Quantum communication based on the Bernstein–Vazirani algorithm

Koji Nagata
Korea Advanced Institute of Science and Technology

Quantum communication based on the Bernstein-Vazirani algorithm

Koji Nagata[1] and Tadao Nakamura[2]

[1]*Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 305-701, 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: March 26, 2016)

In trial, we present quantum key distribution based on Deutsch's algorithm 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. If the function is constant the output qubits are entangled, otherwise separable. Alice and Bob perform the Bell measurement. Alice and Bob get one key if they determine the function f by getting a suitable measurement outcome. Next, we discuss the relation between quantum communication and the Bernstein-Vazirani algorithm. In classical theory, one communication leads us to share one bit of information. However, in quantum theory, the same communication, surprisingly, leads us to share many bits containing much information, even a function itself. First, 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 function Bob has chosen. In classical theory, Alice has to ask Bob N times. In quantum theory, Alice has to ask Bob one time. Alice prepares suitable $N + 1$ partite uncorrelated state, performs the Hadamard transformation to the state, and sends the output state to Bob. And Bob performs the Bernstein-Vazirani algorithm and inputs the information of the function into the finall state. Alice asks him what state is. Alice measures the finall state and she knows the function. If the function is determined, 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.

PACS numbers: 03.67.-a(Quantum information theory), 03.67.Lx(Quantum computer), 03.67.Dd(Quantum cryptography)

I. INTRODUCTION

The quantum theory (cf. [1–6]) gives approximate and at times remarkably accurate numerical predictions. Much experimental data approximately fits 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. As for the applications of the quantum theory, implementation of a quantum algorithm to solve Deutsch's problem [11] on a nuclear magnetic resonance quantum computer is reported firstly [12]. Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is also reported [13]. 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 [14]. Single-photon Bell states are prepared and measured [15]. Also the decoherence-free implementation of Deutsch's algorithm is reported by using such single-photon and by using two logical qubits [16]. More recently, a one-way based experimental implementation of Deutsch's algorithm is reported [17].

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. The best known example is Quantum Key Distribution (QKD).

The most well known and developed application of quantum cryptography is quantum key distribution, which is the process of using quantum communication to establish a shared key between two parties without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. This is achieved by Alice encoding the bits of the key as quantum data and sending them to Bob; if Eve tries to learn these bits, the messages will be disturbed and Alice and Bob will notice. The key is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used as the seed of the same random number generator both by Alice and Bob.

The security of QKD can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution. This is usually described as "unconditional security", although there are some minimal assumptions required including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack would be possible.

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. Recently, it is discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [18]. In 1993, the Bernstein-Vazirani algorithm was reported [19]. It can be considered as an extended Deutsch-Jozsa algorithm. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement on an ensemble quantum computer is reported [20]. We investigate the relation between quantum key distribution and quantum computer more.

In this paper, we present quantum key distribution based on Deutsch's algorithm 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. Next, we discuss quantum communication utilising the Bernstein-Vazirani algorithm. First, 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 function Bob has chosen. In classical theory, Alice has to ask Bob N times. In quantum theory, Alice has to ask Bob one time. 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 function into the finall state. Alice asks him what state is. Alice measures the finall state and she knows the function. If the function is determined, 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.

II. 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 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:

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

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 review 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 review 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

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

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

$$|\psi_2\rangle = \begin{cases} \pm\frac{1}{\sqrt{2}}\left(\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\right) & \text{if} \quad f(0) = f(1) \\ \pm\frac{1}{\sqrt{2}}\left(\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\right) & \text{if} \quad f(0) \neq f(1). \end{cases} \tag{28}$$

The final Hadamard gate on the qubits thus gives us

$$|\psi_3\rangle = \begin{cases} \pm\frac{|1\rangle|0\rangle \pm |0\rangle|1\rangle}{\sqrt{2}} & \text{if} \quad f(0) = f(1) \quad \text{entanglement} \\ \pm\frac{|1\rangle|0\rangle \pm |1\rangle|1\rangle}{\sqrt{2}} & \text{if} \quad f(0) \neq f(1) \quad \text{separable.} \end{cases} \tag{29}$$

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 bases

$$\begin{aligned} |\Psi_+\rangle &= \frac{|1\rangle|0\rangle + |0\rangle|1\rangle}{\sqrt{2}} \\ |\Psi_-\rangle &= \frac{|1\rangle|0\rangle - |0\rangle|1\rangle}{\sqrt{2}} \\ |\Phi_+\rangle &= \frac{|1\rangle|1\rangle + |0\rangle|0\rangle}{\sqrt{2}} \\ |\Phi_-\rangle &= \frac{|1\rangle|1\rangle - |0\rangle|0\rangle}{\sqrt{2}} \end{aligned} \tag{30}$$

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

$$|\langle\psi_3|\Psi_+\rangle|^2 = 1 \ \text{ or } \ |\langle\psi_3|\Psi_-\rangle|^2 = 1 \ \text{ or } \ |\langle\psi_3|\Phi_+\rangle|^2 = 1 \ \text{ or } \ |\langle\psi_3|\Phi_-\rangle|^2 = 1. \tag{31}$$

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

$$|\langle\psi_3|\Psi_+\rangle|^2 = 1/2 \ \text{ or } \ |\langle\psi_3|\Psi_-\rangle|^2 = 1/2 \ \text{ or } \ |\langle\psi_3|\Phi_+\rangle|^2 = 1/2 \ \text{ or } \ |\langle\psi_3|\Phi_-\rangle|^2 = 1/2. \tag{32}$$

Therefore the measurement outcome should be 1/2 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.

