数理解析研究所講究録
950 巻 1996 年 33-38

On the Computational Power of Quantum Turing Machine

Takashi Mihara
三原 孝志

School of Information Science
Japan Advanced Institute of Science and Technology, Hokuriku
15 Asahidai, Tatsunokuchi, Ishikawa 923-12, Japan

1 Introduction

A computation is an evolution from one physical state to another, and so are Today's computers, i.e., the computations of them are changes of electric signals. What are differences of quantum computers from classical computers? The computational principles of classical computers are based on classical physics. In principle, we can construct them from devices based on classical physics without loss of computational resources, where a computational time, for instance, is estimated under a defined unit time (the real movement of one device may be much later than that of another).

On the other hand, the computational principles of quantum computers are based on quantum physics. We do not know whether quantum physics is different from classical physics, however, it is widely believed that they are different. Under this assumption, R. P. Feynman pointed out that the quantum computers are more powerful than the classical computers[6]. Furthermore, there are some results indicating that the quantum computers seem to be more powerful than the classical computers (e.g., [5, 8]).

In this paper, we consider decision problems: let $\mathcal{L}$ be a set, and $P(x)$ a program for an input x. $P(x)$ returns "YES" if $x \in \mathcal{L}$(an accepted state), otherwise $P(x)$ returns "NO"(an unaccepted state). On the quantum computers, when the probabilities recognizing accepted states are given, we estimate the probabilities recognizing unaccepted states.

2 Preliminaries

In quantum physics, a physical state is represented as a vector in a Hilbert space. We use $|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle, |\varphi\rangle, |\varphi_1\rangle$, and $|\varphi_2\rangle$ for vectors in a Hilbert space, $a_1, a_2, \ldots$, and $b_1, b_2, \ldots$, for complex numbers (a^* is the complex conjugate of a), and $\langle\psi_2|\psi_1\rangle$ for the inner product of $|\psi_1\rangle$ and $|\psi_2\rangle$. Then the following conditions are satisfied:

1. $\langle\psi_2|\psi_1\rangle = \langle\psi_1|\psi_2\rangle^*$,

2. $\langle\psi_3|(a_1|\psi_1\rangle + a_2|\psi_2\rangle) = a_1\langle\psi_3|\psi_1\rangle + a_2\langle\psi_3|\psi_2\rangle$,

3. $0 \leq \langle\psi|\psi\rangle < \infty$, and $\langle\psi|\psi\rangle = 0$ implies $|\psi\rangle = 0$.

For a complete overview on Hilbert spaces, for instance, we refer the reader to [3, 9].

Furthermore, Let $|e_i\rangle$ for $i = 1, 2, \ldots, n$ be an orthonormal basis in an n-dimensional Hilbert space $\mathcal{H}^n$, i.e., $\langle e_i|e_j\rangle = \delta_{ij}$, where $\delta_{ii} = 1$ and $\delta_{ij} = 0$ if $i \neq j$. Any vector $|\psi\rangle$ is represented as $|\psi\rangle = \sum_{i=1}^{n} a_i|e_i\rangle$, and the conjugate vector $\langle\psi|$ as $\langle\psi| = \sum_{i=1}^{n} a_i^*\langle e_i|$. The inner product of $|\psi_1\rangle = \sum_{i=1}^{n} a_i|e_i\rangle$ and $|\psi_2\rangle = \sum_{i=1}^{n} b_i|e_i\rangle$ is

$$\langle\psi_2|\psi_1\rangle = \sum_{i=1}^{n} b_i^* a_i.$$

For instance, let $|e_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|e_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ be a basis in $\mathcal{H}^2$, and $|\psi_1\rangle = |e_1\rangle + i|e_2\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}$ and $|\psi_2\rangle = i|e_1\rangle + 3|e_2\rangle = \begin{pmatrix} i \\ 3 \end{pmatrix}$, then $\langle\psi_2|\psi_1\rangle = (-i, 3)\begin{pmatrix} 1 \\ i \end{pmatrix} = 2i$.

