INFORMATIQUE THÉORIQUE ET APPLICATIONS

MASANAO OZAWA
HARUMICHI NISHIMURA

Local transition functions of quantum Turing machines

Informatique théorique et applications, tome 34, n° 5 (2000), p. 379-402

<http://www.numdam.org/item?id=ITA_2000__34_5_379_0>

Theoretical Informatics and Applications
Theoret. Informatics Appl. **34** (2000) 379–402

LOCAL TRANSITION FUNCTIONS OF QUANTUM TURING MACHINES *

MASANAO OZAWA[1, 2] AND HARUMICHI NISHIMURA[1,2]

Abstract. Foundations of the notion of quantum Turing machines are investigated. According to Deutsch's formulation, the time evolution of a quantum Turing machine is to be determined by the local transition function. In this paper, the local transition functions are characterized for fully general quantum Turing machines, including multi-tape quantum Turing machines, extending the results due to Bernstein and Vazirani.

AMS Subject Classification. 68Q05, 81P10.

1. INTRODUCTION

Feynman [5] pointed out that a Turing machine cannot simulate a quantum mechanical process efficiently and suggested that a computing machine based on quantum mechanics might be more powerful than Turing machines. Deutsch introduced quantum Turing machines [3] and quantum circuits [4] for establishing the notion of quantum algorithm exploiting "quantum parallelism". A different approach to quantum Turing machines was taken earlier by Benioff [1] based on the Hamiltonian description of Turing machines. Bernstein and Vazirani [2] instituted quantum complexity theory based on quantum Turing machines and constructed an efficient universal quantum Turing machine. Yao [11] reformulated the quantum

Keywords and phrases: Quantum Turing machines, transition functions, multi-tape quantum Turing machines.

* *Main results of this work were presented at the 4th International Conference on Quantum Communication, Computing, and Measurement (Evanston, IL, August 22-27, 1998) by the first author and appeared in* Quantum Communication, Computing, and Measurement 2, *edited by P. Kumar et al., Plenum, New York (2000) pp. 241-248.*

[1] Graduate School of Human Informatics, School of Informatics and Sciences, Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan; e-mail: mozawa@math.human.nagoya-u.ac.jp & anishi@info.human.nagoya-u.ac.jp

[2] CREST, Japan Science and Technology.

circuit models by singling out the acyclic ones and showed that a computation by a quantum Turing machine can be simulated by a polynomial size quantum circuit. The search for an efficient quantum algorithm for a well-studied but presumably intractable problem was achieved strikingly by Shor [10], who found bounded error probability quantum polynomial time algorithms for the factoring problem and the discrete logarithm problem.

In this paper, foundations of the concept of quantum Turing machines are examined. In Deutsch's formulation [3], a quantum Turing machine is defined to be a quantum system consisting of a processor, a moving head, and a tape, obeying a unitary time evolution determined by local interactions between its components. The machine is then allowed to be in a superposition of computational configurations. Deutsch [3] pointed out that the global transition function between computational configurations should be determined by a local transition function which depends only on local configurations. Bernstein and Vazirani [2] found a simple characterization of the local transition functions for the restricted class of quantum Turing machines in which the head must move either to the right or to the left at each step. Since the above characterization constitutes an alternative definition of quantum Turing machines more tractable in the field of theoretical computer science, it is an interesting problem to find a general characterization valid even when the head is not required to move or more generally when the machine has more than one tape. The purpose of this paper is to solve this problem, while for this and foundational purposes we also provide a completely formal treatment of the theory of quantum Turing machines. Extending the Bernstein–Vazirani theory [2], the computational complexity theory for general quantum Turing machines defined by the conditions given in this paper will be published in our forthcoming paper [8].

The paper is organized as follows. In Section 2, quantum Turing machines are introduced along with Deutsch's original formulation. We extend Deutsch's formulation to the case where the head is not required to move every step. In Section 3, the local transition functions of quantum Turing machines are introduced along with Deutsch's requirement of operations by finite means and the problem of the characterization of local transition functions is formulated. In Section 4, quantum Turing machines are formulated as mathematical structures and we prove a characterization theorem of the local transition functions of quantum Turing machines. We adopt here the column vector approach, where the characterization is obtained from the requirement that the column vectors of the transition matrix are orthonormal. In Section 5, we prove an alternative characterization theorem of the local transition functions along with the row vector approach. In Section 6, the characterization is extended to multi-tape quantum Turing machines.

2. Quantum Turing machine as a physical system

A *quantum Turing machine* $\mathcal{Q}$ is a quantum system consisting of a *processor*, a bilateral infinite *tape*, and a *head* to read and write a symbol on the tape.

Its configuration is determined by the *processor configuration* q from a finite set Q of symbols, the *tape configuration* T represented by an infinite string from a finite set Σ of symbols, and the discretized *head position* ξ taking values in the set $\mathbb{Z}$ of integers. The tape consists of *cells* numbered by the integers. The head position $\xi \in \mathbb{Z}$ stands for the place of the cell numbered by ξ. We assume that Σ contains the symbol B representing the blank cell in the tape. For any integer m the symbol at the cell m on the tape is denoted by $T(m)$. We assume that the possible tape configurations are such that $T(m) = B$ except for finitely many cells m. The set of all the possible tape configurations is denoted by $\Sigma^{\#}$. The set $\Sigma^{\#}$ is a countable set. Thus, any configuration C of $\mathcal{Q}$ is represented by a triple $C = (q, T, \xi)$ in the configuration space $\mathcal{C}(Q, \Sigma) = Q \times \Sigma^{\#} \times \mathbb{Z}$. The quantum state of $\mathcal{Q}$ is represented by a unit vector in the Hilbert space $\mathcal{H}(Q, \Sigma)$ generated by the configuration space $\mathcal{C}(Q, \Sigma)$ so that the vectors in $\mathcal{H}(Q, \Sigma)$ can be identified with the square summable complex-valued functions defined on $Q \times \Sigma^{\#} \times \mathbb{Z}$. The complete orthonormal basis canonically in one-to-one correspondence with the configuration space is called the *computational basis*. Thus, the computational basis is represented by $|C\rangle = |q, T, \xi\rangle$ for any configuration $C = (q, T, \xi) \in \mathcal{C}(Q, \Sigma)$.

In classical physics, physical quantities are represented by real-valued functions defined on the phase space coordinated by the configuration and the generalized momentum. In quantum mechanics, they are called observables and represented by self-adjoint operators on the Hilbert space of quantum states. The procedure to define the observables from the classical description of the system is usually called the quantization. In order to define the observables quantizing the configurations, we assume the numbering of the sets Q and Σ such that $Q = \{q_0, \ldots, q_{|Q|-1}\}$ and $\Sigma = \{\sigma_0, \ldots, \sigma_{|\Sigma|-1}\}$, where we denote by $|X|$ the number of the elements of a set X. We define observables $\hat{q}$, $\hat{T}(m)$ for $m \in \mathbb{Z}$, and $\hat{\xi}$ representing the processor configuration, the symbol at the cell m, and the head position, respectively, as follows:

$$\hat{q} = \sum_{n=0}^{|Q|-1} n|q_n\rangle\langle q_n|, \quad \hat{T}(m) = \sum_{n=0}^{|\Sigma|-1} n|\sigma_n\rangle\langle\sigma_n|, \quad \hat{\xi} = \sum_{\xi\in\mathbb{Z}} \xi|\xi\rangle\langle\xi|.$$

The computation begins at $t = 0$ and proceeds in steps of a fixed unit duration τ. The dynamics of $\mathcal{Q}$ are described by a unitary operator U on $\mathcal{H}(Q, \Sigma)$ which specifies the evolution of the system during a single *computational step* so that we have

$$U^{\dagger}U = UU^{\dagger} = I, \quad |\psi(n\tau)\rangle = U^n|\psi(0)\rangle$$

for all positive integers n.

3. Local transition functions

Deutsch [3] required that the quantum Turing machine operates finitely, *i.e.*, (i) only a finite system is in motion during any one step, (ii) the motion depends only on the quantum state of a local subsystem, and (iii) the rule that specifies

the motion can be given finitely in the mathematical sense. To satisfy the above requirements, the matrix elements of U are required to take the following form[1]:

$$\langle q', T', \xi' | U | q, T, \xi \rangle = \begin{cases} \delta(q, T(\xi), q', T'(\xi), 1) & \text{if } \xi' = \xi + 1 \\ \delta(q, T(\xi), q', T'(\xi), 0) & \text{if } \xi' = \xi \\ \delta(q, T(\xi), q', T'(\xi), -1) & \text{if } \xi' = \xi - 1 \end{cases} \tag{3.1}$$

whenever $T'(m) = T(m)$ for all $m \neq \xi$, and $\langle q', T', \xi' | U | q, T, \xi \rangle = 0$ otherwise, for any configurations (q, T, ξ) and (q', T', ξ'). The above condition ensures that the tape is changed only at the head position ξ at the beginning of each computational step, and that during each step the head position cannot change by more than one unit. The function $\delta(q, T(\xi), q', T'(\xi), d)$, where $q, q' \in Q$, $T(\xi), T'(\xi) \in \Sigma$, and $d \in \{-1, 0, 1\}$, represents a dynamical motion depending only on the local observables $\hat{q}$ and $\hat{T}(\xi)$. It follows that the relation $\delta(q, \sigma, q', \tau, d) = c$ can be interpreted as the following operation of $\mathcal{Q}$: if the processor is in the configuration q and if the head reads the symbol σ, then it follows with the amplitude c that the processor configuration turns to q', the head writes the symbol τ, and that the head moves one cell to the right if $d = 1$, to the left if $d = -1$, or does not move if $d = 0$. We call δ the *local transition function* of the quantum Turing machine $\mathcal{Q}$.

