Int J Theor Phys (2018) 57:1605–1611
https://doi.org/10.1007/s10773-018-3687-5

CrossMark

New Method of Calculating a Multiplication by using the Generalized Bernstein-Vazirani Algorithm

Koji Nagata[1] · **Tadao Nakamura**[2] · **Han Geurdes**[3] · **Josep Batle**[4] · **Soliman Abdalla**[5] · **Ahmed Farouk**[6]

Received: 29 September 2017 / Accepted: 2 February 2018 / Published online: 12 February 2018

Abstract We present a new method of more speedily calculating a multiplication by using the generalized Bernstein-Vazirani algorithm and many parallel quantum systems. Given the set of real values $\{a_1, a_2, a_3, \ldots, a_N\}$ and a function $g : \mathbf{R} \to \{0, 1\}$, we shall determine the following values $\{g(a_1), g(a_2), g(a_3), \ldots, g(a_N)\}$ simultaneously. The speed of determining the values is shown to outperform the classical case by a factor of N. Next, we consider it as a number in binary representation; $M_1 = (g(a_1), g(a_2), g(a_3), \ldots, g(a_N))$. By using M parallel quantum systems, we have M numbers in binary representation, simultaneously. The speed of obtaining the M numbers is shown to outperform the classical case by a factor of M. Finally, we calculate the product; $M_1 \times M_2 \times \cdots \times M_M$. The speed of obtaining the product is shown to outperform the classical case by a factor of $N \times M$.

Keywords Quantum computation · Quantum algorithms

✉ Koji Nagata
ko_mi_na@yahoo.co.jp

1 Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea

2 Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan

3 Geurdes Datascience, KvK 64522202, C vd Lijnstraat 164, 2593 NN, Den Haag, Netherlands

4 Departament de Física, Universitat de les Illes Balears, 07122 Palma de Mallorca, Balearic Islands, Spain

5 Faculty of Science, Department of Physics, King Abdulaziz University Jeddah, P.O. Box 80203, Jeddah 21589, Saudi Arabia

6 Faculty of Computers and Information, Computer Sciences Department, Mansoura University, Mansoura, Egypt

1 Introduction

As for applications of the quantum theory, implementation of a quantum algorithm to solve Deutsch's problem [1–3] on a nuclear magnetic resonance quantum computer is reported firstly [4]. An implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is also reported [5]. There are several attempts to use single-photon two-qubit states for quantum computing. Oliveira *et al.* implements Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [6]. Single-photon Bell states are prepared and measured [7]. Also the decoherence-free implementation of Deutsch's algorithm is reported by using such a single-photon and by using two logical qubits [8]. More recently, a one-way based experimental implementation of Deutsch's algorithm is reported [9].

In 1993, the Bernstein-Vazirani algorithm was reported [10, 11]. It can be considered as an extended Deutsch-Jozsa algorithm. In 1994, Simon's algorithm was reported [12]. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement on an ensemble quantum computer is reported [13]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits is discussed [14]. Quantum learning robust against noise is studied [15]. A quantum algorithm for approximating the influences of Boolean functions and its applications are recently reported [16]. Quantum computation with coherent spin states and the close Hadamard problem are also discussed [17]. Transport implementation of the Bernstein-Vazirani algorithm with ion qubits is more recently reported [18]. Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers are discussed [19]. We mention that the dynamical analysis of Grover's search algorithm in arbitrarily high-dimensional search spaces is studied [20]. A method of computing many functions simultaneously by using many parallel quantum systems is reported [21].

On the other hand, the earliest quantum algorithm, the Deutsch-Jozsa algorithm, is representative to show that quantum computation is faster than the classical counterpart with a magnitude that grows exponentially with the number of qubits. In 2015, it was discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [22]. In 2017, it was discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [23]. Subsequently, a highly speedy secure quantum cryptography based on the Deutsch-Jozsa algorithm is proposed [24].

