数理解析研究所講究録 1396 巻 2004 年 67-71

一般化量子チューリング機械について

入山 聖史, 大矢 雅則
東京理科大学理工学部 情報科学科
千葉県野田市山崎 2641

Satoshi Iriyama and Masanori Ohya
Depertment of Information Sciences
Tokyo University of Science
Noda City, Chiba 278-8510, Japan

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 ε 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, Σ 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 $\mathcal{C} = Q \times \Sigma^* \times \mathbb{Z}$ be the set of all classical configurations of a deterministic Turing machine M_d. Since Σ^* represents a set of all the finite sequences of the characters in Σ, it becomes a countable set. The Hilbert space $\mathcal{H}$ is spanned by the complex valued functions on the set of configurations, $\varphi : \mathcal{C} \to \mathbb{C}$ satisfying

$$\sum_{C\in\mathcal{C}} |\varphi(C)|^2 < \infty.$$

That is, one has

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

According to the countability of the configuration $\mathcal{C}$, 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 $\{e_C\}_{C\in\mathcal{C}}$ parametrized by classical configurations $C \in \mathcal{C}$, which is called a *computational basis*. We define the function $e_C : \mathcal{C} \to \mathbb{C}$ as

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

It can be easily seen that the set $\{e_C\}_{C\in\mathcal{C}}$ 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 α_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 $\{| q, A, i >\}$ 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 Σ; $A \in \Sigma^*$. Let us denote the Hilbert spaces spanned by $\{|q\rangle\}_{q\in Q}$, $\{|A\rangle\}_{A\in\Sigma^*}$ and $\{|i\rangle\}_{i\in\mathbf{Z}}$ 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_δ. We can state the condition by means of the computational basis as follows: One requires that there is a function $\delta : Q \times \Sigma \times Q \times \Sigma \times \Gamma \to \tilde{\mathbb{C}}$ taking its value in the field $\tilde{\mathbb{C}}$ of computable numbers such that the following relation is satisfied:

$$U_\delta |q, A, i\rangle = \sum_{p,b,\sigma} \delta(q, A(i), p, b, \sigma) \left|p, A_i^b, i + \sigma\right\rangle . \tag{2}$$

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 $A_i^b : \mathbb{Z} \to \Sigma$ is defined as

$$A_i^b(j) = \begin{cases} b \text{ if } j = i, \\ A(j) \text{ if } j \neq i. \end{cases}$$

The function δ 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 $\tilde{\mathbb{C}}$ 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

$$\begin{aligned} E_1(q) &= |q\rangle\langle q| \otimes I_2 \otimes I_3 \\ E_2(A) &= I_1 \otimes |A\rangle\langle A| \otimes I_3 \\ E_3(i) &= I_1 \otimes I_2 \otimes |q\rangle\langle q| \end{aligned} \tag{3}$$

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_δ is said to be *stationary*, if for every initial configurations c_0, there exists some positive integer t (which can be infinite) such that $\| E_3(0) E_1(q) U_\delta^t |c_0\rangle \|^2 = 1$ 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_δ 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 ε and slowdown f which is a polynomial function of t and $1/\varepsilon$, if the following conditions are satisfied: For all $q \in Q, T \in \Sigma^*, i \in \mathbb{Z}$,

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

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

Proof. By dovetailing $\mathcal{M}_{BV}$, $\mathcal{M} = (Q, \Sigma, \delta)$ 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 $\mathcal{M}_{BV}$. The third track is used to record the input of M. The fourth and fifth tracks are used to record ε 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, ε 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 $\mathcal{M}_{BV}$ with $\left(x, 6\varepsilon/\pi^2 t^2, t, c(M)\right)$, and write down the result of $\mathcal{M}_{BV}$ 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 SNQTMs 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 $c_{\mathcal{M}} = |q_0\rangle \otimes |\#, \#, x, \varepsilon, c(M), \#\rangle \otimes |0\rangle$. Since $\mathcal{M}_{BV}$ simulates M for any ε, x and t, putting $F\left(t, \frac{1}{\varepsilon}\right) = \sum_{i=i}^{t} f'\left(i, \frac{\pi^2 i^2}{6\varepsilon}\right)$, the simulation of t steps of M requires $t + F\left(t, \frac{1}{\varepsilon}\right)$ steps. For any q, i and T, the following inequality is obtained

$$\left| |\langle q, T, i| U_\delta^t |c_M\rangle|^2 - \left|\langle q, T, i| U_{\delta'}^{t+F\left(t, \frac{1}{\varepsilon}\right)} |c_{\mathcal{M}}\rangle\right|^2 \right| < \frac{6\varepsilon}{\pi^2 t^2}, \tag{5}$$

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

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

$$|p' - p| \leq \sum_{i=1}^{\infty} \frac{6\varepsilon}{\pi^2 i^2} \leq \varepsilon \tag{6}$$

holds.

References

[1] D. Deutsch: Proc.Roy.Soc.London A, **400** (1985). 97-117

[2] E. Bernstein and U. Vazirani.: Quantum complexity theory, in: Proc.of the 25th Annual ACM Symposium on Theory of Computing, ACM, New York, pp.11-22.(1993), SIAM Journal on Computing **26**, 1411 (1997)

[3] Y. Shi: Remarks on universal quantum computer, Phys. Lett. A **293** 277 (2002)

[4] H. Nishimura and M. Ozawa: Computational Complexity of Uniform Quantum Circuit Families and Quantum Turing Machines, Theor.Comput.Sci. 276 147-181 (2002)

[5] M.Ohya and I.V.Volovich: Quantum information, computation, cryptography and teleportation, Springer (to appear).