The local transition function δ can be arbitrarily given except for the requirement that U be unitary. Each choice defines a different quantum Turing machine $\mathcal{Q}[\delta]$ with the same configuration space $C(Q, \Sigma)$. Thus, if we have an intrinsic characterization of the local transition function δ, quantum Turing machines can be defined formally without referring to the unitary operator U as a primitive notion.

From equation (3.1), the time evolution operator U is determined conversely from the local transition function δ by

$$U | q, T, \xi \rangle = \sum_{p, \tau, d} \delta(q, T(\xi), p, \tau, d) | p, T_\xi^\tau, \xi + d \rangle \tag{3.2}$$

for any configuration (q, T, ξ), where T_ξ^τ is the tape configuration defined by

$$T_\xi^\tau(m) = \begin{cases} \tau & \text{if } m = \xi, \\ T(m) & \text{if } m \neq \xi. \end{cases}$$

Now we can formulate the characterization problem of local transition functions of quantum Turing machines: *Let δ be a complex-valued function on $Q \times \Sigma \times Q \times \Sigma \times \{-1, 0, 1\}$ and let U be the operator on $\mathcal{H}(Q, \Sigma)$ defined by equation (3.2). Then, what conditions ensure that the operator U is unitary?*

This problem is answered by the following statement: *The operator U is unitary if and only if δ satisfies the following conditions.*

[1]This condition is a natural extension of Deutsch's condition [3] to the case where the head is not required to move.

(a) *For any* $(q,\sigma) \in Q \times \Sigma$,

$$\sum_{p,\tau,d} |\delta(q,\sigma,p,\tau,d)|^2 = 1.$$

(b) *For any* $(q,\sigma),(q',\sigma') \in Q \times \Sigma$ *with* $(q,\sigma) \neq (q',\sigma')$,

$$\sum_{p,\tau,d} \delta(q',\sigma',p,\tau,d)^* \delta(q,\sigma,p,\tau,d) = 0.$$

(c) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$, *we have*

$$\sum_{p\in Q,d=0,1} \delta(q',\sigma',p,\tau',d-1)^* \delta(q,\sigma,p,\tau,d) = 0.$$

(d) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$, *we have*

$$\sum_{p\in Q} \delta(q',\sigma',p,\tau',-1)^* \delta(q,\sigma,p,\tau,1) = 0.$$

The proof will be given in the next section. If it is assumed that the head must move either to the right or to the left at each step (two-way quantum Turing machines), condition (c) is automatically satisfied. In this case, the above statement is reduced to the result due to Bernstein and Vazirani [2]. In Section 5, we will also characterize the local transition functions of multi-tape quantum Turing machines.

In order to maintain the Church–Turing thesis, we need to require that the unitary operator U is constructive, or that the range of the local transition function δ is in the computable complex numbers. From the complexity theoretical point of view, we need also to require that the matrix elements of U are polynomially computable complex numbers, or that the range of the transition function δ is in the polynomially computable complex numbers.

4. Quantum Turing machine as a mathematical structure

In order to formulate the notion of a quantum Turing machine as a formal mathematical structure rather than a well-described physical system, we shall introduce the following mathematical definitions. A *Turing frame* is a pair (Q,Σ) of a finite set Q and a finite set Σ with a specific element denoted by B. In what follows, let (Q,Σ) be a Turing frame. Let $\Sigma^{\#}$ be the set of functions T from the set $\mathbb{Z}$ of integers to Σ such that $T(m) = B$ except for finitely many $m \in \mathbb{Z}$. The *configuration space* of (Q,Σ) is the product set $\mathcal{C}(Q,\Sigma) = Q \times \Sigma^{\#} \times \mathbb{Z}$.

For any $(p,\tau,d) \in Q \times \Sigma \times \{-1,0,1\}$, denote by $\mathcal{C}(p,\tau,d)$ the set of configurations $(p,T,\xi) \in \mathcal{C}(Q,\Sigma)$ such that $T(\xi - d) = \tau$. Let $(p,\tau,d) \in Q \times \Sigma \times \{-1,0,1\}$.

We define the transformation $\alpha(p,\tau,d)$ from $\mathcal{C}(Q,\Sigma)$ to $\mathcal{C}(p,\tau,d)$ by

$$\alpha(p,\tau,d)(q,T,\xi) = (p, T^{\tau}_{\xi}, \xi + d) \tag{4.1}$$

for all $(q,T,\xi) \in \mathcal{C}(Q,\Sigma)$. It is easy to see that $\alpha(p,\tau,d)$ represents the operation such that the processor configuration turns to p, the head writes the symbol τ, and then moves with $|d|$ step to the direction d. We define the transformation $\beta(p,\tau,d)$ from $\mathcal{C}(Q,\Sigma)$ to $\mathcal{C}(p,\tau,0)$ by

$$\beta(p,\tau,d)(q,T,\xi) = (p, T^{\tau}_{\xi-d}, \xi - d) \tag{4.2}$$

for any $(q,T,\xi) \in \mathcal{C}(Q,\Sigma)$. It is easy to see that $\beta(p,\tau,d)$ represents the operation such that the processor configuration turns to p, the head moves with $|d|$ step to the direction $-d$ and then writes the symbol τ. The following proposition can be checked by straightforward verifications.

Proposition 4.1. (i) *Let* $d \in \{-1,0,1\}$. *If* $(q,\sigma) \neq (q',\sigma') \in Q\times\Sigma$ *then* $\mathcal{C}(q,\sigma,d)\cap \mathcal{C}(q',\sigma',d) = \emptyset$ *and*

$$\mathcal{C}(Q,\Sigma) = \bigcup_{(q,\sigma)\in Q\times\Sigma} \mathcal{C}(q,\sigma,d).$$

(ii) *Let* $(q,\sigma,p,\tau,d) \in Q\times\Sigma\times Q\times\Sigma\times\{-1,0,1\}$. *We have*

$$\beta(q,\sigma,d)\alpha(p,\tau,d)C = C$$

for all $C \in \mathcal{C}(q,\sigma,0)$ *and*

$$\alpha(p,\tau,d)\beta(q,\sigma,d)C' = C'$$

for all $C' \in \mathcal{C}(p,\tau,d)$.

(iii) *The mapping* $\alpha(p,\tau,d)$ *restricted to* $\mathcal{C}(q,\sigma,0)$ *has the inverse mapping* $\beta(q,\sigma,d)$ *restricted to* $\mathcal{C}(p,\tau,d)$, *i.e.*,

$$\mathcal{C}(q,\sigma,0) \underset{\beta(q,\sigma,d)}{\overset{\alpha(p,\tau,d)}{\rightleftarrows}} \mathcal{C}(p,\tau,d).$$

A configuration (q,T,ξ) is said to *precede* a configuration (q',T',ξ'), in symbols $(q,T,\xi) \prec (q',T',\xi')$, if $T'(m) = T(m)$ for all $m \neq \xi$ and $|\xi' - \xi| \leq 1$.

Proposition 4.2. *For any* $C, C' \in \mathcal{C}(Q,\Sigma)$, *the following conditions are equivalent.*

(i) $C \prec C'$.

(ii) *There is some* $(p,\tau,d) \in Q\times\Sigma\times\{-1,0,1\}$ *such that* $C' = \alpha(p,\tau,d)C$.

(iii) *There is some* $(q,\sigma,d) \in Q\times\Sigma\times\{-1,0,1\}$ *such that* $C = \beta(q,\sigma,d)C'$.

Proof. Let $C = (q, T, \xi)$ and $C' = (q', T', \xi')$.
(i) $\Rightarrow$ (ii): If (i) holds, we have $C' = \alpha(q', T'(\xi), \xi' - \xi)C$ so that (ii) holds.
(ii) $\Rightarrow$ (iii): Suppose that (ii) holds. Since $C \in \mathcal{C}(q, T(\xi), 0)$, by Proposition 4.1 (ii) we have

$$\beta(q, T(\xi), d)C' = \beta(q, T(\xi), d)\alpha(p, \tau, d)C = C.$$

(iii) $\Rightarrow$ (i): If (iii) holds, we have $C = (p, T'^{\sigma}_{\xi'-d}, \xi' - d)$ and hence $\xi' - \xi = d$ and $T(m) = T'^{\sigma}_{\xi'-d}(m) = T'(m)$ for $m \neq \xi' - d = \xi$ so that (i) holds. □

The *quantum state space* of the Turing frame (Q, Σ) is the Hilbert space $\mathcal{H}(Q, \Sigma)$ spanned by $\mathcal{C}(Q, \Sigma)$ with the canonical basis $\{|C\rangle |\ C \in \mathcal{C}(Q, \Sigma)\}$ called the *computational basis.* A *local transition function* for (Q, Σ) is a function from $Q \times \Sigma \times Q \times \Sigma \times \{-1, 0, 1\}$ into the complex number field $\mathbb{C}$.

In what follows, let δ be a local transition function for (Q, Σ). The *evolution operator* of δ is a linear operator M_δ on $\mathcal{H}(Q, \Sigma)$ such that

$$M_\delta |q, T, \xi\rangle = \sum_{p,\tau,d} \delta(q, T(\xi), p, \tau, d)|p, T^{\tau}_{\xi}, \xi + d\rangle \tag{4.3}$$

for all $(q, T, \xi) \in \mathcal{C}(Q, \Sigma)$; the summation $\sum_{p,\tau,d}$ is taken over all $(p, \tau, d) \in Q \times \Sigma \times \{-1, 0, 1\}$ above and in the rest of this section unless stated otherwise. Equation (4.3) uniquely defines the bounded operator M_δ on the space $\mathcal{H}(Q, \Sigma)$ as shown in Appendix A.

