Quantum cryptography, quantum communication, and quantum computer in a noisy environment

Koji Nagata[1] and Tadao Nakamura[2]

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*
E-mail: ko_mi_na@yahoo.co.jp

[2] *Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*
E-mail: nakamura@pipelining.jp

(Dated: April 3, 2017)

First, we study several information theories based on quantum computing in a desirable noiseless situation. (1) We present quantum key distribution based on Deutsch's algorithm using an entangled state. (2) We discuss the fact that the Bernstein-Vazirani algorithm can be used for quantum communication including an error correction. Finally, we discuss the main result. We study the Bernstein-Vazirani algorithm in a noisy environment. The original algorithm determines a noiseless function. Here we consider the case that the function has an environmental noise. We introduce a noise term into the function $f(x)$. So we have another noisy function $g(x)$. The relation between them is $g(x) = f(x) \pm O(\epsilon)$. Here $O(\epsilon) \ll 1$ is the noise term. The goal is to determine the noisy function $g(x)$ with a success probability. The algorithm overcomes classical counterpart by a factor of N in a noisy environment.

PACS numbers: 03.67.Lx(Quantum computation architectures and implementations), 03.67.Ac(Quantum algorithms, protocols, and simulations), 03.67.Dd(Quantum cryptography), 03.67.Hk(Quantum communication)

I. INTRODUCTION

Quantum mechanics (cf. [1–6]) gives approximate but frequently remarkably accurate numerical predictions. Much experimental data approximately fit to the quantum predictions for the past some 100 years. We do not doubt the correctness of the quantum theory. The quantum theory also says new science with respect to information theory. The science is called the quantum information theory [6]. Therefore, the quantum theory gives us very useful another theory in order to create new information science and to explain the handling of raw experimental data in our physical world.

As for the foundations of the quantum theory, Leggett-type non-local variables theory [7] is experimentally investigated [8–10]. The experiments report that the quantum theory does not accept Leggett-type non-local variables interpretation. However there are debates for the conclusions of the experiments. See Refs. [11–13].

As for the applications of the quantum theory, implementation of a quantum algorithm to solve Deutsch's problem [14] on a nuclear magnetic resonance quantum computer is reported firstly [15]. Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is also reported [16]. There are several attempts to use single-photon two-qubit states for quantum computing. Oliveira *et al.* implement Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [17]. Single-photon Bell states are prepared and measured [18]. Also the decoherence-free implementation of Deutsch's algorithm is reported by using such single-photon and by using two logical qubits [19]. More recently, a one-way based experimental implementation of Deutsch's algorithm is reported [20]. In 1993, the Bernstein-Vazirani algorithm was reported [21]. It can be considered as an extended Deutsch-Jozsa algorithm. In 1994, Simon's algorithm was reported [22]. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement on an ensemble quantum computer is reported [23]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits is discussed [24]. Quantum learning robust against noise is studied [25]. A quantum algorithm for approximating the influences of Boolean functions and its applications is recently reported [26]. It is discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [27]. Transport implementation of the Bernstein-Vazirani algorithm with ion qubits is more recently reported [28].

Quantum communication is the art of transferring a quantum state from one place to another. Traditionally, the sender is named Alice and the receiver Bob. The basic motivation is that quantum states code quantum information - called qubits in the case of 2-dimensional Hilbert spaces and that quantum information allows one to perform tasks that could only be achieved far less efficiently, if at all, using classical information.

On the other hand, the earliest quantum algorithm, the Deutsch-Jozsa algorithm, is representative to show that quantum computation is faster than classical counterpart with a magnitude that grows exponentially with the number of qubits. In 2015, it is discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [27].

There are many researches concerning quantum computing. In a real experiment, we cannot avoid an environmental noise. We address this problem by providing more concrete way rather than [25].

In this paper, first, we study several information theories based on quantum computing in a noiseless environment. We present secure quantum key distribution based on Deutsch's algorithm. The security of the protocol is based on it of Ekert 91 protocol [29].

Next, we study quantum communication including an error correction based on the Bernstein-Vazirani algorithm. The original algorithms determine a bit-strings. Here we discuss the fact that the Bernstein-Vazirani algorithm can be used for quantum communication including an error correction. Let us explain the situation. Alice has a bit-strings $b = (b_1, b_2, \ldots, b_N)$. Bob has another bit-strings $c = (c_1, c_2, \ldots, c_N)$. The goal is to correct errors of them. We have discussed the fact that the quantum communication overcomes classical counterpart by a factor of N in the protocol.