Next, let us define computations on the quantum computers. For the formal definition of a quantum Turing machine(QTM, for short), we refer the reader to [2, 7]. As mentioned above, a computation is an evolution from one physical state to another. The evolution of a physical state is executed in applying a unitary matrix U (i,e,. $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ is the transposed conjugate of U, and I is the unit matrix) to a vector in a Hilbert space. Let $|\psi_{in}\rangle$ be the initial state, and $|\psi_{out}\rangle$ an output state after T time, then

$$|\psi_{out}\rangle = U^T|\psi_{in}\rangle.$$

When a state is a superposition $|\psi\rangle = a_1|\psi_1\rangle + a_2|\psi_2\rangle$,

$$U|\psi\rangle = U(a_1|\psi_1\rangle + a_2|\psi_2\rangle) = a_1U|\psi_1\rangle + a_2U|\psi_2\rangle.$$

Then the results are obtained in *measuring(or observing)* the output state as follows: we can obtain the $|\psi\rangle$ element with probability $|\langle\psi|\psi_{out}\rangle|^2$.

Furthermore, let us represent the QTM as a physical state(i.e., as a vector). Let $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ be a basis in one-bit space. For n-bit($n \geq 2$) space, any vector $|x_1, x_2, \ldots, x_n\rangle$ for $x_i \in \{0, 1\}$ is represented as the tensor products of one-bit states as follows:

$$|x_1, x_2, \ldots, x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_1\rangle.$$

Let $|e_1\rangle, \cdots, |e_m\rangle$ be a basis in $\mathcal{H}^m$, and $|f_1\rangle, \cdots, |f_n\rangle$ a basis in $\mathcal{H}^n$. Then the tensor product $\mathcal{H}^m \otimes \mathcal{H}^n$ of $\mathcal{H}^m$ and $\mathcal{H}^n$ is defined as mn-dimensional space such that $|e_i\rangle \otimes |f_j\rangle$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$ are the basis. For instance, let $|\psi\rangle$ be any vector in $\mathcal{H}^m$, and $|\varphi\rangle$ be any vector in $\mathcal{H}^n$, i.e., $|\psi\rangle = \sum_{i=1}^m a_i|e_i\rangle$ and $|\varphi\rangle = \sum_{j=1}^n b_j|f_j\rangle$. Then

$$|\psi\rangle \otimes |\varphi\rangle = \sum_{i=1}^m \sum_{j=1}^n a_ib_j|e_i\rangle \otimes |f_j\rangle.$$

The inner product of two vectors, $|\psi_1\rangle \otimes |\varphi_1\rangle$ and $|\psi_2\rangle \otimes |\varphi_2\rangle$, in $\mathcal{H}^m \otimes \mathcal{H}^n$ is

$$((\langle\psi_2| \otimes \langle\varphi_2|)(|\psi_1\rangle \otimes |\varphi_1\rangle) = \langle\psi_2|\psi_1\rangle\langle\varphi_2|\varphi_1\rangle.$$

Let S_m be an operator in $\mathcal{H}^m$, and S_n an operator in $\mathcal{H}^n$.

$$(S_m \otimes S_n)(|\psi_1\rangle \otimes |\psi_2\rangle) = (S_m|\psi_1\rangle) \otimes (S_n|\psi_2\rangle),$$
$$(S_m \otimes S_n)(a_1|\psi_1\rangle + a_2|\psi_2\rangle) = a_1(S_m \otimes S_n)|\psi_1\rangle + a_2(S_m \otimes S_n)|\psi_2\rangle.$$

Finally, let $|C\rangle$ be a finite control, $|T\rangle$ a tape, and $|H\rangle$ a tape head. Each of these is also constructed as a composed system of one-bit physical systems (e.g., $|C\rangle = |c'_1\rangle \otimes |c'_2\rangle \otimes \ldots \otimes |c'_u\rangle$, where $c'_i \in \{0, 1\}$ for $i = 1, 2, \ldots, u$). Then a physical state $|M\rangle$ corresponding to the QTM is represented as a composed system of them as follows:

$$|M\rangle = |C\rangle \otimes |H\rangle \otimes |T\rangle.$$

In general, a state of the QTM corresponds to a superposition of configurations of the QTM. Namely, when $|C\rangle = \sum_{i=1}^l |c_i\rangle$, $|H\rangle = \sum_{j=1}^m |h_j\rangle$, and $|T\rangle = \sum_{k=1}^n |t_k\rangle$, then

$$|M\rangle = \sum_{i=1}^l \sum_{j=1}^m \sum_{k=1}^n |c_i\rangle \otimes |h_j\rangle \otimes |t_k\rangle.$$