Let (q, T, ξ), $(q', T', \xi') \in \mathcal{C}(Q, \Sigma)$. The following formula can be verified from equation (4.3) by straightforward calculation.

$$\langle q', T', \xi' | M_\delta | q, T, \xi\rangle = \begin{cases} \delta(q, T(\xi), q', T'(\xi), \xi' - \xi) & \text{if } (q, T, \xi) \prec (q', T', \xi'), \\ 0 & \text{otherwise.} \end{cases} \tag{4.4}$$

A configuration (q, T, ξ) is said to be *locally like* a configuration (q', T', ξ') if $q = q'$ and $T(\xi + d) = T'(\xi' + d)$ for all $d \in \{-1, 0, 1\}$.

Lemma 4.3. *For any $C_1, C_2 \in \mathcal{C}(Q, \Sigma)$, if they are locally like each other, we have*

$$\langle C_1 | M_\delta M_\delta^\dagger | C_1\rangle = \langle C_2 | M_\delta M_\delta^\dagger | C_2\rangle.$$

Proof. Let $\tau_{-1}, \tau_0, \tau_1 \in \Sigma$. Suppose that a configuration $C' = (p, T', \xi')$ is such that $T'(\xi' - d) = \tau_d$ for all $d \in \{-1, 0, 1\}$. Since every configuration locally like C' also satisfies the above condition, it suffices to show that $\langle C' | M_\delta M_\delta^\dagger | C'\rangle$ depends

only on $p, \tau_{-1}, \tau_0, \tau_1$. By Proposition 4.2 and equation (4.4) we have

$$\begin{aligned}
\langle C'|M_\delta M_\delta^\dagger|C'\rangle &= \sum_{C\in\mathcal{C}(Q,\Sigma)} |\langle C'|M_\delta|C\rangle|^2 \\
&= \sum_{C\prec C'} |\langle C'|M_\delta|C\rangle|^2 \\
&= \sum_{q,\sigma,d} |\langle C'|M_\delta|\beta(q,\sigma,d)C'\rangle|^2 \\
&= \sum_{q,\sigma,d} |\langle p, T', \xi'|M_\delta|q, T'^{\sigma}_{\xi'-d}, \xi'-d\rangle|^2 \\
&= \sum_{q,\sigma,d} |\delta(q, T'^{\sigma}_{\xi'-d}(\xi'-d), p, T'(\xi'-d), d)|^2 \\
&= \sum_{q,\sigma,d} |\delta(q,\sigma,p,\tau_d,d)|^2.
\end{aligned}$$

The first equality above follows from Parseval's identity.

Thus, $\langle C'|M_\delta M_\delta^\dagger|C'\rangle$ depends only on $p, \tau_{-1}, \tau_0, \tau_1$ and the proof is completed. □

For the case where the head is required to move, a proof of the following lemma appeared first in [2]. The following proof not only covers the general case but also simplifies the argument given in [2].

Lemma 4.4. *The evolution operator M_δ of a local transition function δ is unitary if it is an isometry.*

Proof. Suppose that M_δ is an isometry, *i.e.*, $M_\delta^\dagger M_\delta = 1$. Obviously, $M_\delta M_\delta^\dagger$ is a projection. If $\langle C|M_\delta M_\delta^\dagger|C\rangle = 1$ for every $C \in \mathcal{C}(Q,\Sigma)$, the computational basis is included in the range of $M_\delta M_\delta^\dagger$ and then, since the range of any projection is a closed linear subspace, we have $M_\delta M_\delta^\dagger = 1$ so that M_δ is unitary. Thus, it suffices to show that $\langle C|M_\delta M_\delta^\dagger|C\rangle = 1$ for every $C \in \mathcal{C}(Q,\Sigma)$. To show this, suppose that there is a configuration $C_0 \in \mathcal{C}(Q,\Sigma)$ such that $\langle C_0|M_\delta M_\delta^\dagger|C_0\rangle = 1-\epsilon$ with $\epsilon > 0$. For any $n > 2$ and $d \in \{-1, 0, 1\}$, let $S(n,d)$ be the set of configurations such that

$$S(n,d) = \{(q,T,\xi) \in \mathcal{C}(Q,\Sigma)|\ T(m) = B \ \text{ for all } \ m \notin \{1,\dots,n\} \text{ and } \xi \in \{1-d,\dots,n+d\}\}.$$

Let

$$A = \sum_{(C,C')\in S(n,0)\times S(n,1)} |\langle C'|M_\delta|C\rangle|^2 \tag{4.5}$$

and we shall consider evaluations of A in terms of the numbers of elements of the sets $S(n,0)$ and $S(n,1)$. It is easy to see that if $C \in S(n,0)$ and $C \prec C'$

then $C' \in S(n,1)$. It follows from equation (4.4) that $\langle C'|M_\delta|C\rangle = 0$ for any pair (C,C') with $C \in S(n,0)$ and $C' \notin S(n,1)$ so that the summation over $(C,C') \in S(n,0)\times S(n,1)$ in equation (4.5) can be replaced by the summation over $(C,C') \in S(n,0) \times \mathcal{C}(Q,\Sigma)$. By Parseval's identity, we have

$$A = \sum_{(C,C')\in S(n,0)\times\mathcal{C}(Q,\Sigma)} |\langle C'|M_\delta|C\rangle|^2 = \sum_{C\in S(n,0)} \langle C|M_\delta^\dagger M_\delta|C\rangle.$$

Since M_δ is an isometry, we have

$$A = |S(n,0)|.$$

Let $S(C_0)$ be the set of all configurations in $S(n,-1)$ locally like C_0. Then, $S(C_0) \subseteq S(n,1)$. By Lemma 4.3, $\langle C'|M_\delta M_\delta^\dagger|C'\rangle = 1-\epsilon$ for all $C' \in S(C_0)$. Thus, we have

$$\begin{aligned} A &\le \sum_{(C,C')\in\mathcal{C}(Q,\Sigma)\times S(n,1)} |\langle C'|M_\delta|C\rangle|^2 = \sum_{C'\in S(n,1)} \langle C'|M_\delta M_\delta^\dagger|C'\rangle \\ &\le (1-\epsilon)|S(C_0)| + |S(n,1)| - |S(C_0)| = |S(n,1)| - \epsilon|S(C_0)|. \end{aligned}$$

The cardinalities of $S(n,d)$ and $S(C_0)$ are given by $|S(n,d)| = (n+2d)|Q|\,|\Sigma|^n$ and $|S(C_0)| = (n-2)|\Sigma|^{n-3}$. Therefore, we have

$$|\Sigma|^{n-3}(2|Q||\Sigma|^3 - \epsilon(n-2)) = |S(n,1)| - \epsilon|S(C_0)| - |S(n,0)| \ge 0$$

for all $n > 2$. But, for $n > 2 + 2\epsilon^{-1}|Q||\Sigma|^3$, this yields an obvious contradiction and the proof is completed. □

According to discussions in Section 3, a quantum Turing machine can be defined as a mathematical structure (Q,Σ,δ) consisting of a Turing frame (Q,Σ) and a local transition function δ such that the evolution operator M_δ is unitary. The following theorem characterizes intrinsically the local transition functions that give rise to quantum Turing machines.

Theorem 4.5. *The evolution operator M_δ of a local transition function δ for the Turing frame (Q,Σ) is unitary if and only if δ satisfies the following conditions.*

(a) *For any $(q,\sigma) \in Q\times\Sigma$,*

$$\sum_{p,\tau,d} |\delta(q,\sigma,p,\tau,d)|^2 = 1.$$

(b) *For any $(q,\sigma),(q',\sigma') \in Q\times\Sigma$ with $(q,\sigma) \neq (q',\sigma')$,*

$$\sum_{p,\tau,d} \delta(q',\sigma',p,\tau,d)^*\delta(q,\sigma,p,\tau,d) = 0.$$

(c) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$, *we have*

$$\sum_{p\in Q,d=0,1} \delta(q',\sigma',p,\tau',d-1)^*\delta(q,\sigma,p,\tau,d) = 0.$$

(d) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$, *we have*

$$\sum_{p\in Q} \delta(q',\sigma',p,\tau',-1)^*\delta(q,\sigma,p,\tau,1) = 0.$$

Proof. Let δ be a local transition function for a Turing frame (Q,Σ). Let $C = (q,T,\xi) \in \mathcal{C}(Q,\Sigma)$. From equation (4.3) we have

$$\begin{aligned}\langle C|M_\delta^\dagger M_\delta|C\rangle &= \sum_{p,\tau,d}\sum_{p',\tau',d'} \delta(q,T(\xi),p',\tau',d')^*\delta(q,T(\xi),p,\tau,d)\langle p',T_\xi^{\tau'},\xi+d'|p,T_\xi^\tau,\xi+d\rangle \\ &= \sum_{p,\tau,d} |\delta(q,T(\xi),p,\tau,d)|^2.\end{aligned}$$

Since for any $\sigma \in \Sigma$ there are some $T \in \Sigma^\#$ and $\xi \in \mathbb{Z}$ such that $T(\xi) = \sigma$, condition (a) holds if and only if $\langle C|M_\delta^\dagger M_\delta|C\rangle = 1$ for any $C \in \mathcal{C}(Q,\Sigma)$.

Let $C = (q,T,\xi) \in \mathcal{C}(Q,\Sigma)$ and $C' = (q',T',\xi') \in \mathcal{C}(Q,\Sigma)$. From equation (4.3) we have

$$\begin{aligned}\langle C'|M_\delta^\dagger M_\delta|C\rangle &= \sum_{p,\tau,d}\sum_{p',\tau',d'} \delta(q',T'(\xi'),p',\tau',d')^*\delta(q,T(\xi),p,\tau,d)\langle p',T'^{\tau'}_{\xi'},\xi'+d'|p,T_\xi^\tau,\xi+d\rangle \\ &= \sum{}^*\delta(q',T'(\xi'),p,\tau',d')^*\delta(q,T(\xi),p,\tau,d),\end{aligned}$$

where the summation $\sum^*$ is taken over all $p \in Q$, $\tau,\tau' \in \Sigma$, and $d,d' \in \{-1,0,1\}$ such that $T_\xi^\tau = T'^{\tau'}_{\xi'}$ and $\xi + d = \xi' + d'$.