Finally, we study the Bernstein-Vazirani algorithm in a noisy environment. The original algorithm determines a noiseless function. Here we consider the case that the function has an environmental noise. Let us explain the situation. We introduce a noise term into the function $f(x)$. So we have another noisy function $g(x)$. The relation between them is $g(x) = f(x) \pm O(\epsilon)$. Here $O(\epsilon) \ll 1$ is the noise term. The goal is to determine the noisy function $g(x)$ with a success probability. We discuss the fact that the quantum algorithm overcomes classical counterpart by a factor of N.

This paper is organized as follows:

In Sec. II, we review Deutsch's algorithm along with Ref. [6].

In Sec. III, we study Deutsch's algorithm by using another input state. In this case, we cannot perform Deutsch's algorithm.

In Sec. IV, we study Deutsch's algorithm by using the Bell state.

In Sec. V, we discuss the fact that Deutsch's algorithm can be used for quantum key distribution by using an entangled state.

In Sec. VI, we review the Bernstein-Vazirani algorithm.

In Sec. VII, we study quantum communication based on the Bernstein-Vazirani algorithm.

In Sec. VIII, we present an error correction based on the Bernstein-Vazirani algorithm.

In Sec. IX, we present the Bernstein-Vazirani algorithm in a noisy environment.

Section X concludes this paper.

II. A REVIEW OF DEUTSCH'S ALGORITHM

In this section, we review Deutsch's algorithm along with Ref. [6].

Quantum parallelism is a fundamental feature of many quantum algorithms. It allows quantum computers to evaluate the values of a function $f(x)$ for many different values of x simultaneously. Suppose

$$f : \{0, 1\} \rightarrow \{0, 1\} \tag{1}$$

is a function with a one-bit domain and range. A convenient way of computing this function on a quantum computer is to consider a two-qubit quantum computer which starts in the state

$$|x, y\rangle. \tag{2}$$

With an appropriate sequence of logic gates it is possible to transform this state into

$$|x, y \oplus f(x)\rangle, \tag{3}$$

where $\oplus$ indicates addition modulo 2. We give the transformation defined by the map

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle \tag{4}$$

a name, U_f.

Deutsch's algorithm combines quantum parallelism with a property of quantum mechanics known as interference. Let us use the Hadamard gate to prepare the first qubit

$$|0\rangle \tag{5}$$

as the superposition

$$(|0\rangle + |1\rangle)/\sqrt{2}, \tag{6}$$

but let us prepare the second qubit as the superposition

$$(|0\rangle - |1\rangle)/\sqrt{2}, \tag{7}$$

using the Hadamard gate applied to the state

$$|1\rangle. \tag{8}$$

The Hadamard gate is as

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 1| + |1\rangle\langle 0| + |0\rangle\langle 0| - |1\rangle\langle 1|). \tag{9}$$

Let us follow the states along to see what happens in this circuit. The input state

$$|\psi_0\rangle = |01\rangle \tag{10}$$

is sent through two Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{11}$$

A little thought shows that if we apply U_f to the state

$$|x\rangle(|0\rangle - |1\rangle)/\sqrt{2} \tag{12}$$

then we obtain the state

$$(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}. \tag{13}$$

Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1). \end{cases} \tag{14}$$

The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle|1\rangle & \text{if } f(0)=f(1) \\ \pm|1\rangle|1\rangle & \text{if } f(0)\neq f(1). \end{cases} \tag{15}$$

so by measuring the first qubit we may determine $f(0)\oplus f(1)$. This is very interesting indeed: the quantum circuit gives us the ability to determine a global property of $f(x)$, namely $f(0)\oplus f(1)$, using only one evaluation of $f(x)$! This is faster than is possible with a classical apparatus, which would require at least two evaluations.

III. FAILING DEUTSCH'S ALGORITHM

In this section, we study Deutsch's algorithm by using another input state. In this case, we cannot perform Deutsch's algorithm as shown below.

The input state

$$|\psi_0\rangle = |10\rangle \tag{16}$$

is sent through two Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]. \tag{17}$$

We apply U_f to the following state

$$\frac{|0\rangle-|1\rangle}{\sqrt{2}}|x\rangle. \tag{18}$$

If $x=1$

$$\frac{|0\rangle|1\rangle-|1\rangle|1\rangle}{\sqrt{2}} \tag{19}$$

we have

$$\frac{|0\rangle|\overline{f(0)}\rangle-|1\rangle|\overline{f(1)}\rangle}{\sqrt{2}} \tag{20}$$

and if $x=0$

$$\frac{|0\rangle|0\rangle-|1\rangle|0\rangle}{\sqrt{2}} \tag{21}$$

we have

$$\frac{|0\rangle|f(0)\rangle-|1\rangle|f(1)\rangle}{\sqrt{2}}. \tag{22}$$

Thus,

$$\frac{|0\rangle(|f(0)\rangle+|\overline{f(0)}\rangle)-|1\rangle(|f(1)\rangle+|\overline{f(1)}\rangle)}{\sqrt{2}}. \tag{23}$$

Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1). \end{cases} \tag{24}$$

The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm|1\rangle|0\rangle & \text{if } f(0)=f(1) \\ \pm|1\rangle|0\rangle & \text{if } f(0)\neq f(1). \end{cases} \tag{25}$$

In this case we fail to perform Deutsch's algorithm.

