一般化量子チューリング機械について 情報科学と函数解析の接点 [これまでとこれから]  

<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>一般化量子チューリング機械について</td>
<td>情報科学と函数解析の接点 [これまでとこれから]</td>
</tr>
<tr>
<td>数理解析研究所講究録</td>
<td>情報科学と函数解析の接点 [これまでとこれから]</td>
</tr>
<tr>
<td>イメージ</td>
<td>画像</td>
</tr>
</tbody>
</table>

Kyoto University

Kyoto University Research Information Repository

http://hdl.handle.net/2433/25968

Departmental Bulletin Paper

Publisher

Kyoto University
Abstract

In this paper, we construct a novel model of a universal quantum Turing machine (QTM) which is free from the specific time for an input data and efficiently simulates each step of a given QTM.

Deutsch [1] formulated a precise model of a quantum computer as quantum Turing machine (QTM) and proposed a model of universal quantum Turing machine which requires exponential time of \( t \) to simulate any other QTM with \( t \) steps. Bernstein and Vazirani[2] showed the existence of an efficient universal QTM by slightly modifying Deutsch's model. In [3] several issues related with QTM and universal QTM are discussed. Nishimura and Ozawa gave another proof of the existence of a universal QTM by using quantum circuit families [4].

In this paper, we construct a novel model of a universal QTM which does not depend on time \( t \) in an input data. Our universal QTM \( \mathcal{M} \) simulates all the steps of a target (stationary normal) QTM \( M \) for any accuracy \( \varepsilon \) with a slowdown \( F \) (as defined later) which is a polynomial function of \( t \) and \( 1/\varepsilon \). That is, \( \mathcal{M} \) gives an outcome with the probability \( p' \) such that \( |p - p'| \leq \varepsilon \) for \( t + F(t, 1/\varepsilon) \), where \( p' \) is the probability to obtain the same outcome by its simulated quantum Turing machine.

We first review the definition of a quantum Turing machine (see e.g., [5]). A Quantum Turing machine (QTM) \( M \) is represented by a quadruplet \( M = (Q, \Sigma, \mathcal{H}, U) \), where \( Q \) is a set of internal states, \( \Sigma \) is a set of finite alphabets with blank symbol, \( \mathcal{H} \) is a Hilbert space described below in (1) and \( U \) is a unitary operator on the space \( \mathcal{H} \) of the form described below in (2). Let \( C = Q \times \Sigma^* \times \mathbb{Z} \) be the set of all classical configurations of a deterministic Turing machine \( M_d \). Since \( \Sigma^* \) represents a set of all the finite sequences of the characters in \( \Sigma \), it becomes a countable set. The Hilbert space \( \mathcal{H} \) is spanned by the complex valued functions on the set of configurations, \( \varphi : C \rightarrow \mathbb{C} \) satisfying
\[
\sum_{C \in C} |\varphi(C)|^2 < \infty.
\]

That is, one has

\[\mathcal{H} = \left\{ \varphi : C \rightarrow \mathbb{C}, \sum_{C \in C} |\varphi(C)|^2 < \infty \right\}. \tag{1}\]

According to the countability of the configuration \(C\), the Hilbert space \(\mathcal{H}\) is naturally isomorphic to the Hilbert space \(l^2\), so that \(\mathcal{H}\) becomes separable. In order to set the unitary operator \(U\) we have to introduce \(\mathcal{H}\) a special basis \(\{e_C\}_{C \in C}\) parametrized by classical configurations \(C \in C\), which is called a computational basis. We define the function \(e_C : C \rightarrow \mathbb{C}\) as

\[e_C(C') = \begin{cases} 
1 & \text{if } C = C', \\
0 & \text{if } C \neq C'.
\end{cases} \quad C, C' \in C\]

It can be easily seen that the set \(\{e_C\}_{C \in C}\) forms a basis of the Hilbert space \(\mathcal{H}\), so each function \(\varphi \in \mathcal{H}\) can be expressed by

\[\varphi(C) = \sum_{D \in \mathcal{C}} \alpha_D e_D(C),\]

where \(\alpha_D\) are proper complex numbers. Hereafter we will use the following so-called Dirac notation

\[e_C = |C\rangle.\]

Since a configuration \(C\) can be written as \(C = (q, A, i)\), one can claim that the set of functions \(\{|q, A, i\rangle\}\) makes a basis in the Hilbert space \(\mathcal{H}\), where \(q \in Q, i \in \mathbb{Z}\) and \(A\) is a finite sequence of elements of \(\Sigma\); \(A \in \Sigma^*\). Let us denote the Hilbert spaces spanned by \(\{|q\rangle\}_{q \in Q}, \{|A\rangle\}_{A \in \Sigma^*}\) and \(\{|i\rangle\}_{i \in \mathbb{Z}}\) by \(\mathcal{H}_1, \mathcal{H}_2\) and \(\mathcal{H}_3\), respectively. On can see that \(\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3\) holds.