For any $k \in \mathbb{Z}$, let $\mathcal{C}(k)$ be a subset of $\mathcal{C}(Q,\Sigma)^2$ consisting of all pairs $C = (q,T,\xi)$ and $C' = (q',T',\xi')$ with $C \neq C'$ such that $T(m) = T'(m)$ for all $m \notin \{\xi,\xi'\}$ and that $\xi' - \xi = k$. It is easy to see that if $C \neq C'$ and

$$(C,C') \notin \bigcup_{k\in\{0,\pm1,\pm2\}} \mathcal{C}(k)$$

then $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$. We shall show that condition (b), (c), or (d) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C,C') \in \mathcal{C}(0)$, $(C,C') \in \mathcal{C}(1)$, or $(C,C') \in \mathcal{C}(2)$, respectively.

For any $(C,C') \in \mathcal{C}(0)$ with $C = (q,T,\xi)$ and $C' = (q',T',\xi')$, we have $T_\xi^\tau = T'^{\tau'}_{\xi'}$ and $\xi + d = \xi' + d'$ if and only if $\tau = \tau'$ and $d = d'$, so that we have

$$\langle C'|M_\delta^\dagger M_\delta|C\rangle = \sum_{p,\tau,d} \delta(q',T'(\xi'),p,\tau,d)^*\delta(q,T(\xi),p,\tau,d).$$

Since for any $(q,\sigma),(q',\sigma') \in Q \times \Sigma$ with $(q,\sigma) \neq (q',\sigma')$ there are configurations $C = (q,T,\xi)$ and $C' = (q',T',\xi')$ such that $(C,C') \in \mathcal{C}(0)$, $T(\xi) = \sigma$ and $T'(\xi') = \sigma'$, condition (b) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ for all $(C,C') \in \mathcal{C}(0)$.

For any $(C,C') \in \mathcal{C}(1)$ with $C = (q,T,\xi)$ and $C' = (q',T',\xi')$, we have $T_\xi^\tau = T'^{\tau'}_{\xi'}$ and $\xi + d = \xi' + d'$ if and only if $\tau = T'(\xi)$, $\tau' = T(\xi')$, and $(d,d') \in \{(0,-1),(1,0)\}$, so that we have

$$\langle C'|M_\delta^\dagger M_\delta|C\rangle = \sum_{p\in Q,d=0,1} \delta(q',T'(\xi'),p,T(\xi'),d-1)^*\delta(q,T(\xi),p,T'(\xi),d).$$

Since for any $(q,\sigma,\tau),(q',\sigma',\tau') \in Q\times\Sigma^2$ there are configurations $C = (q,T,\xi)$ and $C' = (q',T',\xi')$ such that $C,C' \in \mathcal{C}(1)$, $(T(\xi),T'(\xi)) = (\sigma,\tau)$, and $(T'(\xi'),T(\xi')) = (\sigma',\tau')$, condition (c) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ for any $(C,C') \in \mathcal{C}(1)$.

For any $(C,C') \in \mathcal{C}(2)$ with $C = (q,T,\xi)$ and $C' = (q',T',\xi')$, we have $T_\xi^\tau = T'^{\tau'}_{\xi'}$ and $\xi + d = \xi' + d'$ if and only if $\tau = T'(\xi)$, $\tau' = T(\xi')$, $d = 1$, and $d' = -1$, so that we have

$$\langle C'|M_\delta^\dagger M_\delta|C\rangle = \sum_{p\in Q} \delta(q',T'(\xi'),p,T(\xi'),-1)^*\delta(q,T(\xi),p,T'(\xi),1).$$

Thus, condition (d) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ for all $(C,C') \in \mathcal{C}(2)$.

Since $M_\delta^\dagger M_\delta$ is self-adjoint, M_δ is an isometry if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = \langle C'|C\rangle$ for any $C = (q,T,\xi)$, $C' = (q',T',\xi') \in \mathcal{C}(Q,\Sigma)$ with $\xi \leq \xi'$. Therefore, we have proved that conditions (a–d) hold if and only if M_δ is an isometry. Now, Lemma 4.4 concludes the assertion. □

A quantum Turing machine $M = (Q,\Sigma,\delta)$ is called *unidirectional*, if we have $d = d'$ whenever $\delta(q,\sigma,p,\tau,d)\delta(q',\sigma',p,\tau',d') \neq 0$ for any $q,q' \in Q$, $\sigma,\sigma',\tau,\tau' \in \Sigma$, and $d,d' \in \{-1,0,1\}$. It is easy to see that conditions (c) and (d) are automatically satisfied by every unidirectional quantum Turing machine. Thus, if every quantum Turing machine can be efficiently simulated by a unidirectional one without error, complexity theoretical consideration on quantum Turing machines can be done much easier. For two-way quantum Turing machines, this was shown by Bernstein and Vazirani [2]. For general quantum Turing machines defined by the above conditions, the positive answer will be given in our forthcoming

paper [8], including extension to multi-tape quantum Turing machines defined by the conditions of Theorem 6.2.

5. Alternative approaches to the characterization of local transition functions

Hirvensalo [7] gave the following set of conditions for a local transition function δ to give the unitary evolution operator (see also [6]):

(H-a) For any $(q,\sigma) \in Q \times \Sigma$,

$$\sum_{p,\tau,d} |\delta(q,\sigma,p,\tau,d)|^2 = 1.$$

(H-b) For any $(q,\sigma),(q',\sigma') \in Q \times \Sigma$ with $(q,\sigma) \neq (q',\sigma')$,

$$\sum_{p,\tau,d} \delta(q',\sigma',p,\tau,d)^* \delta(q,\sigma,p,\tau,d) = 0.$$

(H-c) For any $(p,\tau,d),(p',\tau',d') \in Q \times \Sigma \times \{-1,0,1\}$ with $(p,\tau,d) \neq (p',\tau',d')$, we have

$$\sum_{(q,\sigma)\in Q\times\Sigma} \delta(q,\sigma,p,\tau,d)^* \delta(q,\sigma,p',\tau',d') = 0.$$

(H-d) For any $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$ and $d \neq d' \in \{-1,0,1\}$, we have

$$\sum_{p\in Q} \delta(q,\sigma,p,\tau,d)^* \delta(q',\sigma',p,\tau',d') = 0.$$

However, the above set of conditions consists of only a sufficient condition, not a necessary one. To show this, let $Q = \{0,1\}$, $\Sigma = \{B\}$, and define a local transition function δ as follows.

$$\begin{array}{lll}
\delta(0,B,0,B,-1) = 0, & \delta(0,B,0,B,0) = 1/2, & \delta(0,B,0,B,1) = -1/2, \\
\delta(0,B,1,B,-1) = 1/2, & \delta(0,B,1,B,0) = 1/2, & \delta(0,B,1,B,1) = 0, \\
\delta(1,B,0,B,-1) = 0, & \delta(1,B,0,B,0) = 1/2, & \delta(1,B,0,B,1) = 1/2, \\
\delta(1,B,1,B,-1) = 1/2, & \delta(1,B,1,B,0) = -1/2, & \delta(1,B,1,B,1) = 0.
\end{array}$$

Then, δ satisfies conditions (a–d) of Theorem 4.5 and hence gives the unitary evolution operator, but does not satisfy Hirvensalo's conditions. In fact, δ does not satisfy condition (H-c), since

$$\delta(0,B,0,B,0)^* \delta(0,B,1,B,-1) + \delta(1,B,0,B,0)^* \delta(1,B,1,B,-1) = 1/2,$$

and δ does not satisfy condition (H-d), since

$$\delta(0,B,0,B,0)^*\delta(1,B,0,B,1)+\delta(0,B,1,B,0)^*\delta(1,B,1,B,1)=1/4.$$

Thus, conditions (H-d) and (H-c) are not necessary.

The conditions in Theorem 4.4 are obtained from the requirement that the column vectors of the evolution operator are orthonormal in the matrix representation in the computational basis. Hirvensalo's conditions mix requirements for column vectors and for row vectors. In the rest of this section, from the sole requirement that the row vectors are orthonormal, we shall obtain a set of necessary and sufficient conditions for the unitarity of the evolution operator.

The proof of the following lemma is similar to that of Lemma 4.4.

Lemma 5.1. *The evolution operator M_δ of a local transition function δ is unitary if $M_\delta M_\delta^\dagger = 1$.*

Now we give another characterization of the local transition functions that give rise to quantum Turing machines.

