The generalized Bernstein-Vazirani algorithm for determining an integer string

Koji Nagata,[1] Tadao Nakamura,[2] Han Geurdes,[3] Josep Batle,[4] Ahmed Farouk,[5] and Do Ngoc Diep[6]

[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, Europe*
[5]*Computer Sciences Department, Faculty of Computers and Information, Mansoura University, Egypt*
[6]*TIMAS, Thang Long University, Nghiem Xuan Yem, Dai Kim, Hoang Mai, Hanoi, Vietnam*

(Dated: March 8, 2018)

We present the generalized Bernstein-Vazirani algorithm for determining a restricted integer string. Given the set of real values $\{a_1, a_2, a_3, \ldots, a_N\}$ and a function $g : \mathbf{R} \to \mathbf{Z}$, 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. The method determines the maximum of and the minimum of the function g that the finite domain is $\{a_1, a_2, a_3, \ldots, a_N\}$.

PACS numbers: 03.67.Lx, 03.67.Ac
Keywords: Quantum computation, Quantum algorithms

I. INTRODUCTION

In 1993, the Bernstein-Vazirani algorithm was published [1, 2]. This work can be considered an extension of the Deutsch-Jozsa algorithm [3–5]. In 1994, Simon's algorithm [6] and Shor's algorithm [7] were discussed. In 1996, Grover [8] provided the highest motivation for exploring the computational possibilities offered by quantum mechanics.

The original Bernstein-Vazirani algorithm [1, 2] determines a bit string. It is extended to determining the values of a function [9, 10]. The values of the functions are restricted in $\{0, 1\}$. By using the extension, we can consider quantum algorithm of calculating a multiplication [10].

By extending the Bernstein-Vazirani algorithm more, we give an algorithm of determining the values of a function that are extended to the natural numbers $\mathbf{N}$ [11]. That is, the extended algorithm determines a natural number string instead of a bit string. So we have the generalized Bernstein-Vazirani algorithm for determining a restricted natural number string. By using the extension, quantum algorithm for determining a homogeneous linear function is studied.

Here, by extending the quantum algorithm more and more, we present an algorithm of determining the values of a function that are extended to the integers $\mathbf{Z}$. That is, the extended algorithm determines an integer string instead of a natural number string.

In this article, we present the generalized Bernstein-Vazirani algorithm for determining an integer string. Given the set of real values $\{a_1, a_2, a_3, \ldots, a_N\}$ and a function $g : \mathbf{R} \to \mathbf{Z}$, 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. The method determines the maximum of and the minimum of the function g that the finite domain is $\{a_1, a_2, a_3, \ldots, a_N\}$. Our argumentations provide a new insight into the importance of the original Bernstein-Vazirani algorithm.

II. THE QUANTUM ALGORITHM FOR DETERMINING THE MAXIMUM OF AND THE MINIMUM OF A FUNCTION

Let us suppose that the following sequence of real values is given

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

Let us now introduce a function

$$g : \mathbf{R} \to \mathbf{Z}. \tag{2}$$

Our goal is of determining the following values

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

We can determine the maximum of and the minimum of the function g that the finite domain is $\{a_1, a_2, a_3, \ldots, a_N\}$. 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.

We introduce a positive integer d. Throughout the discussion, we consider the problem in the modulo d. Assume the following

$$-(d-1) \le \overbrace{g(a_1), g(a_2), g(a_3), \ldots, g(a_N)}^{N} \le d-1 \tag{4}$$

where $g(a_j) \in \{-(d-1), ..., -1, 0, 1, ..., d-1\}$, and we define

$$g(a) = (g(a_1), g(a_2), g(a_3), \ldots, g(a_N)) \tag{5}$$

where each entry of $g(a)$ is an integer in the modulo d. Here $g(a) \in \{-(d-1), ..., -1, 0, 1, ..., d-1\}^N$. We define $f(x)$ as follows

$$\begin{aligned} f(x) &= g(a) \cdot x \bmod d \\ &= g(a_1)x_1 + g(a_2)x_2 + \cdots + g(a_N)x_N \bmod d \end{aligned} \tag{6}$$

where $x = (x_1, ..., x_N) \in \{-(d-1), ..., -1, 0, 1, ..., d-1\}^N$. Let us follow the quantum states through the algorithm.

The input state is

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

where $|0\rangle^{\otimes N}$ means $\overbrace{|0, 0, ..., 0\rangle}^{N}$. We discuss the general Fourier transform of $|0\rangle$

$$|0\rangle \rightarrow \sum_{y=-(d-1)}^{d-1} \frac{\omega^{y\cdot 0}|y\rangle}{\sqrt{2d-1}} = \sum_{y=-(d-1)}^{d-1} \frac{|y\rangle}{\sqrt{2d-1}} \tag{8}$$

where we have used $\omega^0 = 1$.