IV. DEUTSCH'S ALGORITHM USING THE BELL STATE

In this section, we study Deutsch's algorithm by using the Bell state.

The input state

$$|\psi_0\rangle = \frac{|10\rangle+|01\rangle}{\sqrt{2}} \tag{26}$$

is sent through two Hadamard gates to give

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] + \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]). \tag{27}$$

Applying U_f to $|\psi_1\rangle$ therefore leaves us with one of the two possibilities:

$$|\psi_2\rangle = \pm\frac{1}{\sqrt{2}}(\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] \pm \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]) \tag{28}$$

if $f(0)=f(1)$, or

$$|\psi_2\rangle = \pm\frac{1}{\sqrt{2}}(\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] \pm \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]). \tag{29}$$

if $f(0)\neq f(1)$. The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm\frac{|1\rangle|0\rangle\pm|0\rangle|1\rangle}{\sqrt{2}} & \text{if } f(0)=f(1) \text{ entanglement} \\ \pm\frac{|1\rangle|0\rangle\pm|1\rangle|1\rangle}{\sqrt{2}} & \text{if } f(0)\neq f(1) \text{ separable.} \end{cases} \tag{30}$$

so by measuring the qubits (by means of the Bell measurement) we may determine $f(0)\oplus f(1)$. The Bell measurement is explained as follows: Alice and Bob prepare the Bell basis

$$
\begin{aligned}
|\Psi_+\rangle &= \frac{|1\rangle|0\rangle + |0\rangle|1\rangle}{\sqrt{2}} \\
|\Psi_-\rangle &= \frac{|1\rangle|0\rangle - |0\rangle|1\rangle}{\sqrt{2}} \\
|\Phi_+\rangle &= \frac{|1\rangle|1\rangle + |0\rangle|0\rangle}{\sqrt{2}} \\
|\Phi_-\rangle &= \frac{|1\rangle|1\rangle - |0\rangle|0\rangle}{\sqrt{2}} \qquad (31)
\end{aligned}
$$

If the state $|\psi_3\rangle$ is an entangled state, we have

$$
\begin{aligned}
&|\langle\psi_3|\Psi_+\rangle|^2 = 1 \ \text{ or } \ |\langle\psi_3|\Psi_-\rangle|^2 = 1 \ \text{ or} \\
&|\langle\psi_3|\Phi_+\rangle|^2 = 1 \ \text{ or } \ |\langle\psi_3|\Phi_-\rangle|^2 = 1. \qquad (32)
\end{aligned}
$$

Therefore the measurement outcome should be 1 if the function is constant. If the state $|\psi_3\rangle$ is a separable state, we have

$$
\begin{aligned}
&|\langle\psi_3|\Psi_+\rangle|^2 = 1/2 \ \text{ or } \ |\langle\psi_3|\Psi_-\rangle|^2 = 1/2 \ \text{ or} \\
&|\langle\psi_3|\Phi_+\rangle|^2 = 1/2 \ \text{ or } \ |\langle\psi_3|\Phi_-\rangle|^2 = 1/2. \qquad (33)
\end{aligned}
$$

Therefore the measurement outcome should be not 1 if the function is balanced.

V. QUANTUM KEY DISTRIBUTION BASED ON DEUTSCH'S ALGORITHM

We discuss the fact that Deutsch's algorithm can be used for quantum key distribution by using an entangled state.

Alice and Bob have promised to use a function f which is of one of two kinds; either the value of f is constant or balanced. To Eve, it is secret. Alice's and Bob's goal is to determine with certainty whether they have chosen a constant or a balanced function without information of the function to Eve. If the function is constant the output qubits are entangled, otherwise separable. Alice and Bob perform the Bell measurement. Alice and Bob share one secret bit if they determine the function f by getting a suitable measurement outcome. The existence of Eve destroys entanglement. The security of our protocol is based on it of Ekert 91 protocol [29].

- First Alice prepares the entangled qubits, applies the Hadamard transformation to the state, and sends the output state described in the Bell state to Bob.

- Next, Bob randomly picks a function "f" that is either balanced or constant and Bob applies U_f. He then sends the one qubit to Alice.