In this work we present a new method of more speedily calculating a multiplication by using the generalized Bernstein-Vazirani algorithm and many parallel quantum systems. Given the set of real values $\{a_1, a_2, a_3, \ldots, a_N\}$ and a function $g : \mathbf{R} \to \{0, 1\}$, we shall determine the following values $\{g(a_1), g(a_2), g(a_3), \ldots, g(a_N)\}$ simultaneously. The speed of determining the values is shown to outperform the classical case by a factor of N. Next, we consider it as a number in binary representation; $M_1 = (g(a_1), g(a_2), g(a_3), \ldots, g(a_N))$. By using M parallel quantum systems, we have M numbers in binary representation, simultaneously. The speed of obtaining the M numbers is shown to outperform the classical case by a factor of M. Finally, we calculate the product; $M_1 \times M_2 \times \cdots \times M_M$. The speed of obtaining the product is shown to outperform the classical case by a factor of $N \times M$.

2 The Generalized Bernstein-Vazirani Algorithm

Let us suppose that we are given the following sequence of real values

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

Let us now introduce the function

$$g : \mathbf{R} \to \{0, 1\}. \tag{2}$$

One step is of determining the following values

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

Recall that in the classical case, we need N queries, that is, N separate evaluations of the function (2). In our quantum algorithm, we shall require a single query. Suppose now that we introduce another function

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

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

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

where a_i is a real value. Here $g(a)$ symbolizes

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

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

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle \tag{7}$$

where $|0\rangle^{\otimes N} = \overbrace{|0\rangle \otimes |0\rangle \otimes ... \otimes |0\rangle}^{N}$. After the componentwise Hadamard transforms on the state (7)

$$\overbrace{H|0\rangle \otimes H|0\rangle \otimes ... \otimes H|0\rangle}^{N} \otimes H|1\rangle \tag{8}$$

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

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

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 $y \oplus f(x)$ is the bitwise XOR (exclusive OR) of y and $f(x)$. By checking the cases $x = 0$ and $x = 1$ separately, we see that for a single qubit

$$H|x\rangle = \sum_{z}(-1)^{xz}|z\rangle/\sqrt{2}. \tag{12}$$

Thus

$$H^{\otimes N}|x_1, \ldots, x_N\rangle = \frac{\sum_{z_1,\ldots,z_N}(-1)^{x_1z_1+\cdots+x_Nz_N}|z_1, \ldots, z_N\rangle}{\sqrt{2^N}}. \tag{13}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z(-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}} \tag{14}$$

where $x \cdot z$ is the bitwise inner product of x and z, modulo 2. Using the (14) and (11), we can now evaluate $H^{\otimes N}|\psi_2\rangle = |\psi_3\rangle$

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{15}$$

Thus

$$|\psi_3\rangle = \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+g(a)\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{16}$$

Because we have

$$\sum_x(-1)^x = 0 \tag{17}$$

we can see that

$$\sum_x(-1)^{x\cdot z+g(a)\cdot x} = 2^N\delta_{g(a),z}. \tag{18}$$

Therefore, the sum is zero if $z \neq g(a)$ and is 2^N if $z = g(a)$. Thus

$$\begin{aligned}|\psi_3\rangle &= \pm\sum_z\sum_x \frac{(-1)^{x\cdot z+g(a)\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\\ &= \pm\sum_z \frac{2^N\delta_{g(a),z}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\\ &= \pm|g(a)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\\ &= \pm|g(a_1)g(a_2)\cdots g(a_N)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\end{aligned} \tag{19}$$

from which

$$|g(a_1)g(a_2)\cdots g(a_N)\rangle. \tag{20}$$

can be obtained. That is to say, if we measure $|g(a_1)g(a_2)\cdots g(a_N)\rangle$ then we can retrieve the following values

$$g(a_1), g(a_2), g(a_3), \ldots, g(a_N) \tag{21}$$

using a single query. All we have to do is of performing one quantum measurement.