Subsequently let us define the wave function $|\phi\rangle$ as follows

$$|\phi\rangle = \frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle) \tag{9}$$

where $\omega = e^{2\pi i/d}$. In the following, we discuss the Fourier transform of $|d-1\rangle$

$$\begin{aligned} |d-1\rangle &\rightarrow \sum_{y=0}^{d-1} \frac{\omega^{y\cdot(d-1)}|y\rangle}{\sqrt{d}} = \sum_{y=0}^{d-1} \frac{\omega^{yd-y}|y\rangle}{\sqrt{d}} \\ &= \sum_{y=0}^{d-1} \frac{\omega^{d-y}|y\rangle}{\sqrt{d}} = |\phi\rangle \end{aligned} \tag{10}$$

where we have used $\omega^{yd} = \omega^d = 1$.

The general Fourier transform of $|x_1...x_N\rangle$ is as follows

$$\begin{aligned} &|x_1...x_N\rangle \\ &\rightarrow \sum_{z_1=-(d-1)}^{d-1} \cdots \sum_{z_N=-(d-1)}^{d-1} \frac{\omega^{z_1x_1}|z_1\rangle}{\sqrt{2d-1}} \cdots \frac{\omega^{z_Nx_N}|z_N\rangle}{\sqrt{2d-1}} \\ &= \sum_{z\in K} \frac{\omega^{z\cdot x}|z\rangle}{\sqrt{(2d-1)^N}} \end{aligned} \tag{11}$$

where $K = \{-(d-1), ..., -1, 0, 1, ..., d-1\}^N$ and z is $(z_1, z_2, ..., z_N)$. Hence, for completeness, $\sum_{z\in K}$ is a shorthand to the compound sum

$$\sum_{z_1\in\{-(d-1),...,-1,0,1,...,d-1\}} \cdots \sum_{z_N\in\{-(d-1),...,-1,0,1,...,d-1\}}. \tag{12}$$

After the componentwise general Fourier transforms of the first N qudits state and after the Fourier transform of $|d-1\rangle$ in (7)

$$\overbrace{G|0\rangle \otimes G|0\rangle \otimes ... \otimes G|0\rangle}^{N} \otimes F|d-1\rangle \tag{13}$$

we have

$$|\psi_1\rangle = \sum_{x\in K} \frac{|x\rangle}{\sqrt{(2d-1)^N}}|\phi\rangle. \tag{14}$$

Here, the notation $G|0\rangle$ means the general Fourier transform of $|0\rangle$ and the notation $F|d-1\rangle$ means the Fourier transform of $|d-1\rangle$.

We introduce $SUM_{f(x)}$ gate

$$|x\rangle|j\rangle \rightarrow |x\rangle|(f(x)+j) \bmod d\rangle \tag{15}$$

where

$$f(x) = g(a) \cdot x \bmod d. \tag{16}$$

We have

$$SUM_{f(x)}|x\rangle|\phi\rangle = \omega^{f(x)}|x\rangle|\phi\rangle. \tag{17}$$

In what follows, we will discuss the rationale behind of the above relation (17). Now consider applying the $SUM_{f(x)}$ gate to the state $|x\rangle|\phi\rangle$. Each term in $|\phi\rangle$ is of the form $\omega^{d-j}|j\rangle$. We see

$$\begin{aligned} &SUM_{f(x)}\omega^{d-j}|x\rangle|j\rangle \\ &\rightarrow \omega^{d-j}|x\rangle|(j+f(x)) \bmod d\rangle. \end{aligned} \tag{18}$$

We introduce k such as $f(x)+j = k \Rightarrow d-j = d+f(x)-k$. Hence (18) becomes

$$\begin{aligned} &SUM_{f(x)}\omega^{d-j}|x\rangle|j\rangle \\ &\rightarrow \omega^{f(x)}\omega^{d-k}|x\rangle|k \bmod d\rangle. \end{aligned} \tag{19}$$

Now, when $k < d$ we have $|k \bmod d\rangle = |k\rangle$ and thus, the terms in $|\phi\rangle$ such that $k < d$ are transformed as follows

$$SUM_{f(x)}\omega^{d-j}|x\rangle|j\rangle \rightarrow \omega^{f(x)}\omega^{d-k}|x\rangle|k\rangle. \tag{20}$$

Also, as $f(x)$ and j are bounded above by $d-1$, k is strictly less than $2d$. Hence, when $d \le k < 2d$ we have $|k \bmod d\rangle = |k-d\rangle$. Now, we introduce m such that $k - d = m$ then we have

$$\begin{aligned} &\omega^{f(x)}\omega^{d-k}|x\rangle|k \bmod d\rangle = \omega^{f(x)}\omega^{-m}|x\rangle|m\rangle \\ &= \omega^{f(x)}\omega^{d-m}|x\rangle|m\rangle. \end{aligned} \tag{21}$$

Hence the terms in $|\phi\rangle$ such that $k \ge d$ are transformed as follows

$$SUM_{f(x)}\omega^{d-j}|x\rangle|j\rangle \rightarrow \omega^{f(x)}\omega^{d-m}|x\rangle|m\rangle. \tag{22}$$

Hence from (20) and (22) we have

$$SUM_{f(x)}|x\rangle|\phi\rangle = \omega^{f(x)}|x\rangle|\phi\rangle. \tag{23}$$

Therefore, the relation (17) holds.