- Finally, Alice and Bob perform the Bell measurement. She learns whether f was balanced or constant. If the final qubits are entangled, then the function is constant. If the final qubits are not entangled, then the function is balanced - Alice and Bob now share a secret bit of information (the "type" of $f(x)$).

- The result of the Bell measurement is 1 if the function is constant.

- Alice and Bob compare a subset of all the results of the Bell measurements when the function is constant; all of them should be 1.

- The existence of Eve must destroy entanglement (Ekert 91).

- Eve is detected in the following case; The result of the Bell measurement is not 1 and the function is constant.

In conclusion, we have shown that Deutsch's algorithm can be used for secure quantum key distribution. The security is based on it of Ekert 91 protocol.

VI. A REVIEW OF THE BERNSTEIN-VAZIRANI ALGORITHM

In this section, we review the Bernstein-Vazirani algorithm. Suppose

$$f : \{0,1\}^N \to \{0,1\} \qquad (34)$$

is a function with a N-bit domain and a 1-bit range. We assume the following case

$$
\begin{aligned}
f(x) &= a\cdot x = \sum_{i=1}^{N} a_i x_i (\text{mod}2) \\
&= a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \cdots \oplus a_N x_N, \\
& a \in \{0,1\}^N \qquad (35)
\end{aligned}
$$

The goal is to determine $f(x)$. Let us follow the quantum states through the Bernstein-Vazirani algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \qquad (36)$$

After the Hadamard transformation on the state we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \qquad (37)$$

Next, the function f is evaluated (by Bob) using

$$U_f : |x, y\rangle \to |x, y\oplus f(x)\rangle, \qquad (38)$$

giving

$$|\psi_2\rangle = \pm\sum_{x} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \qquad (39)$$

Here

$$y \oplus f(x) \tag{40}$$

is the bitwise XOR (exclusive OR) of y and $f(x)$. To determine the result of the Hadamard transformation it helps to first calculate the effect of the Hadamard transformation on a state

$$|x\rangle. \tag{41}$$

By checking the cases $x = 0$ and $x = 1$ separately we see that for a single qubit

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}. \tag{42}$$

Thus

$$H^{\otimes N}|x_1, \ldots, x_N\rangle = \frac{\sum_{z_1,\ldots,z_N}(-1)^{x_1z_1+\cdots+x_Nz_N}|z_1, \ldots, z_N\rangle}{\sqrt{2^N}}. \tag{43}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z(-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}}, \tag{44}$$

where

$$x \cdot z \tag{45}$$

is the bitwise inner product of x and z, modulo 2. Using this equation and (39) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{46}$$

Thus,

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+a\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{47}$$

We notice

$$\sum_x(-1)^{x\cdot z+a\cdot x} = 2^N\delta_{a,z}. \tag{48}$$

Thus,

$$\begin{aligned}|\psi_3\rangle &= \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+a\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\\ &= \pm\sum_z \frac{2^N\delta_{a,z}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\\ &= \pm|a\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\\ &= \pm|a_1a_2a_3\cdots a_N\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right].\end{aligned} \tag{49}$$

Alice now observes

$$|a_1a_2a_3\cdots a_N\rangle. \tag{50}$$

Summarizing, if Alice measures $|a_1a_2a_3\cdots a_N\rangle$ the function is

$$f(x_1, x_2, ..., x_N) = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \cdots \oplus a_Nx_N. \tag{51}$$

VII. QUANTUM COMMUNICATION BASED ON THE BERNSTEIN-VAZIRANI ALGORITHM

We study quantum communication based on the Bernstein-Vazirani algorithm.

Alice and Bob have promised to select a function $f(x_1, x_2, ..., x_N) = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \cdots \oplus a_Nx_N$. Alice does not know $a_1, a_2, ..., a_N$. Bob knows $a_1, a_2, ..., a_N$. Alice's goal is to determine with certainty what $a_1, a_2, ..., a_N$ Bob has chosen. In the classical theory, Alice has to ask Bob N questions. In the quantum theory, Alice has to ask Bob "one" question! Alice prepares suitable $N + 1$ partite uncorrelated state, performs the Hadamard transformation to the state, and sends to the output state to Bob. And Bob performs the Bernstein-Vazirani algorithm and inputs the information of the a into the finall state. Alice asks him what state is. Alice measures the finall state and she knows the a. If the a is learned by Alice, Alice and Bob share N bits of information, by one communication with each other. The speed to share N bits improves by a factor of N by comparing the classical case. This shows quantum communication overcomes classical communication by a factor of N.

