The Deutsch-Jozsa algorithm can be used for quantum key distribution

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: July 26, 2015)

We review the new type of Deutsch-Jozsa algorithm proposed in [K. Nagata and T. Nakamura, Int. J. Theor. Phys. **49**, 162 (2010)]. We suggest that the Deutsch-Jozsa algorithm can be used for quantum key distribution. Alice sends input $N+1$ partite uncorrelated state to a black box. Bob measures output state. Now, Alice and Bob has 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. Alice and Bob get one bit if they determine the function f. The speed to get one bit improves by a factor of 2^N. This may improve the speed to establish quantum key distribution by a factor of 2^N.

PACS numbers: 03.67.-a, 03.67.Lx, 03.67.Dd

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].

The most well known and developed application of quantum cryptography is quantum key distribution (QKD), 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.

To date, the relation between quantum computer and QKD is not reported. 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 von Neumann's theory does not meet the Deutsch-Jozsa algorithm [18]. In von Neumann's theory, control of quantum state and observations of quantum state cannot be existential, simultaneously. In reference [18], we propose a solution of the problem. The problem is solved if measurement outcome is $\pm 1/\sqrt{2}$.

In this paper, we review the Deutsch-Jozsa algorithm. We suggest that the Deutsch-Jozsa algorithm can be used for improve quantum key distribution. Alice sends input $N+1$ partite uncorrelated state to a black box. Bob measures output state. Now, Alice and Bob has 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. Alice and Bob get one bit if they determine the function f. The speed to get one bit improves by a factor of 2^N. This may improve the speed to establish quantum key distribution by a factor of 2^N.

II. THE DEUTSCH-JOZSA ALGORITHM CAN BE USED FOR QUANTUM KEY DISTRIBUTION

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.

Let us follow the argumentation presented in [6]. — — The application, known as *Deutsch's problem*, may be described as the following game. Alice, in Amsterdam, selects a number x from 0 to $2^N - 1$, and mails it in a letter to Bob, in Boston. Bob calculates the value of some function

$$f : \{0, \ldots, 2^N - 1\} \to \{0, 1\} \tag{1}$$

and replies with the result, which is either 0 or 1. Now, Bob has promised to use a function f which is of one of two kinds; either the value of $f(x)$ is constant for all values of x, or else the value of $f(x)$ is balanced, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half. Alice's goal is to determine with certainty whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible. How fast can she succeed?

In the classical case, Alice may only send Bob one value of x in each letter. At worst, Alice will need to query Bob at least

$$2^N/2 + 1 \tag{2}$$

times, since she may receive $2^N/2$ 0s before finally getting a 1, telling her that Bob's function is balanced. The best deterministic classical algorithm she can use therefore requires $2^N/2 + 1$ queries. Note that in each letter, Alice sends Bob N bits of information. Furthermore, in this example, physical distance is being used to artificially elevate the cost of calculating $f(x)$, but this is not needed in the general problem, where $f(x)$ may be inherently difficult to calculate.

If Bob and Alice were able to exchange qubits, instead of just classical bits, and if Bob agreed to calculate $f(x)$ using a unitary transformation U_f, then Alice could achieve her goal in just one correspondence with Bob, using the following algorithm.

Alice has an N qubit register to store her query in, and a single qubit register which she will give to Bob, to store the answer in. She begins by preparing both her query and answer registers in a superposition state. Bob will evaluate $f(x)$ using quantum parallelism and leave the result in the answer register. Alice then interferes states in the superposition using a Hadamard transformation (a unitary transformation),

$$H = (\sigma_x + \sigma_z)/\sqrt{2}, \tag{3}$$

on the query register, and finishes by performing a suitable measurement to determine whether f was constant or balanced.

