } n = k \\ (1,0,0) & \text{if } n = k+l \\ (0,0,0) & \text{otherwise,} \end{cases}$$

then on input a_t, the cell of M_t indexed by k will be in the state $(1,1,0)$ after exactly l steps have passed, and at no other time will any cell contain this state.

Now define $M_1 = (Q_1, \Lambda_1, k, A_1)$ as follows. Let $Q_1 = Q \times Q_t$ (with quiescent state $\epsilon_1 = (\epsilon, \epsilon_t)$, let $A_1 = A \times A_t$ and let Λ_1 be as defined by

$$\lambda_1((p,p_t),(q,q_t)) = \lambda(p,q)\lambda_t(p_t,q_t)$$

for $(p,p_t),(q,q_t) \in Q \times Q_t$. Clearly $M_1 \in$ 1d-PQCA. M_1 can be viewed as M and M_t "stacked" on top of one another, evolving independently.

For any given $a \in \mathcal{C}(M)$ and $l \in \mathbb{Z}^+$, if we define $a_1 \in \mathcal{C}(M_1)$ as

$$a_1(n) = (a(n), a_t(n)),$$

where a_t is as defined above, then the probability that M_1 accepts a_1 after l steps is the same as the probability that M accepts a after l steps. Furthermore, the cell of M_1 indexed by k will not contain an accepting state at any other time, and at no time will any other cell contain an accepting state.

Finally, define $Q_a = \{0\} \times \{0,1\} \times \{0\}$, and define $M' = (Q', \Lambda', k, A')$ as follows. Let $Q' = Q_1 \times Q_a$, let $A' = Q_1 \times \{(0,1,0)\}$ and define Λ' as

$$\lambda'((p_1,p_a),(q_1,q_a)) = \begin{cases} \lambda_1(p_1,q_1) & \text{if } q_1 \notin A_1 \text{ and } p_a = q_a \\ & \text{or } q_1 \in A_1 \text{ and } p_a \neq q_a \\ 0 & \text{otherwise} \end{cases}$$

for every $(p_1,p_a),(q_1,q_a) \in Q_1 \times Q_a$. Since Λ_1 is unitary, we must have that Λ' is unitary, so that $M' \in$ 1d-PQCA (with quiescent state $(\epsilon_1, (0,0,0))$.)

Now, for given $a \in \mathcal{C}(M)$ and $l \in \mathbb{Z}^+$, define $a' \in \mathcal{C}(M')$ as

$$a'(n) = (a_1(n), (0,0,0)),$$

where a_1 is as defined above.

Consider the evolution of M' on input a'. By the definition of Λ', we see that any state (p_1,p_a) will be transformed (with nonzero amplitude) into state (q_1,q_a) with $q_a \neq p_a$ (toggling acceptance/rejection) exactly when $q_1 \in A_1$. But if any cell of M' ever contains a state in $A_1 \times Q_a$, then we know that this must be the cell indexed by k and exactly l steps must have passed (by the property of M_1 on input a_1 mentioned above.) Thus, such a transformation will occur at most one time on any given computation path, and only on those paths which correspond to paths of M_1 which accept a_1 after l steps. ■

Acknowledgements

Many thanks to Eric Bach for his valuable insights and advice, and for introducing me to quantum computing. Thanks also to Anne Condon and Walter Ludwig for their helpful comments and suggestions, and to Christoph Dürr for pointing out an error in an earlier version of this paper.

References

[1] R. Feynman, Simulating Physics with Computers, *International Journal of Theoretical Physics*, Vol. 21, nos. 6/7 (1982) 467-488.

[2] D. Deutsch, Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proc. R. Soc. Lond.*, Vol. A400 (1985) 97-117.

[3] E. Bernstein and U. Vazirani, Quantum Complexity Theory, *Proc. 25th Ann. ACM Symp. on Theory of Computing* (1993) 11-20.

[4] A. Yao, Quantum Circuit Complexity, *Proc. 34th Ann. Symp. Foundations of Computer Science* (1993) 352-361.

[5] P. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, *Proc. 35th Ann. Symp. Foundations of Computer Science* (1994) 124-134.

[6] K. Morita and M. Harao, Computation Universality of One-Dimensional Reversible (Injective) Cellular Automata, *Transactions of the IEICE*, Vol. E 72 (1989) 758-762.

[7] R. Cooke, *Infinite Matrices and Sequence Spaces,* Macmillan and Co., London, 1950.

[8] N. Young, *An Introduction to Hilbert Space,* Cambridge University Press, Cambridge, 1988.