- First Alice prepares the qubits in (37) and sends the $N + 1$ qubits to Bob.
- Next, Bob picks N bits "a" and Bob applies U_f Eq. (38) evolving the $N + 1$ qubits to Eq. (39). He then sends the N qubit to Alice.
- Finally, Alice applies the Hadamard transformation to each of the qubits and measures. She learns $f(x) = a \cdot x = \sum_{i=1}^N a_ix_i(\text{mod}2) = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \cdots \oplus a_Nx_N$ - Alice and Bob now share N bits of information (the "type" of $f(x)$).
- In the classical case (without this quantum computing), Alice needs at least N-communication with Bob to share N bits of information.

In conclusion, we have shown quantum communication overcomes classical communication by a factor of N in the Bernstein-Vazirani algorithm case.

However there may be an error between Alice's bits-strings and Bob's one. In the next section, we discuss an error correction based on the Bernstein-Vazirani algorithm.

VIII. AN ERROR CORRECTION BASED ON THE BERNSTEIN-VAZIRANI ALGORITHM

In this section, we present an error correction based on the Bernstein-Vazirani algorithm. Suppose

$$f : \{0, 1\}^N \to \{0, 1\} \tag{52}$$

is a function with a N-bit domain and a 1-bit range. We introduce two functions $g(x)$ and $h(x)$. The relation with the function $f(x)$ is as follows:

$$f(x) = g(x) \oplus h(x). \tag{53}$$

We assume the following case

$$\begin{aligned} & g(x) = b \cdot x = \sum_{i=1}^{N} b_i x_i (\mathrm{mod} 2) \\ & = b_1 x_1 \oplus b_2 x_2 \oplus b_3 x_3 \oplus \cdots \oplus b_N x_N, \\ & h(x) = c \cdot x = \sum_{i=1}^{N} c_i x_i (\mathrm{mod} 2) \\ & = c_1 x_1 \oplus c_2 x_2 \oplus c_3 x_3 \oplus \cdots \oplus c_N x_N, \\ & f(x) = \sum_{i=1}^{N} (b_i \oplus c_i) x_i (\mathrm{mod} 2) \\ & = (b_1 \oplus c_1) x_1 \oplus (b_2 \oplus c_2) x_2 \oplus (b_3 \oplus c_3) x_3 \oplus \cdots \\ & \oplus (b_N \oplus c_N) x_N, \\ & b_j, c_j = 0, 1, \ x_j = 0, 1. \end{aligned} \tag{54}$$

Alice has a bit-strings $b = (b_1, b_2, \ldots, b_N)$. Bob has another bit-strings $c = (c_1, c_2, \ldots, c_N)$. We want to correct errors of them.

Let us follow the quantum states through the algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N} |1\rangle. \tag{55}$$

After the Hadamard transformation on the state we have

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \tag{56}$$

Next, the function f is evaluated using

$$U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle, \tag{57}$$

giving

$$|\psi_2\rangle = \pm \sum_{x} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \tag{58}$$

After the Hadamard transformation, by using (58) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \tag{59}$$

We have

$$\begin{aligned} |\psi_3\rangle & = \pm \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + g(x) \oplus h(x)} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ & = \pm \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + x \cdot b \oplus x \cdot c} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ & = \pm \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + x \cdot (b+c)} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right], \end{aligned} \tag{60}$$

where

$$b + c = (b_1 \oplus c_1, b_2 \oplus c_2, \ldots, b_N \oplus c_N). \tag{61}$$

We notice

$$\sum_{x} (-1)^{x \cdot z + x \cdot (b+c)} = 2^N \delta_{(b+c), z}. \tag{62}$$

Thus,

$$\begin{aligned} |\psi_3\rangle & = \pm \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + x \cdot (b+c)} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ & = \pm \sum_{z} \frac{2^N \delta_{(b+c), z} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ & = \pm |b + c\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ & = \pm |b_1 \oplus c_1, b_2 \oplus c_2, b_3 \oplus c_3, \ldots, b_N \oplus c_N\rangle \\ & \times \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \end{aligned} \tag{63}$$

Alice now observes

$$|b_1 \oplus c_1, b_2 \oplus c_2, b_3 \oplus c_3, \ldots, b_N \oplus c_N\rangle. \tag{64}$$

Summarizing, if Alice measures $|100 \cdots 0\rangle$ the relation is

$$b_1 \oplus c_1 = 1, b_2 \oplus c_2 = 0, \ldots, b_N \oplus c_N = 0. \tag{65}$$

Thus there is an errors for the first bit:

$$b_1 \neq c_1, b_2 = c_2, \ldots, b_N = c_N. \tag{66}$$

Hence Alice detects the error. In general, Alice can know where such errors are.