If a state of the QTM is not a superposed one, the state of the QTM is equal to a configuration of the QTM. Moreover, the QTM can execute all operations of ordinary reversible Turing machines [1], and unitary transformations for one-bit space[4].

$$V_0 = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \; V_1 = \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix}, \; V_2 = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & 1 \end{pmatrix}, \; V_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix},$$

$$V_4 = V_0^{-1}, \;\; V_5 = V_1^{-1}, \;\; V_6 = V_2^{-1}, \;\; V_7 = V_3^{-1},$$

where α is any irrational multiple of π.

3 Results

The significant methods to solve problems efficiently on the QTM are quantum parallel computations, interferences, and measurements. Interferences and measurements are used in combination with quantum parallel computations. The QTM can make a superposition of some states. For instance, let a function $f : \mathbf{Z}_2^2 \to \mathbf{Z}_2$, where $\mathbf{Z}_2 = \{0,1\}$. The computation of f is executed as follows:

$$\begin{aligned} |0,0,0\rangle &\xrightarrow{V_4} \frac{1}{2^{1/2}}(|0,0,0\rangle + |1,0,0\rangle) \\ &\xrightarrow{V_4} \frac{1}{2}(|0,0,0\rangle + |0,1,0\rangle + |1,0,0\rangle + |1,1,0\rangle) \\ &\xrightarrow{U_f} \frac{1}{2}(|0,0,f(0,0)\rangle + |0,1,f(0,1)\rangle + |1,0,f(1,0)\rangle + |1,1,f(1,1)\rangle). \end{aligned}$$

The QTM can compute all the values of f in parallel, so we call these computations *quantum parallel computations.*

Next, *interferences* are used efficiently in the following way. Let $|\psi\rangle = \sum_{i=1}^n a_i|e_i\rangle$ be a state, where $|e_i\rangle$ for $i = 1,\ldots,n$ are a basis. Now, let $|e_i\rangle$ be executed as $|e_i\rangle \to \sum_{j=1}^n b_{ij}|e_j\rangle$. Then

$$|\psi\rangle \to \sum_{j=1}^{n}(\sum_{i=1}^{n} a_i b_{ij})|e_j\rangle \equiv |\psi'\rangle.$$

For instance, when $\sum_{i=1}^n a_i b_{ij} = \delta_{jk}$ for some k, then $|\psi'\rangle = |e_k\rangle$. This implies that we can obtain $|e_k\rangle$ element with certainty. P. W. Shor used efficiently this method to solve discrete logarithms and factor integers. Namely, he used the following property:

$$\sum_{j=0}^{M-1} e^{2\pi ijK/M} = \begin{cases} M & \text{(if } K \text{ is a multiple of } M\text{)}, \\ 0 & \text{(otherwise)}. \end{cases}$$

Measurements are used efficiently as follows. Let $|e_i'\rangle$ for $i = 1,\ldots,n$ be another basis, and $|e_i\rangle = \sum_{j=1}^n c_{ij}|e_j'\rangle$(for orthonormal bases, $\sum_{i=1}^n c_{ik}^* c_{il} = \delta_{kl}$ and $\sum_{i=1}^n c_{ki}^* c_{li} = \delta_{kl}$). Then

$$|\psi\rangle = \sum_{j=1}^{n}(\sum_{i=1}^{n} a_i c_{ij})|e_j'\rangle.$$

If we can take the good another basis, we will obtain efficiently the results. Note that in this case, since the state does not change, the computational time also does not increase (the measurement time may change).