Theorem 5.2. *The evolution operator M_δ of a local transition function δ for the Turing frame (Q,Σ) is unitary if and only if δ satisfies the following conditions.*

(a) *For any $p\in Q$ and $\tau_{-1},\tau_0,\tau_1\in\Sigma$,*

$$\sum_{q\in Q,\sigma\in\Sigma,d\in\{-1,0,1\}}|\delta(q,\sigma,p,\tau_d,d)|^2=1.$$

(b) *For any $p,p'\in Q$ with $p\neq p'$ and any $\tau_{-1},\tau_0,\tau_1\in\Sigma$,*

$$\sum_{q\in Q,\sigma\in\Sigma,d\in\{-1,0,1\}}\delta(q,\sigma,p',\tau_d,d)^*\delta(q,\sigma,p,\tau_d,d)=0.$$

(c) *For any $p,p'\in Q$ and $\tau_0,\tau_1\in\Sigma$,*

$$\sum_{q\in Q,\sigma\in\Sigma,d=0,1}\delta(q,\sigma,p',\tau_d,d-1)^*\delta(q,\sigma,p,\tau_d,d)=0.$$

(d) *For any $(p,\tau),(p',\tau')\in Q\times\Sigma$ with $\tau\neq\tau'$ and any $d\in\{-1,0,1\}$, we have*

$$\sum_{q\in Q,\sigma\in\Sigma}\delta(q,\sigma,p',\tau',d)^*\delta(q,\sigma,p,\tau,d)=0.$$

(e) *For any $(p,\tau),(p',\tau')\in Q\times\Sigma$ with $\tau\neq\tau'$ and any $d=0,1$, we have*

$$\sum_{q\in Q,\sigma\in\Sigma}\delta(q,\sigma,p',\tau',d-1)^*\delta(q,\sigma,p,\tau,d)=0.$$

(f) *For any* $(p,\tau),(p',\tau') \in Q \times \Sigma$, *we have*

$$\sum_{q\in Q,\sigma\in\Sigma} \delta(q,\sigma,p',\tau',-1)^*\delta(q,\sigma,p,\tau,1) = 0.$$

Proof. Let δ be a local transition function for a Turing frame (Q,Σ). Let $C = (p,T,\xi) \in \mathcal{C}(Q,\Sigma)$. From Proposition 4.2 and equation (4.4), we have

$$\begin{aligned}
M_\delta^\dagger|p,T,\xi\rangle &= \sum_{C'\in\mathcal{C}(Q,\Sigma)} |C'\rangle\langle C'|M_\delta^\dagger|C\rangle \\
&= \sum_{C':C'\prec C} \langle C|M_\delta|C'\rangle^*|C'\rangle \\
&= \sum_{q,\sigma,d} \langle C|M_\delta|\beta(q,\sigma,d)C\rangle^*|\beta(q,\sigma,d)C\rangle \\
&= \sum_{q,\sigma,d} \langle p,T,\xi|M_\delta|q,T^\sigma_{\xi-d},\xi-d\rangle^*|q,T^\sigma_{\xi-d},\xi-d\rangle \\
&= \sum_{q,\sigma,d} \delta(q,T^\sigma_{\xi-d}(\xi-d),p,T(\xi-d),d)^*|q,T^\sigma_{\xi-d},\xi-d\rangle \\
&= \sum_{q,\sigma,d} \delta(q,\sigma,p,T(\xi-d),d)^*|q,T^\sigma_{\xi-d},\xi-d\rangle. \qquad (5.1)
\end{aligned}$$

From equation (5.1) we have

$$\begin{aligned}
\langle C|M_\delta M_\delta^\dagger|C\rangle &= \sum_{q,\sigma,d}\sum_{q',\sigma',d'} \delta(q,\sigma,p,T(\xi-d),d)^*\delta(q',\sigma',p,T(\xi-d'),d') \\
&\quad \times\langle q',T^{\sigma'}_{\xi-d'},\xi-d'|q,T^\sigma_{\xi-d},\xi-d\rangle \\
&= \sum_{q,\sigma,d} |\delta(q,\sigma,p,T(\xi-d),d)|^2.
\end{aligned}$$

Since for any $\tau_{-1},\tau_0,\tau_1 \in \Sigma$ there are some $T \in \Sigma^\#$ and $\xi \in \mathbb{Z}$ such that $T(\xi-d) = \tau_d$, condition (a) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C\rangle = 1$ for any $C \in \mathcal{C}(Q,\Sigma)$.

Let $C = (p,T,\xi) \in \mathcal{C}(Q,\Sigma)$ and $C' = (p',T',\xi') \in \mathcal{C}(Q,\Sigma)$. From equation (5.1) we have

$$\begin{aligned}
\langle C|M_\delta M_\delta^\dagger|C'\rangle &= \sum_{q,\sigma,d}\sum_{q',\sigma',d'} \delta(q',\sigma',p',T'(\xi'-d'),d')^*\delta(q,\sigma,p,T(\xi-d),d) \\
&\quad \times\langle q,T^\sigma_{\xi-d},\xi-d|q',T'^{\sigma'}_{\xi'-d'},\xi'-d'\rangle \\
&= \sum\nolimits^{**} \delta(q,\sigma,p',T'(\xi'-d'),d')^*\delta(q,\sigma,p,T(\xi-d),d),
\end{aligned}$$

where the summation $\sum^{**}$ is taken over all $q \in Q$, $\sigma \in \Sigma$, and $d,d' \in \{-1,0,1\}$ such that $T^\sigma_{\xi-d} = T'^\sigma_{\xi'-d'}$ and $\xi - d = \xi' - d'$.

For any $k \in \mathbb{Z}$ and $d \in \{-1,0,1\}$, let $A(k)$ be a subset of $\mathcal{C}(Q,\Sigma)^2$ consisting of all pairs $C = (p,T,\xi)$ and $C' = (p',T',\xi')$ with $C \neq C'$, $T = T'$ and $\xi - \xi' = k$, and $B(k,d)$ be a subset of $\mathcal{C}(Q,\Sigma)^2$ consisting of all pairs $C = (p,T,\xi)$ and $C' = (p',T',\xi')$ with $T \neq T'$ and $\xi - \xi' = k$ such that $T(m) = T'(m)$ for all $m \neq \xi - d$. It is easy to see that if $C \neq C'$ and

$$(C,C') \notin \left(\bigcup_{k\in\{0,\pm1,\pm2\}} A(k) \right) \cup \left(\bigcup_{(k,d):|k-d|\leq 1} B(k,d) \right)$$

then $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$. Let $B(0) = B(0,1) \cup B(0,0) \cup B(0,-1)$ and $B(1) = B(1,1) \cup B(1,0)$. We shall show that condition (b), (c), (d), (e) or (f) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in A(0)$, $(C,C') \in A(1)$, $(C,C') \in B(0)$, $(C,C') \in B(1)$, or $(C,C') \in A(2) \cup B(2,1)$, respectively.

For any $(C,C') \in A(0)$ with $C = (p,T,\xi)$ and $C' = (p',T,\xi)$, we have $T^\sigma_{\xi-d} = T^\sigma_{\xi-d'}$ and $\xi - d = \xi - d'$ if and only if $d = d'$, so that we have

$$\langle C|M_\delta M_\delta^\dagger|C'\rangle = \sum_{q,\sigma,d} \delta(q,\sigma,p',T(\xi-d),d)^*\delta(q,\sigma,p,T(\xi-d),d).$$

Since for any $p,p' \in Q$ with $p \neq p'$ and any $\tau_{-1},\tau_0,\tau_1 \in \Sigma$ there are configurations $C = (p,T,\xi)$ and $C' = (p',T,\xi)$ such that $(C,C') \in A(0)$ and $T(\xi-d) = \tau_d$ for all $d \in \{-1,0,1\}$, condition (b) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for
all $(C,C') \in A(0)$.

For any $(C,C') \in A(1)$ with $C = (p,T,\xi)$ and $C' = (p',T,\xi')$, we have $T^\sigma_{\xi-d} = T^\sigma_{\xi'-d'}$ and $\xi - d = \xi' - d'$ if and only if $(d,d') \in \{(1,0),(0,-1)\}$, so that we have

$$\langle C|M_\delta M_\delta^\dagger|C'\rangle = \sum_{q\in Q,\sigma\in\Sigma,d=0,1} \delta(q,\sigma,p',T(\xi-d),d-1)^*\delta(q,\sigma,p,T(\xi-d),d).$$

Since for any $p,p' \in Q$ and $\tau_0,\tau_1 \in \Sigma$ there are configurations $C = (p,T,\xi)$ and $C' = (p',T,\xi')$ such that $(C,C') \in A(1)$ and $T(\xi-d) = \tau_d$ for all $d \in \{0,1\}$, condition (c) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in A(1)$.

For any $(C,C') \in B(0,1)$ with $C = (p,T,\xi)$ and $C' = (p',T',\xi)$, we have $T^\sigma_{\xi-d} = T'^\sigma_{\xi-d'}$ and $\xi - d = \xi - d'$ if and only if $d = d' = 1$, because $T(\xi-1) \neq T'(\xi-1)$ and $T^\sigma_{\xi-d}(\xi-1) = T'^\sigma_{\xi-d'}(\xi-1)$. Thus we have

$$\langle C|M_\delta M_\delta^\dagger|C'\rangle = \sum_{q\in Q,\sigma\in\Sigma} \delta(q,\sigma,p',T'(\xi-1),1)^*\delta(q,\sigma,p,T(\xi-1),1).$$

Since for any $(p,\tau),(p',\tau') \in Q \times \Sigma$ with $\tau \neq \tau'$ there are configurations $C = (p,T,\xi)$ and $C' = (p',T',\xi')$ such that $(C,C') \in B(0,1), T(\xi-1) = \tau$, and $T'(\xi-1) = \tau'$, the case $d = 1$ of condition (d) holds if and only

if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in B(0,1)$. Similarly we can show the case $d = 0$ or $d = -1$ of condition (d) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in B(0,0)$ or $B(0,-1)$. Thus condition (d) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in B(0)$.

For any $(C,C') \in B(1,1)$ with $C = (p,T,\xi)$ and $C' = (p',T',\xi')$, we have $T^\sigma_{\xi-d} = T'^\sigma_{\xi'-d'}$ and $\xi - d = \xi' - d'$ if and only if $d = 1$ and $d' = 0$, because $T(\xi-1) \neq T'(\xi-1)$ and $T^\sigma_{\xi-d}(\xi-1) = T'^\sigma_{\xi'-d'}(\xi-1)$. Thus we have

$$\langle C|M_\delta M_\delta^\dagger|C'\rangle = \sum_{q\in Q,\sigma\in\Sigma} \delta(q,\sigma,p',T'(\xi-1),0)^*\delta(q,\sigma,p,T(\xi-1),1).$$

Since for any $(p,\tau),(p',\tau') \in Q\times\Sigma$ with $\tau \neq \tau'$ there are configurations $C = (p,T,\xi)$ and $C' = (p',T',\xi')$ such that $(C,C') \in B(1,1), T(\xi-1) = \tau$, and $T'(\xi-1) = \tau'$, the case $d = 1$ of condition (e) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in B(1,1)$. Similarly we can show the case $d = 0$ of condition (e) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in B(1,0)$. Thus condition (e) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in B(1)$.