As in the classical Turing machine, the dynamics of the quantum Turing machine must be a local one, namely, having a condition imposing on the unitary operator \(U_\delta\). We can state the condition by means of the computational basis as follows: One requires that there is a function \(\delta : Q \times \Sigma \times Q \times \Sigma \times \Gamma \rightarrow \tilde{\mathbb{C}}\) taking its value in the field \(\tilde{\mathbb{C}}\) of computable numbers such that the following relation is satisfied:

\[U_\delta |q, A, i\rangle = \sum_{p, b, \sigma} \delta(q, A(i), p, b, \sigma) |p, A^b_i, i + \sigma\rangle. \tag{2}\]
Here the sum runs over the states \( p \in Q \), the symbols \( b \in \Sigma \) and the elements \( \sigma \in \Gamma = \{1, -1, 0\} \). Since this is a finite sum, the function \( A^{b}_{i} : \mathbb{Z} \to \Sigma \) is defined as

\[
A^{b}_{i}(j) = \begin{cases} 
  b & \text{if } j = i, \\
  A(j) & \text{if } j \neq i.
\end{cases}
\]

The function \( \delta \) is called a quantum transition function, which plays a analogous role as the transition function for the classical Turing machine. A quantum Turing machine is determined by specifying a quantum transition function satisfying the unitarity condition. The restriction to the computable number field \( \mathbb{C} \) instead of all the complex number \( \mathbb{C} \) is needed since otherwise we can not construct or design a quantum Turing machine.

Let \( E_{1}(q), E_{2}(A) \) and \( E_{3}(i) \) be projections on the Hilbert space \( \mathcal{H} \), defined as

\[
E_{1}(q) = \langle q | I_{2} \otimes I_{3}, \quad E_{2}(A) = I_{1} \otimes | A \rangle \langle A | I_{3}, \quad E_{3}(i) = I_{1} \otimes I_{2} \otimes | q \rangle \langle q | \quad (3)
\]

where \( I_{1}, I_{2} \) and \( I_{3} \) are the identity operator on \( \mathcal{H}_{1}, \mathcal{H}_{2} \) and \( \mathcal{H}_{3} \), respectively. A QTM \( M = (Q, \Sigma, \delta) \) with a unitary operator \( U_{\delta} \) is said to be stationary, if for every initial configurations \( c_{0} \), there exists some positive integer \( t \) (which can be infinite) such that \( \| E_{3}(0) E_{1}(q) U_{\delta}^{s} | c_{0} \rangle \|^{2} = 1 \) and it holds \( \| E_{1}(q_{f}) U_{\delta}^{s} | c_{0} \rangle \|^{2} = 0 \) for all \( s < t \). A QTM \( M = (Q, \Sigma, \delta) \) is said to be in normal form if \( \delta(q_{f}, \sigma, q_{0}, \sigma, 1) = 1 \) for any \( \sigma \in \Sigma \). We call a stationary and normal form QTM a SNQTM.

Here, we state some results, proved in [2].

**Lemma 1 (Dovetailing Lemma)** If \( M_{1} \) and \( M_{2} \) are SNQTMs with the same alphabet, then there exists a SNQTM \( M \) which carries out the computation of \( M_{1} \) followed by the computation of \( M_{2} \).

**Lemma 2 (Branching Lemma)** If \( M_{1} \) and \( M_{2} \) are SNQTMs with the same alphabet, then there exists a multi-track SNQTM \( M \) such that \( M \) carries out the computation of \( M_{1} \) on its first track if the second track is empty, and it leaves the second track empty. If the second track has a special mark 1 in the start cell, \( M \) carries out the computation of \( M_{2} \) on its first track and leaves the special mark.

**Theorem 3 (Synchronization Theorem)** Let \( g \) be a map from strings to strings can be computed in deterministic polynomial time, and such that the length of \( g(x) \) depends only on the length of \( x \). There exists a polynomial time SNQTM which, for a given input \( x \), produces output \( g(x) \), and whose running time depends only on the length of \( x \).
Suppose that $M = (Q, \Sigma, \delta)$ and $M' = (Q', \Sigma', \delta')$ are quantum Turing machines with the unitary operators $U_\delta$ and $U_{\delta'}$, respectively. Let $t$ be a positive integer and $\varepsilon > 0$, we say that a QTM $M'$ with its input $c_0$ simulates $M$ and its input $c_0$ for $t$ steps with accuracy $\varepsilon$ and slowdown $f$ which is a polynomial function of $t$ and $1/\varepsilon$, if the following conditions are satisfied: For all $q \in Q, T \in \Sigma^*, i \in \mathbb{Z}$,

$$\left| \langle q, T, i | U^t_\delta | c_0 \rangle \right|^2 - \left| \langle q, T, i | U^{t+f(t,\frac{1}{\varepsilon})}_{\delta'} | c'_0 \rangle \right|^2 < \varepsilon. \quad (4)$$