In this section, we investigate the power of measurements. Here, we consider decision problems. A decision problem is as follows: let $\mathcal{L}$ be a set, and $P(x)$ a program for an input x. The result of $P(x)$ returns "YES" if $x \in \mathcal{L}$(an accepted state), otherwise it returns "NO"(an unaccepted state). On the QTM, the computational state for executing $P(x)$ is represented as a physical state $|\varphi\rangle$, and the result of it is obtained from the measurement of $|\varphi\rangle$ using another vector $|\psi\rangle$ with probability $|\langle\psi|\varphi\rangle|^2$. In the following, we use that the states are

$$\begin{cases} |\varphi_y\rangle, |\varphi_{y_1}\rangle, |\varphi_{y_2}\rangle, \dots & (\text{if } x \in \mathcal{L}), \\ |\varphi_n\rangle, |\varphi_{n_1}\rangle, |\varphi_{n_2}\rangle, \dots & (\text{otherwise}). \end{cases}$$

First, we show that we can decompose any unit vector into a unit vector and the orthonormal vector. In the following, let the dimension of the Hilbert space be $n \geq 3$.

Lemma 3.1 *Any n-dimensional unit vector $|\psi\rangle$ can be decomposed into a unit vector $|\varphi\rangle$ and the orthonormal vector $|\varphi_\perp\rangle$ (i.e., $\langle\varphi_\perp|\varphi\rangle = 0$).*

$$|\psi\rangle = \alpha|\varphi\rangle + \beta|\varphi_\perp\rangle,$$

where α and β are complex numbers, and these vectors are normalized, i.e., $\langle\psi|\psi\rangle = 1$, $\langle\varphi|\varphi\rangle = 1$ and $\langle\varphi_\perp|\varphi_\perp\rangle = 1$.

proof: Let $|e_i\rangle$ for $i = 1, 2, \dots, n$ be an orthonormal basis, $|\psi\rangle = \sum_{i=1}^n a_i|e_i\rangle$, and $|\varphi\rangle = \sum_{i=1}^n b_i|e_i\rangle$, where a_i and b_i for $i = 1, 2, \dots, n$ are complex numbers. Then $|\psi\rangle = \alpha|\varphi\rangle + \sum_{i=1}^n (a_i - \alpha b_i)|e_i\rangle$. Since $\langle\varphi|(\sum_{i=1}^n (a_i - \alpha b_i)|e_i\rangle) = \sum_{i=1}^n (b_i^* a_i - \alpha|b_i|^2) = 0$ and $\langle\psi|\psi\rangle = 1$, then $\alpha = \sum_{i=1}^n b_i^* a_i = \langle\varphi|\psi\rangle$ and $|\beta|^2 = 1 - |\alpha|^2$. □

Next, we show that the probability between two states is conservative if the two computational times are equal.

Lemma 3.2 *Let $|\varphi_1\rangle$ and $|\varphi_2\rangle$ be states. Moreover, let $|\varphi_{1_{in}}\rangle$ and $|\varphi_{2_{in}}\rangle$ be the initial states corresponding to the states above, respectively. If the two computational times are equal, i.e., for the unitary matrix U and the computational time T, $|\varphi_1\rangle = U^T|\varphi_{1_{in}}\rangle$ and $|\varphi_2\rangle = U^T|\varphi_{2_{in}}\rangle$, then $\langle\varphi_2|\varphi_1\rangle = \langle\varphi_{2_{in}}|\varphi_{1_{in}}\rangle$.*

proof: Since $U^\dagger U = I$, $\langle\varphi_2|\varphi_1\rangle = (\langle\varphi_{2_{in}}|(U^\dagger)^T)(U^T|\varphi_{1_{in}}\rangle) = \langle\varphi_{2_{in}}|\varphi_{1_{in}}\rangle$. □

Let T_y be the computational time of an accepted state, T_n be that of an unaccepted state, and $T \geq T_y, T_n$. This lemma implies that if we may measure to obtain the results on the QTM after T time, we can estimate the probability between the accepted state and the unaccepted state before the execution.

Now, let us consider estimating the probabilities of unaccepted states. First, we consider a simplified case such that there exist only one accepted state $|\varphi_y\rangle$ and one unaccepted state $|\varphi_n\rangle$.