- 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 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 all the results of the Bell measurements when the function is constant; all of them should be 1.
- Eve is detected in the following case; the result of the Bell measurement is not 1 and the function is constant.

VI. THE BERNSTEIN-VAZIRANI ALGORITHM

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

$$f : \{0,1\}^N \rightarrow \{0,1\} \tag{33}$$

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

$$\begin{aligned} f(x) &= a \cdot x = \sum_{i=1}^{N} a_i x_i (\mathrm{mod} 2) \\ &= a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus \cdots \oplus a_N x_N, \\ & a \in \{0,1\}^N \end{aligned} \tag{34}$$

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

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \tag{35}$$

After the Hadamard transformation on the state we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{36}$$

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

$$U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle, \tag{37}$$

giving

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{38}$$

Here

$$y \oplus f(x) \tag{39}$$

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

$$|x\rangle. \tag{40}$$

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

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}. \tag{41}$$

Thus

$$\begin{aligned} & H^{\otimes N}|x_1, \ldots, x_N\rangle \\ &= \frac{\sum_{z_1,\ldots,z_N} (-1)^{x_1 z_1 + \cdots + x_N z_N} |z_1, \ldots, z_N\rangle}{\sqrt{2^N}}. \end{aligned} \tag{42}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}}, \tag{43}$$

where

$$x \cdot z \tag{44}$$

is the bitwise inner product of x and z, modulo 2. Using this equation and (38) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{45}$$

Thus,

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

We notice

$$\sum_x (-1)^{x\cdot z + a\cdot x} = 2^N \delta_{a,z}. \tag{47}$$

Thus,

$$\begin{aligned}|\psi_3\rangle &= \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + a\cdot x}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \pm \sum_z \frac{2^N \delta_{a,z}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \pm |a\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \pm |a_1 a_2 a_3 \cdots a_N\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \end{aligned} \tag{48}$$

Alice now observes

$$|a_1 a_2 a_3 \cdots a_N\rangle \tag{49}$$

Summarizing, if Alice measures $|a_1 a_2 a_3 \cdots a_N\rangle$ the function is

$$\begin{aligned}&f(x_1, x_2, ..., x_N) \\ &= a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus \cdots \oplus a_N x_N. \end{aligned} \tag{50}$$

VII. QUANTUM COMMUNICATION UTILISING THE BERNSTEIN-VAZIRANI ALGORITHM

We describe quantum communication utilising the Bernstein-Vazirani algorithm.

- First Alice prepares the qubits in (36) and sends the $N+1$ qubits to Bob.
- Next, Bob picks a function "f" and Bob applies U_f Eq. (37) evolving the $N+1$ qubits to Eq. (38). He then sends the N qubit to Alice.
- Finally, Alice applies the Hadamard transformation to each of the qubits and measures. She learns $f(x) = a \cdot x = \sum_{i=1}^{N} a_i x_i (\text{mod}2) = a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus \cdots \oplus a_N x_N$ - Alice and Bob now share N bits of information (the "type" of $f(x)$).

VIII. CONCLUSIONS

In conclusion, we have presented quantum key distribution based on Deutsch's algorithm 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 has been secret. Alice's and Bob's goal has been to determine with certainty whether they have chosen a constant or a balanced function without information of the function to Eve. If the function has been constant the output qubits are entangled, otherwise separable. Alice and Bob have performed the Bell measurement. Alice and Bob have shared one secret bit if they determine the function f by getting a suitable measurement outcome. Next, we have discussed quantum communication utilising the Bernstein-Vazirani algorithm. First, 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 have known $a_1, a_2, ..., a_N$. Bob has known $a_1, a_2, ..., a_N$. Alice's goal has been to determine with certainty what function Bob has chosen. In classical theory, Alice has to have asked Bob N questions. In quantum theory, Alice has to have asked Bob one question. Alice has prepared suitable $N + 1$ partite uncorrelated state, has performed the Hadamard transformation to the state, and has sent the output state to Bob. And Bob has performed the Bernstein-Vazirani algorithm and has input the information of the function into the finall state. Alice has asked him what state is. Alice has measured the finall state and she has known the function. If the function has been determined, Alice and Bob share N bits of information, by one communication with each other. The speed to share N bits has improved by a factor of N by comparing the classical case. This has shown quantum communication overcomes classical communication by a factor of N.

On safety, a questionable point has been left in various ways, but this has been a future problem.

[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] D. Deutsch, *Proc. Roy. Soc. London Ser. A* **400**, 97 (1985).

[12] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).

[13] 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).

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

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

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

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

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

[19] 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).

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