The speed of determining N values improves by a factor of N as compared to the classical counterpart. Notice that we recover the Bernstein-Vazirani algorithm when $g : a_i \rightarrow a_i$.

3 Calculating a Multiplication by using the Generalized Bernstein-Vazirani Algorithm

We present a new method of more speedy calculating a multiplication by using many parallel quantum systems. By using M parallel quantum systems, we can compute M functions $g^1, g^2, ..., g^M$ simultaneously.

Let us suppose that we are given the following another sequence of real values

$$b_1, b_2, b_3, \ldots, b_N. \tag{22}$$

Let us now introduce the function

$$g^2 : \mathbf{R} \to \{0, 1\}. \tag{23}$$

We can determine the following values by using the generalized Bernstein-Vazirani algorithm

$$g^2(b_1), g^2(b_2), g^2(b_3), \ldots, g^2(b_N). \tag{24}$$

By using M parallel quantum systems, we can retrieve the following values

$$\begin{aligned} &g^1(a_1), g^1(a_2), g^1(a_3), \ldots, g^1(a_N) \\ &g^2(b_1), g^2(b_2), g^2(b_3), \ldots, g^2(b_N) \\ &\ldots \\ &g^M(c_1), g^M(c_2), g^M(c_3), \ldots, g^M(c_N). \end{aligned} \tag{25}$$

In the case, we measure the following quantum state

$$\begin{aligned} &|g^1(a_1)g^1(a_2)\cdots g^1(a_N)\rangle \otimes \\ &|g^2(b_1)g^2(b_2)\cdots g^2(b_N)\rangle \otimes \\ \cdots \otimes &|g^M(c_1)g^M(c_2)\cdots g^M(c_N)\rangle. \end{aligned} \tag{26}$$

All we have to do is of performing one quantum measurement.

We consider them as numbers in binary representation

$$\begin{aligned} &M_1 = (g^1(a_1), g^1(a_2), g^1(a_3), \ldots, g^1(a_N)) \\ &M_2 = (g^2(b_1), g^2(b_2), g^2(b_3), \ldots, g^2(b_N)) \\ &\ldots \\ &M_M = (g^M(c_1), g^M(c_2), g^M(c_3), \ldots, g^M(c_N)). \end{aligned} \tag{27}$$

Therefore, by using M parallel quantum systems, we have M numbers in binary representation, simultaneously. The speed of obtaining the M numbers is shown to outperform the classical case by a factor of M. Finally, we calculate the product; $M_1 \times M_2 \times \cdots \times M_M$. The speed of obtaining the product is shown to outperform the classical case by a factor of $N \times M$.

As an example, if $N = 2$ and $M = 3$, we may have

$$(g^1(a_1), g^1(a_2)) = (0, 1) = 1 \tag{28}$$

$$(g^2(b_1), g^2(b_2)) = (1, 0) = 2 \tag{29}$$

$$(g^3(c_1), g^3(c_2)) = (1, 1) = 3 \tag{30}$$

and we have

$$(g^1(a_1), g^1(a_2)) \times (g^2(b_1), g^2(b_2))$$
$$\times (g^3(c_1), g^3(c_2)) = 1 \times 2 \times 3 = 6. \quad (31)$$

An experimental evidence is very interesting and it is a further investigation.

4 Conclusions

In conclusion, we have presented a new method of more speedily calculating a multiplication by using the generalized Bernstein-Vazirani algorithm and many parallel quantum systems. Given the set of real values $\{a_1, a_2, a_3, \ldots, a_N\}$ and a function $g : \mathbf{R} \rightarrow \{0, 1\}$, we shall have determined the following values $\{g(a_1), g(a_2), g(a_3), \ldots, g(a_N)\}$ simultaneously. The speed of determining the values has been shown to outperform the classical case by a factor of N. Next, we have considered it as a number in binary representation; $M_1 = (g(a_1), g(a_2), g(a_3), \ldots, g(a_N))$. By using M parallel quantum systems, we have had M numbers in binary representation, simultaneously. The speed of obtaining the M numbers has been shown to outperform the classical case by a factor of M. Finally, we have calculated the product; $M_1 \times M_2 \times \cdots \times M_M$. The speed of obtaining the product has been shown to outperform the classical case by a factor of $N \times M$.