Lemma 3.3 *Let $|\varphi_y\rangle$ and $|\varphi_n\rangle$ be the accepted state and the unaccepted state, respectively, and we measure the states using an state $|\psi\rangle$. Moreover, let $|\langle\psi|\varphi_y\rangle|^2 = p_y$, $|\langle\psi|\varphi_n\rangle|^2 = p_n$, and $|\langle\varphi_n|\varphi_y\rangle|^2 = p_{ny}$, where $0 \leq p_y, p_{ny} \leq 1$. Then*

$$\begin{cases} p_n = p_y p_{ny} & (\text{if } p_y = 1 \text{ or } p_{ny} = 1), \\ 0 \leq p_n \leq (\sqrt{p_y p_{ny}} + \sqrt{(1-p_y)(1-p_{ny})})^2 & (\text{if } p_y + p_{ny} \leq 1), \\ (\sqrt{p_y p_{ny}} - \sqrt{(1-p_y)(1-p_{ny})})^2 \leq p_n \leq (\sqrt{p_y p_{ny}} + \sqrt{(1-p_y)(1-p_{ny})})^2 & \\ & (\text{otherwise}). \end{cases}$$

proof: By Lemma 3.1,

$$|\psi\rangle = \sqrt{p_y}e^{i\theta_1}|\varphi_y\rangle + \sqrt{1-p_y}e^{i\theta_2}|\varphi_{y\perp}\rangle,$$
$$|\varphi_n\rangle = \sqrt{p_{ny}}e^{i\theta_3}|\varphi_y\rangle + \sqrt{1-p_{ny}}e^{i\theta_4}|\varphi'_{y\perp}\rangle, \text{ and}$$
$$\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle = |\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle|e^{i\theta'},$$

where $\theta_1, \theta_2, \theta_3, \theta_4$ and θ' are some real numbers determined by the given states, and $\langle\varphi_y|\varphi_{y\perp}\rangle = 0$ and $\langle\varphi_y|\varphi'_{y\perp}\rangle = 0$. Since

$$\langle\psi|\varphi_n\rangle = \sqrt{p_y p_{ny}}e^{i(\theta_3-\theta_1)} + \sqrt{(1-p_y)(1-p_{ny})}|\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle|e^{i(\theta_4-\theta_2+\theta')},$$

then

$$p_n = |\langle\psi|\varphi_n\rangle|^2 = |\sqrt{p_y p_{ny}} + \sqrt{(1-p_y)(1-p_{ny})}|\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle|e^{i\theta}|^2,$$

where $\theta = \theta_1 - \theta_2 - \theta_3 + \theta_4 + \theta'$.

If $p_y = 1$ or $p_{ny} = 1$, $p_n = p_y p_{ny}$. So, in the following, let $p_y \neq 1$ and $p_{ny} \neq 1$. The value of p_n is maximum if $e^{i\theta} = 1$ and $|\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle| = 1$. Next, we estimate the minimum of p_n. To satisfy $\sqrt{p_y p_{ny}} + \sqrt{(1-p_y)(1-p_{ny})}|\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle|e^{i\theta} = 0$, we have $e^{i\theta} = -1$ and $|\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle| = \sqrt{\frac{p_y p_{ny}}{(1-p_y)(1-p_{ny})}}$. Then, since $|\langle\varphi_{y\perp}|\varphi'_{y\perp}\rangle| \le 1, p_y + p_{ny} \le 1$. Therefore, if $p_y + p_{ny} \le 1$, the minimum of p_n is zero, otherwise it is $(\sqrt{p_y p_{ny}} - \sqrt{(1-p_y)(1-p_{ny})})^2$. Then

$$\begin{cases} p_n = p_y p_{ny} & (\text{if } p_y = 1 \text{ or } p_{ny} = 1), \\ 0 \le p_n \le (\sqrt{p_y p_{ny}} + \sqrt{(1-p_y)(1-p_{ny})})^2 & (\text{if } p_y + p_{ny} \le 1), \\ (\sqrt{p_y p_{ny}} - \sqrt{(1-p_y)(1-p_{ny})})^2 \le p_n \le (\sqrt{p_y p_{ny}} + \sqrt{(1-p_y)(1-p_{ny})})^2 & \\ & (\text{otherwise}). \end{cases}$$

□

Using this lemma, we obtain the following theorem.