If Alice measures $|000 \cdots 0\rangle$ the relation is

$$b_1 \oplus c_1 = 0, b_2 \oplus c_2 = 0, \ldots, b_N \oplus c_N = 0. \tag{67}$$

Thus Alice and Bob share N-bits of information.

$$b_1 = c_1, b_2 = c_2, \ldots, b_N = c_N. \tag{68}$$

We discuss the fact that the quantum error correction overcomes classical counterpart by a factor of N in this case.

IX. THE BERNSTEIN-VAZIRANI ALGORITHM IN A NOISY ENVIRONMENT

In this section, we present the Bernstein-Vazirani algorithm in a noisy environment. Suppose

$$f : \{0, 1\}^N \rightarrow \{0, 1\} \tag{69}$$

is a noiseless function with a N-bit domain and a 1-bit range. We introduce a noisy function g by using the function $f(x)$

$$g(x) = f(x) \pm O(\epsilon). \tag{70}$$

Here $O(\epsilon) \ll 1$ is the noise term.

The noise is explained as follows. Suppose two qubits are described by a superposition state and the value of a function ($f(1)$) has an error. Then there must be two error states. (For example, when we treat 100 bits and there are two errors, the error probability is 2/100=1/50).

Let us explain by using a quantum state:

$$\begin{aligned}|\psi\rangle &= \frac{|1\rangle_1+|0\rangle_1}{\sqrt{2}}\frac{|1\rangle_2+|0\rangle_2}{\sqrt{2}}\\ &= \frac{|1\rangle_1|1\rangle_2+|1\rangle_1|0\rangle_2+|0\rangle_1|1\rangle_2+|0\rangle_1|0\rangle_2}{2} \end{aligned} \quad (71)$$

is the superposition state. The function f is evaluated using

$$U_f : |x,y\rangle \rightarrow |x, y\oplus f(x)\rangle. \quad (72)$$

Thus,

$$\begin{aligned}U_f|\psi\rangle &= U_f\frac{|1,1\rangle+|1,0\rangle+|0,1\rangle+|0,0\rangle}{2}\\ &= (1/2)(|1,1\oplus f(1)\rangle+|1,0\oplus f(1)\rangle\\ &+|0,1\oplus f(0)\rangle+|0,0\oplus f(0)\rangle). \end{aligned}\quad (73)$$

Therefore, there are two $f(1)$s in the output state. If there is an error for $f(1)$, then the following two states

$$|1,1\oplus f(1)\rangle, |1,0\oplus f(1)\rangle \quad (74)$$

have an error, simultaneously. Thus the number of errors is even. Here we globally treat such errors in a statistical model.

We assume the following case

$$\begin{aligned}g(x) &= a\cdot x = \sum_{i=1}^{N} a_i' x_i (\mathrm{mod} 2) \pm O(\epsilon)\\ &= a_1'x_1 \oplus a_2'x_2 \oplus a_3'x_3 \oplus \cdots \oplus a_N'x_N\\ &\pm\epsilon(x_1+x_2\cdots+x_N) = f(x)\pm O(\epsilon),\\ & a_j = a_j' \pm \epsilon,\ a_j' = 0,1,\ x_j = 0,1. \end{aligned}\quad (75)$$

We want to determine $a_1, a_2, ..., a_N$ with a success probability simultaneously so that we determine the noisy function $g(x)$ with the success probability. It is the Bernstein-Vazirani algorithm in a noisy environment.

Let us follow the quantum states through the algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \quad (76)$$

After the Hadamard transformation on the state we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \quad (77)$$

Next, the function g is approximately evaluated using

$$U_g : |x,y\rangle \rightarrow |x, y\oplus [g(x)]\rangle. \quad (78)$$

On a real line, $[g(x)]$ is the nearest natural number from $g(x)$. Here we see $[g(x)] = 0,1$ and

$$[g(x)] = f(x). \quad (79)$$

We have

$$|\psi_2\rangle = \pm\sum_x \frac{(-1)^{[g(x)]}|x\rangle}{\sqrt{2^N}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \quad (80)$$

After the Hadamard transformation, by using (80) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+[g(x)]}|z\rangle}{2^N}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \quad (81)$$

So we have

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+g(x)\pm O(\epsilon)}|z\rangle}{2^N}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \quad (82)$$

We notice

$$(-1)^{\pm O(\epsilon)}|z\rangle = (e^{\pm i\pi O(\epsilon)})|z\rangle \simeq |z\rangle \quad (83)$$

because $(e^{\pm i\pi O(\epsilon)}) \simeq 1$.