Acknowledgements All authors are grateful to the anonymous referees who provided a great insight into the completion of the final manuscript.

References

1. Deutsch, D.: Proc. Roy. Soc. London Ser. A **400**, 97 (1985)
2. Deutsch, D., Jozsa, R.: Proc. Roy. Soc. London Ser. A **439**, 553 (1992)
3. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Proc. Roy. Soc. London Ser. A **454**, 339 (1998)
4. Jones, J.A., Mosca, M.: J. Chem. Phys. **109**, 1648 (1998)
5. Gulde, S., Riebe, M., Lancaster, G.P.T., Becher, C., Eschner, J., Häffner, H., Schmidt-Kaler, F., Chuang, I.L., Blatt, R.: Nature (London) **421**, 48 (2003)
6. de Oliveira, A.N., Walborn, S.P., Monken, C.H.: J. Opt. B: Quantum Semiclass. Opt. **7**, 288–292 (2005)
7. Kim, Y.-H.: Phys. Rev. A **67**, 040301(R) (2003)
8. Mohseni, M., Lundeen, J.S., Resch, K.J., Steinberg, A.M.: Phys. Rev. Lett. **91**, 187903 (2003)
9. Tame, M.S., Prevedel, R., Paternostro, M., Böhi, P., Kim, M.S., Zeilinger, A.: Phys. Rev. Lett. **98**, 140501 (2007)
10. Bernstein, E., Vazirani, U.: In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC '93), pp. 11–20 (1993). https://doi.org/10.1145/167088.167097
11. Bernstein, E., Vazirani, U.: SIAM J. Comput. **26–5**, 1411–1473 (1997)
12. Simon, D.R.: Foundations of computer science. In: 35th Annual Symposium on Proceedings, pp. 116–123, retrieved 2011-06-06 (1994)
13. Du, J., Shi, M., Zhou, X., Fan, Y., Ye, B.J., Han, R., Wu, J.: Phys. Rev. A **64**, 042306 (2001)
14. Brainis, E., Lamoureux, L.-P., Cerf, N.J., Emplit, P.h., Haelterman, M., Massar, S.: Phys. Rev. Lett. **90**, 157902 (2003)
15. Cross, A.W., Smith, G., Smolin, J.A.: Phys. Rev. A **92**, 012327 (2015)
16. Li, H., Yang, L.: Quantum Inf. Process. **14**, 1787 (2015)
17. Adcock, M.R.A., Hoyer, P., Sanders, B.C.: Quantum Inf. Process. **15**, 1361 (2016)
18. Fallek, S.D., Herold, C.D., McMahon, B.J., Maller, K.M., Brown, K.R., Amini, J.M.: J. Phys. **18**, 083030 (2016)
19. Diep, D.N., Giang, D.H., Van Minh, N.: Int. J. Theor. Phys. **56**, 1948 (2017). https://doi.org/10.1007/s10773-017-3340-8
20. Jin, W.: Quantum Inf. Process. **15**, 65 (2016)

21. Nagata, K., Resconi, G., Nakamura, T., Batle, J., Abdalla, S., Farouk, A., Geurdes, H.: Asian J. Math. Phys. **1**(1), 1–4 (2017)
22. Nagata, K., Nakamura, T.: Open Access Library J. **2**, e1798 (2015). https://doi.org/10.4236/oalib.1101798
23. Nagata, K., Nakamura, T.: Int. J. Theor. Phys. **56**, 2086 (2017). https://doi.org/10.1007/s10773-017-3352-4
24. Nagata, K., Nakamura, T., Farouk, A.: Int. J. Theor. Phys. **56**, 2887 (2017). https://doi.org/10.1007/s10773-017-3456-x