We have $|\psi_2\rangle$ by operating $SUM_{f(x)}$ to $|\psi_1\rangle$

$$SUM_{f(x)}|\psi_1\rangle = |\psi_2\rangle = \sum_{x\in K} \frac{\omega^{f(x)}|x\rangle}{\sqrt{(2d-1)^N}}|\phi\rangle. \tag{24}$$

After the general Fourier transform of $|x\rangle$, using the previous equations (11) and (24) we can now evaluate $|\psi_3\rangle$ as follows

$$|\psi_3\rangle = \sum_{z\in K}\sum_{x\in K}\frac{(\omega)^{x\cdot z+f(x)}|z\rangle}{(2d-1)^N}|\phi\rangle$$
$$= \sum_{z\in K}\sum_{x\in K}\frac{(\omega)^{x\cdot z+g(a)\cdot x}|z\rangle}{(2d-1)^N}|\phi\rangle. \quad (25)$$

Because we have

$$\sum_{x\in K}(\omega)^x = 0 \quad (26)$$

we may notice

$$\sum_{x\in K}(\omega)^{x\cdot(z+g(a))} = (2d-1)^N\delta_{z+g(a),0}$$
$$= (2d-1)^N\delta_{z,-g(a)}. \quad (27)$$

Therefore, the above summation is zero if $z \neq -g(a)$ and the above summation is $(2d-1)^N$ if $z = -g(a)$. Thus we have

$$|\psi_3\rangle = \sum_{z\in K}\sum_{x\in K}\frac{(\omega)^{x\cdot z+g(a)\cdot x}|z\rangle}{(2d-1)^N}|\phi\rangle$$
$$= \sum_{z\in K}\frac{(2d-1)^N\delta_{z,-g(a)}|z\rangle}{(2d-1)^N}|\phi\rangle$$
$$= -|(g(a_1),g(a_2),g(a_3),\ldots,g(a_N))\rangle|\phi\rangle \quad (28)$$

from which

$$|(g(a_1),g(a_2),g(a_3),\ldots,g(a_N))\rangle \quad (29)$$

can be obtained. That is to say, if we measure the first N qudits state of the state $|\psi_3\rangle$, that is, $|(g(a_1),g(a_2),g(a_3),\ldots,g(a_N))\rangle$, then we can retrieve the following values

$$g(a_1),g(a_2),g(a_3),\ldots,g(a_N) \quad (30)$$

using a single query. The method determines the maximum of and the minimum of the function g that the finite domain is $\{a_1,a_2,a_3,\ldots,a_N\}$.

III. CONCLUSIONS

In conclusion, we have presented the generalized Bernstein-Vazirani algorithm for determining an integer string. Given the set of real values $\{a_1,a_2,a_3,\ldots,a_N\}$ and a function $g:\mathbf{R}\to\mathbf{Z}$, 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. The method has determined the maximum of and the minimum of the function g that the finite domain is $\{a_1,a_2,a_3,\ldots,a_N\}$.

ACKNOWLEDGEMENTS

We thank Professor Germano Resconi for valuable comments.

[1] E. Bernstein and U. Vazirani, 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

[2] E. Bernstein and U. Vazirani, SIAM J. Comput. 26-5, pp. 1411-1473 (1997). https://doi.org/10.1137/S0097539796300921

[3] D. Deutsch, *Proc. Roy. Soc. London Ser. A* **400**, 97 (1985). https://doi.org/10.1098/rspa.1985.0070

[4] D. Deutsch and R. Jozsa, *Proc. Roy. Soc. London Ser. A* **439**, 553 (1992). https://doi.org/10.1098/rspa.1992.0167

[5] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Proc. Roy. Soc. London Ser. A* **454**, 339 (1998). https://doi.org/10.1098/rspa.1998.0164

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

[7] P. W. Shor, Proceedings of the 35th IEEE Symposium on Foundations of Computer Science. 124 (1994).

[8] L. K. Grover, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. 212 (1996).

[9] K. Nagata, G. Resconi, T. Nakamura, J. Batle, S. Abdalla, and A. Farouk, MOJ Ecology and Environmental Science, Volume 2, Issue 1, 00010, (2017). https://doi.org/10.15406/mojes.2017.02.00010

[10] K. Nagata, T. Nakamura, H. Geurdes, J. Batle, S. Abdalla, and A. Farouk, Int J Theor Phys (2018). https://doi.org/10.1007/s10773-018-3687-5

[11] K. Nagata, T. Nakamura, H. Geurdes, J. Batle, S. Abdalla, A. Farouk, and D. N. Diep, Int J Theor Phys (2017). https://doi.org/10.1007/s10773-017-3630-1