Theorem 3.1 *Let $|\varphi_y\rangle$ and $|\varphi_n\rangle$ be the accepted state and the unaccepted state, respectively, and we measure the states using an state $|\psi\rangle$. Moreover, let $|\langle\psi|\varphi_y\rangle|^2 = p_y$, $|\langle\psi|\varphi_n\rangle|^2 = p_n$, and $|\langle\varphi_n|\varphi_y\rangle|^2 = p_{ny}$, where $1/2 < p_y \le 1$. Then, if $p_{ny} < \frac{1}{2}$, $p_n < \frac{1}{2}$.*

proof: To prove this, we use Lemma 3.3. If $p_y = 1$, $p_n = p_{ny}$. Then $p_{ny} < \frac{1}{2}$ iff $p_n < \frac{1}{2}$. So, in the following, let $p_y = \frac{1}{2} + \varepsilon$, where $0 < \varepsilon < \frac{1}{2}$. By Lemma 3.3, $p_n \le (\sqrt{(\frac{1}{2}+\varepsilon)p_{ny}} + \sqrt{(\frac{1}{2}-\varepsilon)(1-p_{ny})})^2 \equiv p_{n_{max}}$. When $p_{n_{max}} < \frac{1}{2}$, $p_{ny} < \frac{1}{2} - \sqrt{\frac{1}{4}-\varepsilon^2} < \frac{1}{2}$. □

Corollary 1 *1. When $p_y = 1$, $p_{ny} = 0$ iff $p_n = 0$.*

2. When $\frac{1}{2} < p_y < 1$, $0 \le p_n \le 1 - p_y$ even if $p_{ny} = 0$, and we may be able to take $p_n = 0$ if $0 \le p_{ny} \le 1 - p_y$. □

These results imply that, when there exists a unitary matrix V such that $|\varphi_y\rangle \to V|\varphi_y\rangle = e^{i\theta}|\varphi_y\rangle$, we may be able to take θ such that the probability corresponding to the new unaccepted state $|\varphi'_n\rangle = V|\varphi_n\rangle$ is $|\langle\phi|\varphi'_n\rangle|^2 = |\langle\phi|(V|\varphi_n\rangle)|^2 < |\langle\phi|\varphi_n\rangle|^2$.

Next, we investigate about more general states.

Theorem 3.2 *Let $|\varphi_y\rangle$ and $|\varphi_{n_j}\rangle$ for $j = 1, \ldots, K$ be the accepted state and the unaccepted states, respectively, and we measure the states using an state $|\psi\rangle$. Moreover, let $|\langle\psi|\varphi_y\rangle|^2 = p_y$, $|\langle\psi|\varphi_{n_j}\rangle|^2 = p_{n_j}$, and $|\langle\varphi_{n_j}|\varphi_y\rangle|^2 = p_{n_j y}$, where $0 \le p_y, p_{n_j y} \le 1$. Then, for $j = 1, \ldots, K$,*

$$\begin{cases} p_n = p_y p_{n_j y} & (\textit{if } p_y = 1 \textit{ or } p_{n_j y} = 1), \\ 0 \le p_{n_j} \le (\sqrt{p_y p_{n_j y}} + \sqrt{(1-p_y)(1-p_{n_j y})})^2 & (\textit{if } p_y + p_{n_j y} \le 1), \\ (\sqrt{p_y p_{n_j y}} - \sqrt{(1-p_y)(1-p_{n_j y})})^2 \le p_{n_j} \le (\sqrt{p_y p_{n_j y}} + \sqrt{(1-p_y)(1-p_{n_j y})})^2 & \\ & (\textit{otherwise}). \end{cases}$$

Especially, let $1/2 < p_y \le 1$. Then, if $p_{n_j y} < \frac{1}{2}$, $p_{n_j} < \frac{1}{2}$.

proof: We can obtain by Lemma 3.3 and Theorem 3.1. □

The problem in [5] comes under this theorem. For $L(\ge 2)$ accepted states and one unaccepted state, we can obtain the similar theorem by exchanging the accepted states and the unaccepted state.