For any $(C,C') \in A(2)\cup B(2,1)$ with $C = (p,T,\xi)$ and $C' = (p',T',\xi')$, we have $T^\sigma_{\xi-d} = T'^\sigma_{\xi'-d'}$ and $\xi - d = \xi' - d'$ if and only if $d = 1$ and $d' = -1$, so that we have

$$\langle C|M_\delta M_\delta^\dagger|C'\rangle = \sum_{q\in Q,\sigma\in\Sigma} \delta(q,\sigma,p',T'(\xi-1),-1)^*\delta(q,\sigma,p,T(\xi-1),1).$$

Since for any $(p,\tau),(p',\tau') \in Q\times\Sigma$ there are configurations $C = (p,T,\xi)$ and $C' = (p',T',\xi')$ such that $(C,C') \in A(2)\cup B(2,1), T(\xi-1) = \tau$, and $T'(\xi-1) = \tau'$, condition (f) holds if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = 0$ holds for all $(C,C') \in A(2)\cup B(2,1)$.

Since $M_\delta M_\delta^\dagger$ is self-adjoint, $M_\delta M_\delta^\dagger = 1$ if and only if $\langle C|M_\delta M_\delta^\dagger|C'\rangle = \langle C|C'\rangle$ for any $C = (p,T,\xi)$, $C' = (p',T',\xi') \in \mathcal{C}(Q,\Sigma)$ with $\xi' \leq \xi$. Therefore, we have proved that conditions (a–f) hold if and only if $M_\delta M_\delta^\dagger = 1$. Now, Lemma 5.1 concludes the assertion. □

6. Multi-tape quantum Turing machines

In the preceding sections, we have discussed solely single tape quantum Turing machines, but our arguments can be adapted easily to multi-tape quantum Turing machines, which are quantum analogues of multi-tape deterministic Turing machines.

First, we explain how to adapt our arguments to multi-tape quantum Turing machines by considering two-tape quantum Turing machines. A two-tape quantum Turing machine is a quantum system consisting of a processor, two bilateral infinite tapes with heads to read and write symbols on their tapes. In order

to discuss local transition functions, we adapt the formal definitions as follows. Let (Q, Σ_1, Σ_2) be a triple, called a *two-tape Turing frame*, consisting of finite sets Q, Σ_1, and Σ_2 with specific elements $B_1 \in \Sigma_1$ and $B_2 \in \Sigma_2$. The *configuration space* of (Q, Σ_1, Σ_2) is the product set $C(Q, \Sigma_1, \Sigma_2) = Q \times \Sigma_1^{\#} \times \Sigma_2^{\#} \times \mathbb{Z}^2$. Thus, the configuration of a two-tape quantum Turing machine $\mathcal{Q}$ with the frame (Q, Σ_1, Σ_2) is determined by the processor configuration $q \in Q$, the first and second tape configurations $T_1 \in \Sigma_1^{\#}$, $T_2 \in \Sigma_2^{\#}$, and the head positions $\xi_1 \in \mathbb{Z}$, $\xi_2 \in \mathbb{Z}$ in the first and second tapes. The *quantum state space* of (Q, Σ_1, Σ_2) is the Hilbert space $\mathcal{H}(Q, \Sigma_1, \Sigma_2)$ generated by $C(Q, \Sigma_1, \Sigma_2)$. A *local transition function* for (Q, Σ_1, Σ_2) is defined to be a complex-valued function on $Q \times \Sigma \times Q \times \Sigma \times \{-1, 0, 1\}^2$, where $\Sigma = \Sigma_1 \times \Sigma_2$. The relation $\delta(q, (\sigma_1, \sigma_2), p, (\tau_1, \tau_2), (d_1, d_2)) = c$ can be interpreted as the following operation of $\mathcal{Q}$: if the processor is in the configuration q and if the head of the i-th tape $(i = 1, 2)$ reads the symbol σ_i, then it follows with the amplitude c that the processor configuration turns to p, the head of the i-th tape writes the symbol τ_i and moves one cell to the right if $d_i = 1$, to the left if $d_i = -1$, or does not move if $d_i = 0$. The *evolution operator* of δ is a linear operator M_δ on $\mathcal{H}(Q, \Sigma_1, \Sigma_2)$ such that

$$M_\delta |q, (T_1, T_2), (\xi_1, \xi_2)\rangle = \sum \delta(q, (T_1(\xi_1), T_2(\xi_2)), p, (\tau_1, \tau_2), (d_1, d_2)) |p, (T_{1\xi_1}^{\tau_1}, T_{2\xi_2}^{\tau_2}), (\xi_1 + d_1, \xi_2 + d_2)\rangle$$

for all $(q, (T_1, T_2), (\xi_1, \xi_2)) \in C(Q, \Sigma_1, \Sigma_2)$, where the summation is taken over all $(p, (\tau_1, \tau_2), (d_1, d_2)) \in Q \times \Sigma \times \{-1, 0, 1\}^2$. Then, local transition functions of two-tape quantum Turing machines are characterized as follows.

Theorem 6.1. *The evolution operator M_δ of a local transition function δ for the two-tape Turing frame (Q, Σ_1, Σ_2) is unitary if and only if δ satisfies the following conditions.*

(1) *For any $(q, \sigma) \in Q \times \Sigma$,*

$$\sum_{p \in Q, \tau \in \Sigma, d_1, d_2 \in \{-1,0,1\}} |\delta(q, \sigma, p, \tau, (d_1, d_2))|^2 = 1.$$

(2) *For any $(q, \sigma), (q', \sigma') \in Q \times \Sigma$ with $(q, \sigma) \neq (q', \sigma')$,*

$$\sum_{p \in Q, \tau \in \Sigma, d_1, d_2 \in \{-1,0,1\}} \delta(q', \sigma', p, \tau, (d_1, d_2))^* \delta(q, \sigma, p, \tau, (d_1, d_2)) = 0.$$

(3) *For any $(q, \sigma, \tau_2), (q', \sigma', \tau_2') \in Q \times \Sigma \times \Sigma_2$,*

$$\sum_{\substack{p \in Q, \tau_1 \in \Sigma_1 \\ d_1 \in \{-1,0,1\}, d_2 = 0,1}} \delta(q', \sigma', p, (\tau_1, \tau_2'), (d_1, d_2 - 1))^* \delta(q, \sigma, p, (\tau_1, \tau_2), (d_1, d_2)) = 0.$$

(4) *For any* $(q,\sigma,\tau_2),(q',\sigma',\tau_2')\in Q\times\Sigma\times\Sigma_2$,

$$\sum_{p\in Q,\tau_1\in\Sigma_1,d_1\in\{-1,0,1\}}\delta(q',\sigma',p,(\tau_1,\tau_2'),(d_1,-1))^*\delta(q,\sigma,p,(\tau_1,\tau_2'),(d_1,1))=0.$$

(5) *For any* $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_1=0,1}\delta(q',\sigma',p,\tau',(d_1-1,1))^*\delta(q,\sigma,p,\tau,(d_1,-1))=0.$$

(6) *For any* $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_1=0,1,d_2=0,1}\delta(q',\sigma',p,\tau',(d_1-1,d_2))^*\delta(q,\sigma,p,\tau,(d_1,d_2-1))=0.$$

(7) *For any* $(q,\sigma,\tau_1),(q',\sigma',\tau_1')\in Q\times\Sigma\times\Sigma_1$,

$$\sum_{\substack{p\in Q,\tau_1\in\Sigma_1\\ d_1=0,1,d_2\in\{-1,0,1\}}}\delta(q',\sigma',p,(\tau_1',\tau_2),(d_1-1,d_2))^*\delta(q,\sigma,p,(\tau_1,\tau_2),(d_1,d_2))=0.$$

(8) *For any* $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_1=0,1,d_2=0,1}\delta(q',\sigma',p,\tau',(d_1-1,d_2-1))^*\delta(q,\sigma,p,\tau,(d_1,d_2))=0.$$

(9) *For any* $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_1=0,1}\delta(q',\sigma',p,\tau',(d_1-1,-1))^*\delta(q,\sigma,p,\tau,(d_1,1))=0.$$

(10) *For any* $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$,

$$\sum_{p\in Q}\delta(q',\sigma',p,\tau',(-1,1))^*\delta(q,\sigma,p,\tau,(1,-1))=0.$$

(11) *For any* $(q,\sigma,\tau),(q',\sigma',\tau')\in Q\times\Sigma^2$,

$$\sum_{p\in Q,d_2=0,1}\delta(q',\sigma',p,\tau',(-1,d_2))^*\delta(q,\sigma,p,\tau,(1,d_2-1))=0.$$

(12) *For any* $(q,\sigma,\tau_1),(q',\sigma',\tau_1')\in Q\times\Sigma\times\Sigma_1$,

$$\sum_{p\in Q,\tau_2\in\Sigma_2,d_2\in\{-1,0,1\}}\delta(q',\sigma',p,(\tau_1',\tau_2),(-1,d_2))^*\delta(q,\sigma,p,(\tau_1,\tau_2),(1,d_2))=0.$$

(13) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$,

$$\sum_{p\in Q, d_2=0,1} \delta(q',\sigma',p,\tau',(-1,d_2-1))^*\delta(q,\sigma,p,\tau,(1,d_2)) = 0.$$

(14) *For any* $(q,\sigma,\tau),(q',\sigma',\tau') \in Q \times \Sigma^2$,

$$\sum_{p\in Q} \delta(q',\sigma',p,\tau',(-1,-1))^*\delta(q,\sigma,p,\tau,(1,1)) = 0.$$

If each head is required to move either to the right or to the left at each step, conditions (3, 5–9, 11), and (13) are automatically satisfied. It is also easy to see that conditions (3–14) are automatically satisfied by unidirectional two-tape quantum Turing machines, for which (d_1,d_2) is uniquely determined by p in the non-zero amplitude $\delta(q,\sigma,p,\tau,(d_1,d_2))$.

