A new quantum algorithm without the Hadamard transformation in case of a special function

Koji Nagata,[1] Tadao Nakamura,[2] and Ahmed Farouk[3, 4, 5]

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon, 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, Japan*

[3] *Computer Sciences Department, Faculty of Computers and Information, Mansoura University*

[4] *University of Science and Technology, Zewail City of Science and Technology, Giza, Egypt*

[5] *Scientific Research Group, Egypt*

(Dated: March 31, 2017)

We present a new quantum algorithm. It determines a property of a function. It is either $f(x) = f(-x)$ or $f(x) \neq f(-x)$. The quantum algorithm does not use the Hadamard transformation. Our quantum algorithm overcomes a classical counterpart by a factor of $O(2^N)$.

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

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 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 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, 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]. Quantum computation with coherent spin states and the close Hadamard problem is also discussed [27].

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 [28]. In 2017, it is discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [29].

In this paper, we newly propose a new quantum algorithm. It determines a property of a function. It is either $f(x) = f(-x)$ or $f(x) \neq f(-x)$. The quantum algorithm does not use the Hadamard transformation. Our quantum algorithm overcomes a classical counterpart by a factor of $O(2^N)$.

II. QUANTUM COMPUTING DETERMINING A PROPERTY OF A FUNCTION

Suppose

$$\begin{aligned} f &: \{-(2^N-1), -(2^N-2), .., 2^N-2, 2^N-1\} \\ &\to \{-(2^N-1), -(2^N-2), .., 2^N-2, 2^N-1\}. \end{aligned} \quad (1)$$

is a function. The goal is of determining either $f(-x) = f(x)$ or $f(-x) \neq f(x)$. We assume the following case

$$\begin{aligned} & f(x) = f(-x), \\ & x \in \{0,1\}^N. \end{aligned} \quad (2)$$

Our algorithm combines quantum parallelism with a property of quantum mechanics known as interference.

Let us follow the quantum states through the algorithm. Throughout the paper, we omit the normalization factor. The input state is

$$|\psi_1\rangle = \sum_{-(2^N-1)}^{2^N-1} |x\rangle|0,0,...,0\rangle. \tag{3}$$

Next, the function f is evaluated using

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

and

$$\begin{aligned} U_f : \quad & |x,y\rangle \rightarrow |x, y \oplus f(x)\rangle \\ & \Leftrightarrow -|x,y\rangle \rightarrow -|x, y \oplus f(x)\rangle \\ & \Leftrightarrow |-x,y\rangle \rightarrow |-x, y \oplus f(x)\rangle \\ & \Leftrightarrow |-x,y\rangle \rightarrow |-x, y \oplus f(-x)\rangle, \end{aligned} \tag{5}$$

by using $f(x) = f(-x)$. Thus, we have

$$|\psi_2\rangle = \sum_{-(2^N-1)}^{2^N-1} |x\rangle|f(x)\rangle. \tag{6}$$

Hence we have

$$\begin{aligned} |\psi_2\rangle &= \sum_{-(2^N-1)}^{2^N-1} |x\rangle|f(x)\rangle \\ &= \sum_{-(2^N-1)}^{0} |x\rangle|f(x)\rangle + \sum_{0}^{2^N-1} |x\rangle|f(x)\rangle \\ &\quad -|0,0,...,0\rangle|f(0,0,...,0)\rangle \\ &= \sum_{0}^{2^N-1} |-x\rangle|f(-x)\rangle + \sum_{0}^{2^N-1} |x\rangle|f(x)\rangle \\ &\quad -|0,0,...,0\rangle|f(0,0,...,0)\rangle \\ &= \sum_{0}^{2^N-1} |-x\rangle|f(x)\rangle + \sum_{0}^{2^N-1} |x\rangle|f(x)\rangle \\ &\quad -|0,0,...,0\rangle|f(0,0,...,0)\rangle \\ &= +|0,0,...,0\rangle|f(0,0,...,0)\rangle, \end{aligned} \tag{7}$$

by using $f(x) = f(-x)$.

Finally, we measure $|\psi_2\rangle$. If all the results of measurements are zero, (that is, we measure $|0,0,...,0\rangle$) we can determine the property of the function

$$f(x) = f(-x). \tag{8}$$

Otherwise, (for example, one of the results of measurements is $+1$) the function is $f(x) \neq f(-x)$. The quantum algorithm does not use the Hadamard transformation. Our quantum algorithm overcomes a classical counterpart by a factor of $O(2^N)$.

III. CONCLUSIONS

In conclusion, we have presented a new quantum algorithm. It has determined a property of a function. It has been either $f(x) = f(-x)$ or $f(x) \neq f(-x)$. The quantum algorithm does not have used the Hadamard transformation. Our quantum algorithm has overcome a classical counterpart by a factor of $O(2^N)$.

[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] M. R. A. Adcock, P. Hoyer, and B. C. Sanders, Quantum Inf. Process. **15**, 1361 (2016).

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

[29] K. Nagata and T. Nakamura, “Quantum Cryptography, Quantum Communication, and Quantum Computer in a Noisy Environment”, International Journal of Theoretical Physics (accepted),
DOI: 10.1007/s10773-017-3352-4.