Bernstein and Vazirani proved that there exists a normal form QTM $M_{BV}$ simulating any SNQTM $M$ with any accuracy $\varepsilon$ for $t$ steps with slowdown $f(t, \frac{1}{\varepsilon})$ which can be computed in polynomial steps of $t$ and $\varepsilon$. This QTM $M_{BV}$ is known as one of the models of universal QTM. The input data of $M_{BV}$ is a quadruplet $(x, \varepsilon, t, c(M))$ where $x$ is an input of $M$, $\varepsilon$ is accuracy of the simulation, $t$ is a simulation time and $c(M)$ is a code of $M$. Note that it is necessary there to give a time $t$ as an input of $M_{BV}$.

Now, we consider another model of universal QTM whose input data is $(x, \varepsilon, c(M))$, that is, we do not need a simulated time $t$ as an input. It suggests that we do not need to know when the given QTM halts. We prove the following theorem.

**Theorem 4** For any SNQTM $M$, there exists a SNQTM $\mathcal{M}$ which simulates each step of $M$ for an input data $(x, \varepsilon, c(M))$ where $x$ is an input of $M$, $\varepsilon$ is accuracy of the simulation and $c(M)$ is a code of $M$.

**Proof.** By dovetailing $M_{BV}$, $\mathcal{M} = (Q, \Sigma, \delta)$ is constructed to have six two-way tracks which moves as follows: The first track of $\mathcal{M}$ is used to represent the result of computation of $M$. The second track contains a counter of $t$ for $M_{BV}$. The third track is used to record the input of $M$. The fourth and fifth tracks are used to record $\varepsilon$ and $c(M)$, respectively. The sixth track is used as a working track. Precisely, for $(x, \varepsilon, c(M))$ as an input data, $\mathcal{M}$ carries out the following algorithm:

i) $\mathcal{M}$ transfers $x, \varepsilon$ and $c(M)$ to the fixed tracks.
ii) $\mathcal{M}$ sets the counter $t = 1$ and store the value of $t$ on the second track.
iii) $\mathcal{M}$ calculates $\frac{6\varepsilon}{\pi^2 t^2}$ and transfers it to the fourth track.
iv) $\mathcal{M}$ carries out $M_{BV}$ with $(x, 6\varepsilon/\pi^2 t^2, t, c(M))$, and write down the result of $M_{BV}$ on the first track. The calculation of $\mathcal{M}$ is carried out on the sixth track and $\mathcal{M}$ empties the work space finally.
vi) If the simulated result of $M$ is the final state, then $\mathcal{M}$ halts, otherwise $\mathcal{M}$ increases the counter by one and repeats iii) and iv).

Using the Synchronization theorem, we can construct SNQTM$\mathcal{Ms}$ which execute steps i), ii) and iii), respectively, and by dovetailing them, QTM $\mathcal{M}$ is obtained. We denote the time required to compute the steps from i) to vi) by $f'\left(t, \frac{\pi^2 t^2}{6\varepsilon}\right)$, which is polynomial of both variables. Let $c_M$ and $c_\mathcal{M}$ be the initial configurations of $M$ and $\mathcal{M}$, respectively, we denote $c_M = |q_0\rangle \otimes |x\rangle \otimes |0\rangle$.
and $c_M = |q_0 \rangle \otimes |\#, \#, x, \epsilon, c(M), \#\rangle \otimes |0\rangle$. Since $\mathcal{M}_{BV}$ simulates $M$ for any $\epsilon, x$ and $t$, putting $F(t, \epsilon) = \sum_{i=1}^{t} f'(i, \pi^2 i^2 / 6 \epsilon)$, the simulation of $t$ steps of $M$ requires $t + F(t, 1 / \epsilon)$ steps. For any $q, i$ and $T$, the following inequality is obtained

$$\left| \langle q, T, i | U_\delta^{t} | c_M \rangle \right|^2 - \left| \langle q, T, i | U_{\delta'}^{t+F(t, \epsilon)} | c_M \rangle \right|^2 < \frac{6\epsilon}{\pi^2 t^2}, \quad (5)$$

where $U_\delta$ and $U_{\delta'}$ are the unitary operator corresponding to $M$ and $\mathcal{M}$ respectively. $\blacksquare$

Suppose that $M$ halts at time $t$ and gives an outcome with probability $p$, $\mathcal{M}$ gives the same outcome with probability $p'$ satisfying $|p-p'| \leq \epsilon$ by $t+F(t, 1/\epsilon)$. In fact,

$$|p' - p| \leq \sum_{i=1}^{\infty} \frac{6\epsilon}{\pi^2 i^2} \leq \epsilon \quad (6)$$

holds.

References