Thus we have

$$|\psi_3\rangle \simeq \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+a\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \quad (84)$$

In what follows, we evaluate $\sum_x(-1)^{x\cdot z+a\cdot x}$. We notice

$$\begin{aligned}&\sum_x (e^{i\pi})^{x_1z_1+\cdots+x_Nz_N}(e^{i\pi})^{x_1a_1+\cdots+x_Na_N}\\ &= \sum_x (e^{i\pi})^{x_1(z_1+a_1)+\cdots+x_N(z_N+a_N)}\\ &= \sum_{x_1}(e^{i\pi})^{x_1(z_1+a_1)}\cdots\sum_{x_N}(e^{i\pi})^{x_N(z_N+a_N)}. \end{aligned}\quad (85)$$

We have the following:

$$\sum_{x_1}(e^{i\pi})^{x_1(z_1+a_1)} = (1+(e^{i\pi z_1})(e^{i\pi a_1})). \quad (86)$$

By checking the cases $z_1 = 0$ and $z_1 = 1$ separately we see that

$$\begin{aligned}&(1+(e^{i\pi a_1}))|0\rangle_1 + (1-(e^{i\pi a_1}))|1\rangle_1\\ =&2e^{i\pi a_1/2}\frac{(e^{-i\pi a_1/2}+(e^{i\pi a_1/2})}{2}|0\rangle_1\\ &+2ie^{i\pi a_1/2}\frac{(e^{-i\pi a_1/2}-(e^{i\pi a_1/2})}{2i}|1\rangle_1\\ &= 2(i)^{a_1}\cos(a_1\pi/2)|0\rangle_1 - i(i)^{a_1}2\sin(a_1\pi/2)|1\rangle_1. \end{aligned}\quad (87)$$

Thus we have

$$\begin{aligned}|\psi_3\rangle &\simeq \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+a\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\\ &= \pm\sum_z \frac{(1+(-1)^{z_1}e^{i\pi a_1}))\cdots(1+(-1)^{z_N}e^{i\pi a_N}))|z\rangle}{2^N}\\ &\times\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\\ &= \pm\prod_{j=1\ldots N}[(i)^{a_j}\cos(a_j\pi/2)|0\rangle_j - i(i)^{a_j}\sin(a_j\pi/2)|1\rangle_j]\\ &\times\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \end{aligned}\quad (88)$$

We now observe a quantum state $|100\cdots 1\rangle$ with high probability if

$$(a_1 = 1 \pm \epsilon), |\cos(a_1\pi/2)|^2 \ll |\sin(a_1\pi/2)|^2,$$
$$(a_2 = \pm\epsilon), |\cos(a_2\pi/2)|^2 \gg |\sin(a_2\pi/2)|^2,$$
$$(a_3 = \pm\epsilon), |\cos(a_3\pi/2)|^2 \gg |\sin(a_3\pi/2)|^2, ...,$$
$$(a_N = 1 \pm \epsilon), |\cos(a_N\pi/2)|^2 \ll |\sin(a_N\pi/2)|^2. \quad (89)$$

Therefore, we present the Bernstein-Vazirani algorithm in a noisy environment.

We introduce a success probability of finding a_1: It is the probability of detecting $|1\rangle_1$ if $a_1 = 1 \pm \epsilon$. On the other hand, an error probability of finding a_1 is as follows: It is the probability of detecting $|0\rangle$ if $a_1 = 1 \pm \epsilon$. In what follows, we evaluate the success probability of the algorithm. It is the probability that we detect the desirable quantum states for all $a_1, a_2, \ldots, a_N$.

The error probability for a_1 is

$$|\cos(a_1\pi/2)|^2 = E_1. \quad (90)$$

The error probability for a_2 is

$$|\sin(a_2\pi/2)|^2 = E_2, \quad (91)$$

and so on. The success probability for a_1 is

$$|\sin(a_1\pi/2)|^2 = 1 - E_1. \quad (92)$$

The success probability for a_2 is

$$|\cos(a_2\pi/2)|^2 = 1 - E_2, \quad (93)$$

and so on. The success probability S for the algorithm is

$$S = (1 - E_1)(1 - E_2)\cdots(1 - E_N). \quad (94)$$

The algorithm we discussed determines $a_1, a_2, ..., a_N$ simultaneously with the success probability S. So we can know the noisy function $g(x)$ with the success probability S.

We discuss the fact that the quantum algorithm overcomes classical counterpart by a factor of N in the algorithm over an environmental noise.

X. CONCLUSIONS

In conclusion, first, we have presented quantum key distribution based on Deutsch's algorithm by using an entangled state. The idea of the security of the protocol has been based on it of Ekert 91 protocol. The existence of eavesdroppers must has destroyed entanglement.