The proof of Theorem 6.1 is analogous to the proof of Theorem 4.5. Let $\mathcal{C}(k_1,k_2)$ be a subset of $\mathcal{C}(Q,\Sigma_1,\Sigma_2)^2$ consisting of all pairs $C = (q,(T_1,T_2),(\xi_1,\xi_2))$ and $C' = (q',(T_1',T_2'),(\xi_1',\xi_2'))$ with $C \neq C'$ such that $T_i(m_i) = T_i'(m_i)$ for $m_i \notin \{\xi_i,\xi_i'\}$ and that $\xi_i' - \xi_i = k_i$ for $i = 1,2$. This plays a role similar to $\mathcal{C}(k)$ in the proof of Theorem 4.5. In the proof of Theorem 4.5, we showed that condition (b, c), or (d) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C,C') \in \mathcal{C}(0)$, $(C,C') \in \mathcal{C}(1)$, or $(C,C') \in \mathcal{C}(2)$, respectively. In the case of Theorem 6.1, we can show similarly that for $(k_1,k_2) \in (\{0\}\times\{0,1,2\}) \cup (\{1,2\}\times\{0,\pm1,\pm2\})$, condition $(5k_1+k_2+2)$ holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C,C') \in \mathcal{C}(k_1,k_2)$. For example, condition (2) holds if and only if $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$ holds for all $(C,C') \in \mathcal{C}(0,0)$. (This is the case of $k_1 = k_2 = 0$.) Moreover, it is trivial that condition (1) holds if and only if $\langle C|M_\delta^\dagger M_\delta|C\rangle = 1$ holds for all $C \in \mathcal{C}(Q,\Sigma_1,\Sigma_2)$, and that if $C \neq C'$ and

$$(C,C') \notin \bigcup_{(k_1,k_2)\in\{0,\pm1,\pm2\}^2} \mathcal{C}(k_1,k_2)$$

then $\langle C'|M_\delta^\dagger M_\delta|C\rangle = 0$. Since $M_\delta^\dagger M_\delta$ is self-adjoint, M_δ is an isometry if and only if we have $\langle C'|M_\delta^\dagger M_\delta|C\rangle = \langle C'|C\rangle$ for any $C = (q,(T_1,T_2),(\xi_1,\xi_2))$, $C' = (q,(T_1',T_2'),(\xi_1',\xi_2')) \in \mathcal{C}(Q,\Sigma_1,\Sigma_2)$ with $\xi_1 < \xi_1'$ or with $\xi_1 = \xi_1'$ and $\xi_2 \leq \xi_2'$. Therefore, we can show that conditions (1–14) hold if and only if M_δ is an isometry. We can also show that M_δ is unitary if it is an isometry by a similar argument with the proof of Lemma 4.4. Thus we can prove Theorem 6.1.

We now consider k-tape quantum Turing machines. In what follows, $\vec{a}$ abbreviates $(a_1,\ldots,a_k)$. For $j \in \{0,\ldots,k-1\}$, let $\vec{a}_{\leq j} = (a_1,\ldots,a_j)$ and $\vec{a}_{>j} = (a_{j+1},\ldots,a_k)$. For any set $S = \{i_1,\ldots,i_m\} \subseteq \{1,\ldots,k\}$, let $\vec{a}[S] = (a_{i_1},\ldots,a_{i_m})$ and $\bar{S} = \{1,\ldots,k\}\backslash S$. Moreover, for any tuple $(a_{i_1},\ldots,a_{i_m})$, the symbol $(a_{i_1},\ldots,a_{i_m})^t$ denotes $(a_{I(1)},\ldots,a_{I(m)})$, where $\{I(1),\ldots,I(m)\} = \{i_1,\ldots,i_m\}$ and $I(1) < \cdots < I(m)$. Extending the arguments for the two-tape quantum Turing machines, the local transition functions of k-tape quantum Turing machines can be characterized as follows:

Theorem 6.2. *The evolution operator M_δ of a local transition function δ for the k-tape Turing frame $(Q, \Sigma_1, \Sigma_2, \ldots, \Sigma_k)$ is unitary if and only if δ satisfies the following conditions.*

(1) *For any $(q, \vec{\sigma}) \in Q \times \Sigma$,*

$$\sum_{p \in Q, \vec{\tau} \in \Sigma, \vec{d} \in \{-1,0,1\}^k} |\delta(q, \vec{\sigma}, p, \vec{\tau}, \vec{d})|^2 = 1.$$

(2) *For any $(q, \vec{\sigma}), (q', \vec{\sigma'}) \in Q \times \Sigma$ with $(q, \vec{\sigma}) \neq (q', \vec{\sigma'})$,*

$$\sum_{p \in Q, \vec{\tau} \in \Sigma, \vec{d} \in \{-1,0,1\}^k} \delta(q', \vec{\sigma'}, p, \vec{\tau}, \vec{d})^* \delta(q, \vec{\sigma}, p, \vec{\tau}, \vec{d}) = 0.$$

(3) *For each $j \in \{1, \ldots, k\}$ and $\vec{D}_{>k-j} = (D_{k-j+1}, \ldots, D_k) \in \{1,2\} \times \{0, \pm 1, \pm 2\}^{j-1}$, the following condition holds. For any $(q, \vec{\sigma}, \vec{\tau}[S(\vec{D}_{>k-j})]), (q', \vec{\sigma'}, \vec{\tau'}[S(\vec{D}_{>k-j})]) \in Q \times \Sigma \times \prod_{i \in S(\vec{D}_{>k-j})} \Sigma_i$ we have*

$$\sum \delta(q', \vec{\sigma'}, p, (\vec{\tau}[\bar{S}(\vec{D}_{>k-j})], \vec{\tau'}[S(\vec{D}_{>k-j})])^t, (\vec{d}_{\leq k-j}, \vec{d'}_{>k-j}))^* \times \delta(q, \vec{\sigma}, p, (\vec{\tau}[\bar{S}(\vec{D}_{>k-j})], \vec{\tau}[S(\vec{D}_{>k-j})])^t, (\vec{d}_{\leq k-j}, \vec{d}_{>k-j})) = 0,$$

where the summation is taken over $p \in Q$, $\vec{\tau}[\bar{S}(\vec{D}_{>k-j})] \in \prod_{i \in \bar{S}(\vec{D}_{>k-j})} \Sigma_i$, $\vec{d}_{\leq k-j} \in \{-1,0,1\}^{k-j}$, and $\vec{d'}_{>k-j}, \vec{d}_{>k-j} \in \{-1,0,1\}^j$ such that $\vec{d}_{>k-j} - \vec{d'}_{>k-j} = \vec{D}_{>k-j}$. Here, $S(\vec{D}_{>k-j}) = \{i \in \{k-j+1, \ldots, k\} | \ D_i \neq 0\}$.

Note that condition (3) of Theorem 6.2 contains $2 \times \sum_{j=0}^{k-1} 5^j$ conditions (the number of different pairs $(j, \vec{D}_{>k-j})$). Thus, the local transition functions of k-tape quantum Turing machines can be characterized by

$$1 + 1 + 2 \times \sum_{j=0}^{k-1} 5^j = 1 + (1/2)(5^k + 1)$$

conditions.

Multi-tape Turing machines are often used for theoretical consideration in complexity theory [9] because it is often easier to construct a multi-tape machine than a single tape machine in order to realize a given algorithm. Hence, multi-tape quantum Turing machines can be expected as useful tools for quantum complexity theory. In such applications, it appears to be a tedious task to check that a constructed local transition function satisfies the unitarity conditions. However, it should be noted that restricted classes of multi-tape machines are characterized much more simply; the unidirectional multi-tape machines are characterized by only two conditions, conditions (1) and (2) in Theorem 6.2.

Appendix A. The bound of M_δ

Theorem A.1. *Let δ be a complex valued function defined on $Q \times \Sigma \times Q \times \Sigma \times \{-1,0,1\}$. Then, there is uniquely a bounded operator M_δ on $\mathcal{H}(Q,\Sigma)$ satisfying equation (4.3). The operator norm of M_δ is bounded by $\sqrt{5}K|Q||\Sigma|^2$, where*

$$K = \max_{(q,\sigma)\in Q\times\Sigma} \left(\sum_{(p,\tau,d)\in Q\times\Sigma\times\{-1,0,1\}} |\delta(q,\sigma,p,\tau,d)|^2 \right)^{\frac{1}{2}}.$$

Proof. For any $C = (q,T,\xi) \in \mathcal{C}(Q,\Sigma)$, let $|F(C)\rangle$ be defined by

$$|F(C)\rangle = \sum_{p,\tau,d} \delta(q,T(\xi),p,\tau,d)|p,T_\xi^\tau,\xi+d\rangle,$$

where (p,τ,d) varies over the finite set $Q \times \Sigma \times \{-1,0,1\}$. Then we have

$$|| \, |F(C)\rangle||^2 = \sum_{p,\tau,d} |\delta(q,T(\xi),p,\tau,d)|^2 \leq K^2.$$

