Generalization of 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: August 7, 2016)

We present generalization of the Bernstein-Vazirani algorithm. Suppose there are many natural numbers: $a_1, a_2, a_3, \ldots, a_N$. Here, we introduce a function: $g : \mathbf{N} \rightarrow \{0, 1\}$. Our goal is to determine the following values simultaneously: $g(a_1), g(a_2), g(a_3), \ldots, g(a_N)$. The speed to determine N values improves by a factor of N by comparing the classical case. We obtain the Bernstein-Vazirani algorithm when $g : a_i \rightarrow a_i$.

PACS numbers: 03.67.-a(Quantum information theory), 03.67.Lx(Quantum computer), 03.65.Ca(Formalism)

I. INTRODUCTION

The quantum theory (cf. [1–6]) gives approximate but frequently remarkably accurate numerical predictions. Much experimental data approximately have 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, the implementation of a quantum algorithm to solve Deutsch's problem [14] on a nuclear magnetic resonance quantum computer is reported first [15]. The 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]. In addition, the decoherence-free implementation of Deutsch's algorithm is reported using such single photon and 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, 22]. It can be considered as an extended Deutsch-Jozsa algorithm. In 1994, Simon's algorithm was reported [23]. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement on an ensemble quantum computer is reported [24]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits is discussed [25]. A quantum algorithm for approximating the influences of Boolean functions and its applications is recently reported [26]

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]. As we have said, the Bernstein-Vazirani algorithm can be considered as an extended Deutsch-Jozsa algorithm. Here, we extend the Bernstein-Vazirani algorithm more.

In this paper, we present generalization of the Bernstein-Vazirani algorithm. Suppose there are many natural numbers: $a_1, a_2, a_3, \ldots, a_N$. Here, we introduce a function: $g : \mathbf{N} \rightarrow \{0, 1\}$. Our goal is to determine the following values simultaneously: $g(a_1), g(a_2), g(a_3), \ldots, g(a_N)$. The speed to determine N values improves by a factor of N by comparing the classical case. We obtain the Bernstein-Vazirani algorithm when $g : a_i \rightarrow a_i$.

II. GENERALIZATION OF THE BERNSTEIN-VAZIRANI ALGORITHM

In this section, we present generalization of the Bernstein-Vazirani algorithm. Suppose a sequence of natural numbers as follows:

$$a_1, a_2, a_3, \ldots, a_N. \tag{1}$$

We introduce a function:

$$g : \mathbf{N} \rightarrow \{0, 1\}. \tag{2}$$

Our goal is to determine the following values:

$$g(a_1), g(a_2), g(a_3), \ldots, g(a_N). \tag{3}$$

In classical case, we need N queries. In quantum algorithm, we need a query. Our algorithm is indeed faster than classical counterpart.

We introduce another function: Suppose

$$f: \{0,1\}^N \rightarrow \{0,1\} \tag{4}$$

is a function with a N-bit domain and a 1-bit range. We construct the following function:

$$\begin{aligned} f(x) &= g(a) \cdot x = \sum_{i=1}^{N} g(a_i) x_i (\mathrm{mod} 2) \\ &= g(a_1)x_1 \oplus g(a_2)x_2 \oplus g(a_3)x_3 \oplus \cdots \oplus g(a_N)x_N, \\ & x_i \in \{0,1\}^N, g(a_i) \in \{0,1\}, a_i \in \mathbf{N} \end{aligned} \tag{5}$$

where a_i is a natural number. Here $g(a)$ means

$$g(a_1)g(a_2)\cdots g(a_N). \tag{6}$$

In what follows, we show that we can know the following values only by a query

$$g(a_1), g(a_2), g(a_3), \ldots, g(a_N). \tag{7}$$

In classical case, we need N queries. Let us follow the quantum states through the algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \tag{8}$$

After the Hadamard transformation on the state we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{9}$$

Next, the function f is evaluated using

$$U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle, \tag{10}$$

giving

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{11}$$

Here

$$y \oplus f(x) \tag{12}$$

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

$$|x\rangle. \tag{13}$$

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

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}. \tag{14}$$

Thus

$$\begin{aligned} & H^{\otimes N}|x_1, \ldots, x_N\rangle \\ &= \frac{\sum_{z_1,\ldots,z_N} (-1)^{x_1 z_1 + \cdots + x_N z_N}|z_1, \ldots, z_N\rangle}{\sqrt{2^N}}. \end{aligned} \tag{15}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}}, \tag{16}$$

where

$$x \cdot z \tag{17}$$

is the bitwise inner product of x and z, modulo 2. Using this equation and (11) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{18}$$

Thus,

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + g(a)\cdot x}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{19}$$

We notice

$$\sum_x (-1)^{x\cdot z + g(a)\cdot x} = 2^N \delta_{g(a),z}. \tag{20}$$

Thus,

$$\begin{aligned} |\psi_3\rangle &= \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + g(a)\cdot x}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \pm \sum_z \frac{2^N \delta_{g(a),z}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \pm |g(a)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\ &= \pm |g(a_1)g(a_2)\cdots g(a_N)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \end{aligned} \tag{21}$$

We now observe

$$|g(a_1)g(a_2)\cdots g(a_N)\rangle. \tag{22}$$

Summarizing, if we measures $|g(a_1)g(a_2)\cdots g(a_N)\rangle$ then we can know the following values only by a query

$$g(a_1), g(a_2), g(a_3), \ldots, g(a_N). \tag{23}$$

All we have to do is to perform one quantum measurement.

The speed to determine N values improves by a factor of N by comparing the classical case. This shows quantum computer overcomes classical computer by a factor of N in this case. We obtain the Bernstein-Vazirani algorithm when $g : a_i \rightarrow a_i$.

III. CONCLUSIONS

In conclusion, we have presented generalization of the Bernstein-Vazirani algorithm. We have supposed there are many natural numbers: $a_1, a_2, a_3, \ldots, a_N$. Here, we have introduced a function: $g : \mathbf{N} \rightarrow \{0,1\}$. Our goal has been to determine the following values simultaneously: $g(a_1), g(a_2), g(a_3), \ldots, g(a_N)$. The speed to determine N values has improved by a factor of N by comparing the classical case. We have obtained the Bernstein-Vazirani algorithm when $g : a_i \rightarrow a_i$.

[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.

[22] E. Bernstein and U. Vazirani, SIAM J. Comput. 26-5, pp. 1411-1473 (1997).

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

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

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

[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.