Next, we have studied quantum communication including an error correction. It has been based on the Bernstein-Vazirani algorithm. The original algorithm has determined a bit-strings. Here we have discussed the fact that the Bernstein-Vazirani algorithm can be used for quantum communication including an error correction. Let us explain the situation. Alice has had a bit-strings $b = (b_1, b_2, \ldots, b_N)$. Bob has had another bit-strings $c = (c_1, c_2, \ldots, c_N)$. The goal has been to correct errors of them. We have discussed the fact that the quantum communication overcomes classical counterpart by a factor of N in the Bernstein-Vazirani algorithm.

Finally, we have studied the Bernstein-Vazirani algorithm having an environmental noise. The original algorithm has determined a noiseless function. Here we have considered the case that the function has an environmental noise. Let us explain the situation. We have introduced a noise term into the original function $f(x)$. So we have had another noisy function $g(x)$. The relation between them has been $g(x) = f(x) \pm O(\epsilon)$. Here $O(\epsilon) \ll 1$ has been the noise term. The goal has been to determine the noisy function $g(x)$ with a success probability. We have discussed the fact that the quantum algorithm overcomes classical counterpart by a factor of N in the algorithm including the noise function case.

[1] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, New Jersey, 1955).
[2] R. P. Feynman, R. B. Leighton, and M. Sands, *Lectures on Physics, Volume III, Quantum mechanics* (Addison-Wesley Publishing Company, 1965).
[3] M. Redhead, *Incompleteness, Nonlocality, and Realism* (Clarendon Press, Oxford, 1989), 2nd ed.
[4] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, The Netherlands, 1993).
[5] J. J. Sakurai, *Modern Quantum Mechanics* (Addison-Wesley Publishing Company, 1995), Revised ed.
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[7] A. J. Leggett, Found. Phys. **33**, 1469 (2003).
[8] S. Gröblacher, T. Paterek, R. Kaltenbaek, Č. Brukner, M. Żukowski, M. Aspelmeyer, and A. Zeilinger, Nature (London) **446**, 871 (2007).
[9] T. Paterek, A. Fedrizzi, S. Gröblacher, T. Jennewein, M. Żukowski, M. Aspelmeyer, and A. Zeilinger, Phys. Rev. Lett. **99**, 210406 (2007).
[10] C. Branciard, A. Ling, N. Gisin, C. Kurtsiefer, A. Lamas-Linares, and V. Scarani, Phys. Rev. Lett. **99**, 210407 (2007).
[11] A. Suarez, Found. Phys. **38**, 583 (2008).
[12] M. Żukowski, Found. Phys. **38**, 1070 (2008).
[13] A. Suarez, Found. Phys. **39**, 156 (2009).
[14] D. Deutsch, *Proc. Roy. Soc. London Ser. A* **400**, 97 (1985).
[15] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).
[16] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J.

Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature (London) **421**, 48 (2003).

[17] A. N. de Oliveira, S. P. Walborn, and C. H. Monken, J. Opt. B: Quantum Semiclass. Opt. **7**, 288-292 (2005).

[18] Y.-H. Kim, Phys. Rev. A **67**, 040301(R) (2003).

[19] M. Mohseni, J. S. Lundeen, K. J. Resch, and A. M. Steinberg, Phys. Rev. Lett. **91**, 187903 (2003).

[20] M. S. Tame, R. Prevedel, M. Paternostro, P. Böhi, M. S. Kim, and A. Zeilinger, Phys. Rev. Lett. **98**, 140501 (2007).

[21] E. Bernstein and U. Vazirani, Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC '93), pp. 11-20 (1993), doi:10.1145/167088.167097; SIAM J. Comput. 26-5, pp. 1411-1473 (1997).

[22] D. R. Simon, Foundations of Computer Science, (1994) Proceedings., 35th Annual Symposium on: 116-123, retrieved 2011-06-06.

[23] J. Du, M. Shi, X. Zhou, Y. Fan, B. J. Ye, R. Han, and J. Wu, Phys. Rev. A **64**, 042306 (2001).

[24] E. Brainis, L.-P. Lamoureux, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, Phys. Rev. Lett. **90**, 157902 (2003).

[25] A. W. Cross, G. Smith, and J. A. Smolin, Phys. Rev. A **92**, 012327 (2015).

[26] H. Li and L. Yang, Quantum Inf. Process. **14**, 1787 (2015).

[27] K. Nagata and T. Nakamura, Open Access Library Journal, 2: e1798 (2015). http://dx.doi.org/10.4236/oalib.1101798.

[28] S. D. Fallek, C. D. Herold, B. J. McMahon, K. M. Maller, K. R. Brown, and J. M. Amini. New J. Phys. **18**, 083030 (2016).

[29] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).