By the Schwarz inequality, we have

$$|\langle F(C')|F(C)\rangle| \leq || \, |F(C')\rangle|| \cdot || \, |F(C)\rangle|| \leq K^2$$

for any $C, C' \in \mathcal{C}(Q,\Sigma)$. For any $(p,\tau) \in Q \times \Sigma$, let $\gamma_0(p,\tau)$ be the mapping on $\mathcal{C}(Q,\Sigma)$ defined by

$$\gamma_0(p,\tau)(q,T,\xi) = (p,T_\xi^\tau,\xi).$$

According to equation (4.1), we have $\gamma_0(p,\tau) = \alpha(p,\tau,0)$. By Proposition 4.1(iii), $\gamma_0(p,\tau)$ is a bijection between $\mathcal{C}(q,\sigma,0)$ and $\mathcal{C}(p,\tau,0)$. Thus, the operator

$$A_0(p,\tau;q,\sigma) = \sum_{C\in\mathcal{C}(q,\sigma,0)} \langle F(\gamma_0(p,\tau)C)|F(C)\rangle|\gamma_0(p,\tau)C\rangle\langle C|$$

is bounded and its operator norm is at most K^2. By Proposition 4.1(i),

$$\sum_{(q,\sigma)\in Q\times\Sigma} A_0(p,\tau;q,\sigma) = \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(\gamma_0(p,\tau)C)|F(C)\rangle|\gamma_0(p,\tau)C\rangle\langle C|,$$

so that the operator

$$A_0(p,\tau) = \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(\gamma_0(p,\tau)C)|F(C)\rangle|\gamma_0(p,\tau)C\rangle\langle C|$$

is bounded and its operator norm is at most $K^2|Q||\Sigma|$. Moreover,

$$A_0 = \sum_{(p,\tau)\in Q\times\Sigma} A_0(p,\tau)$$

is also bounded and $||A_0|| \leq K^2|Q|^2|\Sigma|^2$.

For any $(p,\tau,\tau') \in Q \times \Sigma^2$ and $i = \pm 1, \pm 2$, let $\gamma_i(p,\tau,\tau')$ be the mapping on $\mathcal{C}(Q,\Sigma)$ defined by

$$\gamma_i(p,\tau,\tau')(q,T,\xi) = (p, T^{\tau,\tau'}_{\xi,\xi+i}, \xi + i),$$

where $T^{\tau,\tau'}_{\xi,\xi+i}$ is the tape configuration defined by

$$T^{\tau,\tau'}_{\xi,\xi+i}(m) = \begin{cases} \tau & \text{if } m = \xi, \\ \tau' & \text{if } m = \xi + i, \\ T(m) & \text{if } m \neq \xi, \xi + i. \end{cases}$$

For any $(q,\sigma,\sigma') \in Q \times \Sigma^2$ and $i = \pm 1, \pm 2$, let $\mathcal{C}(q,\sigma,\sigma',i)$ be the set

$$\mathcal{C}(q,\sigma,\sigma',i) = \{(q,T,\xi) \in \mathcal{C}(Q,\Sigma) |\ T(\xi) = \sigma \text{ and } T(\xi + i) = \sigma'\}.$$

It is straightforward to check that $\gamma_i(p,\tau,\tau')$ is a bijection between $\mathcal{C}(q,\sigma,\sigma',i)$ and $\mathcal{C}(p,\tau',\tau,-i)$. Thus, for each $i = \pm 1, \pm 2$, the operator

$$A_i(p,\tau,\tau';q,\sigma,\sigma') = \sum_{C\in\mathcal{C}(q,\sigma,\sigma',i)} \langle F(\gamma_i(p,\tau,\tau')C)|F(C)\rangle |\gamma_i(p,\tau,\tau')C\rangle\langle C|$$

is bounded and $||A_i(p,\tau,\tau';q,\sigma,\sigma')|| \leq K^2$. For any $i \in \{\pm 1, \pm 2\}$, we can verify easily that if $(q,\sigma_1,\sigma_2) \neq (q',\sigma_1',\sigma_2') \in Q \times \Sigma^2$, then $\mathcal{C}(q,\sigma_1,\sigma_2,i) \cap \mathcal{C}(q',\sigma_1',\sigma_2',i) = \emptyset$ and

$$\mathcal{C}(Q,\Sigma) = \bigcup_{(q,\sigma,\sigma')\in Q\times\Sigma^2} \mathcal{C}(q,\sigma,\sigma',i).$$

Thus, we have

$$\sum_{(q,\sigma,\sigma')\in Q\times\Sigma^2} A_i(p,\tau,\tau';q,\sigma,\sigma') = \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(\gamma_i(p,\tau,\tau')C)|F(C)\rangle |\gamma_i(p,\tau,\tau')C\rangle\langle C|,$$

and the operator

$$A_i(p,\tau,\tau') = \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(\gamma_i(p,\tau,\tau')C)|F(C)\rangle |\gamma_i(p,\tau,\tau')C\rangle\langle C|$$

is bounded and its operator norm is at most $K^2|Q||\Sigma|^2$. Moreover,

$$A_i = \sum_{(p,\tau,\tau')\in Q\times\Sigma^2} A_i(p,\tau,\tau')$$

is also bounded and $||A_i|| \leq K^2|Q|^2|\Sigma|^4$.

Now, for $i = 0, \pm 1, \pm 2$, let

$$S(C,i) = \{(q',T',\xi') \in \mathcal{C}(Q,\Sigma)|\ \xi' - \xi = i \text{ and } T(m) = T'(m) \text{ for any } m \notin \{\xi,\xi'\}\},$$

where $C = (q,T,\xi) \in \mathcal{C}(Q,\Sigma)$. Let

$$A = \sum_{i=-2}^{2} \sum_{C'\in S(C,i)} \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(C')|F(C)\rangle |C'\rangle\langle C|.$$

Since for any $C' \in S(C,0)$ there is uniquely a pair $(p,\tau) \in Q\times\Sigma$ such that $C' = \gamma_0(p,\tau)C$ and for any $C' \in S(C,i)$, where $i = \pm 1, \pm 2$, there is uniquely a triple $(p,\tau,\tau') \in Q\times\Sigma^2$ such that $C' = \gamma_i(p,\tau,\tau')C$, we have

$$\begin{aligned} A &= \sum_{(p,\tau)\in Q\times\Sigma} \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(\gamma_0(p,\tau)C)|F(C)\rangle |\gamma_0(p,\tau)C\rangle\langle C| \\ &\quad + \sum_{i\in\{\pm 1,\pm 2\}} \sum_{(p,\tau,\tau')\in Q\times\Sigma^2} \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle F(\gamma_i(p,\tau,\tau')C)|F(C)\rangle |\gamma_i(p,\tau,\tau')C\rangle\langle C| \\ &= A_0 + A_1 + A_{-1} + A_2 + A_{-2} \end{aligned}$$

is bounded and we have

$$||A|| \leq K^2|Q|^2|\Sigma|^2 + 4K^2|Q|^2|\Sigma|^4 \leq 5K^2|Q|^2|\Sigma|^4.$$

Moreover, if $C' \notin \bigcup_{i=0,\pm 1,\pm 2} S(C,i)$, then $\langle F(C')|F(C)\rangle = 0$. Thus,

$$A = \sum_{C',C\in\mathcal{C}(Q,\Sigma)} \langle F(C')|F(C)\rangle |C'\rangle\langle C|.$$

For any $|\psi\rangle \in \mathcal{H}(Q,\Sigma)$, we have

$$\begin{aligned} \left|\left| \sum_{C\in\mathcal{C}(Q,\Sigma)} \langle C|\psi\rangle |F(C)\rangle \right|\right|^2 &= \sum_{C',C\in\mathcal{C}(Q,\Sigma)} \langle\psi|C'\rangle\langle C|\psi\rangle\langle F(C')|F(C)\rangle \\ &= \langle\psi|A|\psi\rangle \\ &\leq 5K^2|Q|^2|\Sigma|^4||\,|\psi\rangle||^2 < \infty. \end{aligned}$$

Now, let M_δ be an operator on $\mathcal{H}(Q,\Sigma)$ which transforms $|\psi\rangle$ to $\sum_{C\in\mathcal{C}(Q,\Sigma)}\langle C|\psi\rangle|F(C)\rangle$. Then, M_δ is a unique bounded operator satisfying equation (4.3) and

$$||M_\delta|| \leq \sqrt{5}K|Q||\Sigma|^2.$$

□

References

[1] P. Benioff, The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *J. Statist. Phys.* **22** (1980) 563-591.

[2] E. Bernstein and U. Vazirani, Quantum complexity theory. *SIAM J. Comput.* **26** (1997) 1411-1473.

[3] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. Roy. Soc. London Ser. A* **400** (1985) 97-117.

[4] D. Deutsch, Quantum computational networks. *Proc. Roy. Soc. London Ser. A* **425** (1989) 73-90.

[5] R.P. Feynman, Simulating physics with computers. *Internat. J. Theoret. Phys.* **21** (1982) 467-488.

[6] J. Gruska, *Quantum Computing.* McGraw–Hill, London (1999).

[7] M. Hirvensalo, *On quantum computation.* Ph.D. Thesis, Turku Center for Computer Science, Finland (1997).

[8] H. Nishimura and M. Ozawa, Computational complexity of uniform quantum circuit families and quantum Turing machines. *Theoret. Comput. Sci.* (to appear). Available at the LANL quantum physics e-print archive at http://xxx.lanl.gov/archive/quant-ph/9906095

[9] C.H. Papadimitriou, *Computational Complexity.* Addison–Wesley, Reading, MA (1994).

[10] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proc. 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser. IEEE Computer Society Press, Los Alamitos, CA (1994) 124-134.

[11] A. Yao, Quantum circuit complexity, in *Proc. 34th Annual Symposium on Foundations of Computer Science.* IEEE Computer Society Press, Los Alamitos, CA (1993) 352-361.

Communicated by J. Gruska.
Received October, 2000. Accepted January, 2001.