Finally, let us consider L accepted states and K unaccepted states.

Theorem 3.3 *Let $|\varphi_{y_i}\rangle$ for $i = 1, \ldots, L$, and $|\varphi_{n_j}\rangle$ for $j = 1, \ldots, K$ be the accepted states and the unaccepted states, respectively, and we measure the states using an state $|\psi\rangle$. Moreover, let $|\langle\psi|\varphi_{y_i}\rangle|^2 = p_{y_i}$, $|\langle\varphi_{n_j}|\varphi_{y_i}\rangle|^2 = p_{n_j y_i}$, and $|\langle\psi|\varphi_{n_j}\rangle|^2 = p_{n_j}$, where $0 \leq p_{y_i}, p_{n_j y_i} \leq 1$. Then, for $j = 1, \ldots, K$,*

$$\begin{cases} p_n = p_{y_m} p_{n_j y_m} & (\textit{if } p_{y_m} = 1 \textit{ or } p_{n_j y_m} = 1 \textit{ for some } m), \\ 0 \leq p_{n_j} \leq p_{n_{j_{max}}} & (\textit{if } p_{y_i} + p_{n_j y_i} \leq 1 \textit{ for all } i), \\ p_{n_{j_{min}}} \leq p_{n_j} \leq p_{n_{j_{max}}} & (\textit{otherwise}), \end{cases}$$

where, when $p_{n_j}(i)_\pm = (\sqrt{p_{y_i} p_{n_j y_i}} \pm \sqrt{(1 - p_{y_i})(1 - p_{n_j y_i})})^2$, then, for $h(= h_1, \ldots, h_l)$ satisfying $p_{y_h} + p_{n_j y_h} > 1$, $p_{n_{j_{min}}} = \max\{p_{n_j}(h_1)_-, \ldots, p_{n_j}(h_l)_-\}$, and $p_{n_{j_{max}}} = \min\{p_{n_j}(1)_+, \ldots, p_{n_j}(L)_+\}$. Especially, let $1/2 < p_{y_i} \leq 1$ for all i. Then, if $p_{n_j y_g} < \frac{1}{2}$ for $p_{n_j}(g)_+ = p_{n_{j_{max}}}$, $p_{n_j} < \frac{1}{2}$.

proof: We can obtain by Lemma 3.3 and Theorem 3.1. □

4 Conclusions

In this paper, when the probabilities of accepted states and the probabilities between accepted states and unaccepted states are given, we estimated the probabilities of unaccepted states. This is one indication to estimate the power of the QTM. Moreover, we will need to investigate the power of the QTM from several points of view. With investigations like this, the limitations of the power of the QTM will become more clear.

References

[1] C. H. Bennett, "Logical reversibility of computation", *IBM J. Res. Dev.*, **17**(1973), pp. 525-532.

[2] E. Bernstein and U. V. Vazirani, "Quantum complexity theory", in: *Proc. of 25th ACM Symposium on Theory of Computing* (San Diego, California, 1993), pp. 11-20.

[3] L. Debnath and P. Mikusiński, *Introduction to Hilbert spaces with applications* (Academic Press, San Diego, 1990).

[4] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proc. R. Soc. Lond.*, **A 400**(1985), pp. 97-117.

[5] D. Deutsch and R. Jozsa "Rapid Solution of Problems by Quantum Computation", *Proc. R. Soc. Lond.*, **A 439**(1992), pp. 553-558.

[6] R. P. Feynman, "Simulating Physics with Computers", *Int. J. Theor. Phys.*, **21**(1982), pp. 467-488.

[7] T. Mihara and T. Nishino, "Quantum computation and NP-complete problems", *Algorithms and Computation*, Lecture Notes in Computer Science, **834**(1994), pp. 387-395.

[8] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", in: *Proc. of 35th Annual Symposium on Foundations of Computer Science* (Santa Fe, New Mexico, 1994), pp. 124-134.

[9] K. Yoshida, *Functional analysis, 6th ed.* (Springer-Verlag, Berlin, 1980).