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

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \tag{4}$$

Here the query register describes the state of N qubits all prepared in the

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

state. After the Hadamard transformation on the query register and the Hadamard gate on the answer register we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{6}$$

The query register is now a superposition of all values, and the answer register is in an evenly weighted superposition of

$$|0\rangle \tag{7}$$

and

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

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

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle, \tag{9}$$

giving

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{10}$$

Here

$$y \oplus f(x) \tag{11}$$

is the bitwise XOR (exclusive OR) of y and $f(x)$. Alice now has a set of qubits in which the result of Bob's function evaluation is stored in the amplitude of the qubit superposition state. She now interferes terms in the superposition using a Hadamard transformation on the query register. To determine the result of the Hadamard transformation it helps to first calculate the effect of the Hadamard transformation on a state

$$|x\rangle. \tag{12}$$

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

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}. \tag{13}$$

Thus

$$H^{\otimes N}|x_1,\ldots,x_N\rangle = \frac{\sum_{z_1,\ldots,z_N}(-1)^{x_1z_1+\cdots+x_Nz_N}|z_1,\ldots,z_N\rangle}{\sqrt{2^N}}. \quad (14)$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z(-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}}, \quad (15)$$

where

$$x \cdot z \quad (16)$$

is the bitwise inner product of x and z, modulo 2. Using this equation and (10) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{\sqrt{2^N}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \quad (17)$$

Alice now observes the query register. Note that the absolute value of the amplitude for the state

$$|0\rangle^{\otimes N} \quad (18)$$

is

$$\sum_x(-1)^{f(x)}/2^N. \quad (19)$$

Let's look at the two possible cases — f constant and f balanced — to discern what happens. In the case where f is constant the absolute value of the amplitude for

$$|0\rangle^{\otimes N} \quad (20)$$

is $+1$. Because

$$|\psi_3\rangle \quad (21)$$

is of unit length it follows that all the other amplitudes must be zero, and an observation will yield

$$+1/\sqrt{2} \quad (22)$$

times for all N qubits in the query register. Thus, global measurement outcome is

$$+1/\sqrt{2^N}. \quad (23)$$

If f is balanced then the positive and negative contributions to the absolute value of the amplitude for

$$|0\rangle^{\otimes N} \quad (24)$$

cancel, leaving an amplitude of zero, and a measurement must yield a result other than

$$+1/\sqrt{2}, \quad (25)$$

that is,

$$-1/\sqrt{2}, \quad (26)$$

on at least one qubit in the query register. Summarizing, if Alice measures all $+1/\sqrt{2}$s and global measurement outcome is $+1/\sqrt{2^N}$ the function is constant; otherwise the function is balanced.

We suggest that the Deutsch-Jozsa algorithm can be used for quantum key distribution.

- First Alice prepares the qubits in (6) and sends the $N+1$ qubits to Bob.
- Next, Bob picks a random function "f" that is either balanced or constant and Bob applies U_f Eq. (9) evolving the $N+1$ qubits to Eq. (10). He then sends the N qubit Query register to Alice.
- Finally, Alice applies the Hadamard transformation to each of the qubits and measures. She learns whether f was balanced or constant - Alice and Bob now share a random bit of information (the "type" of $f(x)$).

On safety, a questionable point is left in various ways, but this is a future problem. For example, we can consider the following situation:

Alice has to send the Query (N-qubit) and Answer (1-qubit) registers to Bob. Bob will then apply U_f and send the Query register back to Alice who will apply the second step of the Deutsch-Jozsa algorithm to this register and learn the "type" of $f(x)$. What's to prevent the attacker Eve from doing this same thing? That is, Eve will capture the N qubits from Bob, apply $H^{\otimes N}$ to the query qubits, and measure. She now learns the type of $f(x)$ and thus the key bit. She can then prepare fresh qubits of the form:

$H^{\otimes N}|00\ldots0\rangle$ if her measurement result was all zeros (f is constant) $H^{\otimes N}|$ random qubits not all zero$\rangle$ otherwise (f is balanced)

Alice will then apply $H^{\otimes N}$ (the second part of the Deutsch-Jozsa algorithm) unaware that Eve interfered. Her action will cancel out Eve's operation and Alice will then measure either all zeros if f is constant or some random non-zero state otherwise. This seems like an undetectable attack. We will need to find a way to counter this in our protocol somehow.

III. CONCLUSIONS

In conclusion, we have reviewed the new type of Deutsch-Jozsa algorithm. We have suggested that the Deutsch-Jozsa algorithm can be used for quantum key distribution. Alice has sent input $N+1$ partite uncorrelated state to a black box. Bob has measured output state. Now, Alice and Bob has 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. Alice and Bob have gotten one bit if they determine the function f. The speed to get one bit has improved by a factor of 2^N. This may have improved the speed to establish quantum key distribution by a factor of 2^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, Int. J. Theor. Phys. **49**, 162 (2010).