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 Diep6

1Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea
2Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan
3Geurdes Datascience, KeK 6452202, C vd Lijnstraat 164, 2593 NN, Den Haag Netherlands
4Departament de Física, Universitat de les Illes Balears, 07122 Palma de Mallorca, Balearic Islands, Europe
5Computer Sciences Department, Faculty of Computers and Information, Mansoura University, Egypt
6TIMAS, 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 \( g: \mathbb{R} \to \mathbb{Z} \), 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 arguments provide a new insight into the importance of the original Bernstein-Vazirani algorithm.

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 to \{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 \( \mathbb{N} \) [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 \( \mathbb{Z} \). 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 \( g: \mathbb{R} \to \mathbb{Z} \), 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

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

\[
a_1, a_2, a_3, \ldots, a_N.
\]

Let us now introduce a function

\[
g: \mathbb{R} \to \mathbb{Z}.
\]

Our goal is of determining the following values

\[
g(a_1), g(a_2), g(a_3), \ldots, g(a_N).
\]

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

\[
-(d-1) \leq g(a_1), g(a_2), g(a_3), \ldots, g(a_N) \leq d-1
\]

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

\[
g(a) = (g(a_1), g(a_2), g(a_3), \ldots, g(a_N))
\]
where each entry of \( g(a) \) is an integer in the modulo \( d \). Here \( g(a) \in \{-d+1, \ldots, -1,0,1,\ldots, d-1\}^N \). We define \( f(x) \) as follows
\[
f(x) = g(a) \cdot x \mod d
\]
(6)
where \( x = (x_1, \ldots, x_N) \in \{-d+1, \ldots, -1,0,1,\ldots, d-1\}^N \). Let us follow the quantum states through the algorithm.

The input state is
\[
|\psi_0\rangle = |0\rangle \otimes \cdots \otimes |0\rangle \rangle (d-1)
\]
(7)
where \( |0\rangle \otimes \cdots \otimes |0\rangle \rangle (d-1) \) means \( |0,0,\ldots,0\rangle \). We discuss the general Fourier transform of \( |0\rangle \)
\[
|0\rangle \rightarrow \sum_{y=-\cdots,0} \frac{\omega^y|y\rangle}{\sqrt{d}} = \sum_{y=0}^{d-1} \frac{\omega^y|y\rangle}{\sqrt{d}}
\]
(8)
where we have used \( \omega^d = 1 \).

Subsequently let us define the wave function \( |\phi\rangle \) as follows
\[
|\phi\rangle = \frac{1}{\sqrt{d}} (\omega^0|0\rangle + \omega^{-1}|1\rangle + \cdots + \omega^{d-1}|d-1\rangle)
\]
(9)
where \( \omega = e^{2\pi i/d} \). In the following, we discuss the Fourier transform of \( |d-1\rangle \)
\[
|d-1\rangle \rightarrow \sum_{y=0}^{d-1} \frac{\omega^y|y\rangle}{\sqrt{d}} = \sum_{y=0}^{d-1} \frac{\omega^{y-d}|y\rangle}{\sqrt{d}}
\]
\[
= \sum_{y=0}^{d-1} \frac{\omega^{y-d}|y\rangle}{\sqrt{d}} = |\phi\rangle
\]
(10)
where we have used \( \omega^{yd} = \omega^d = 1 \).

The general Fourier transform of \( |x_1 \ldots x_N\rangle \) is as follows
\[
|x_1 \ldots x_N\rangle \rightarrow \sum_{z_1=\cdots,0} \sum_{z_N=\cdots,0} \frac{\omega^{z_1x_1}|z_1\rangle \cdots \omega^{z_Nx_N}|z_N\rangle}{\sqrt{2d-1}^{N}}
\]
(11)
where \( K = \{-d+1, \ldots, -1,0,1,\ldots, d-1\}^N \) and \( z \) is \( (z_1,z_2,\ldots,z_N) \). Hence, for completeness, \( \sum_{x \in K} z \) is a shorthand to the compound sum
\[
\sum_{z_1\in\{-d+1, \ldots, -1,0,1,\ldots, d-1\}} \cdots \sum_{z_N\in\{-d+1, \ldots, -1,0,1,\ldots, d-1\}}
\]
(12)

After the componentwise general Fourier transforms of the first \( N \) qudits state and after the Fourier transform of \( |d-1\rangle \) in (7)
\[
G(0) \otimes G(0) \otimes \cdots \otimes G(0) \otimes F|d-1\rangle
\]
(13)
we have
\[
|\psi_1\rangle = \sum_{x \in K} \frac{|x\rangle}{\sqrt{2d-1}^N} |\phi\rangle
\]
(14)
Here, the notation \( G(0) \) 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
\[
|x\rangle |j\rangle \rightarrow |x\rangle |(f(x) + j) \mod d\rangle
\]
(15)
where
\[
f(x) = g(a) \cdot x \mod d.
\]
(16)
We have
\[
SUM_f(x)|x\rangle |\phi\rangle = \omega^{f(x)} |x\rangle |\phi\rangle.
\]
(17)
In what follows, we will discuss the rationale behind 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
\[
SUM_f(x)|x\rangle |\phi\rangle = \omega^{f(x)} |x\rangle |\phi\rangle
\]
(18)
We introduce \( k \) such as \( f(x)+j = k \) \( \Rightarrow d-j = d+f(x)-k \). Hence (18) becomes
\[
SUM_f(x)|w^{d-k} |x\rangle |\phi\rangle
\]
(19)
Now, when \( k < d \) we have \( |k \mod d = |k \rangle \) and thus, the terms in \( |\phi\rangle \) such that \( k < d \) are transformed as follows
\[
SUM_f(x)|w^{d-k} |x\rangle |\phi\rangle \rightarrow SUM_f(x)|w^{d-k} |x\rangle |\phi\rangle.
\]
(20)
Also, as \( f(x) \) and \( j \) are bounded above by \( d-1 \), \( k \) is strictly less than \( 2d \). Hence, when \( d \leq k < 2d \) we have \( |k \mod d = |k-d \rangle \). Now, we introduce \( m \) such that \( k-d = m \) then we have
\[
\omega^{f(x)}w^{d-k} |x\rangle |m\rangle = \omega^{f(x)}w^{d-m} |x\rangle |m\rangle
\]
(21)
Hence the terms in \( |\phi\rangle \) such that \( k \geq d \) are transformed as follows
\[
SUM_f(x)|w^{d-j} |x\rangle |\phi\rangle \rightarrow SUM_f(x)|w^{d-m} |x\rangle |\phi\rangle.
\]
(22)
Hence from (20) and (22) we have
\[
SUM_f(x)|x\rangle |\phi\rangle = \omega^{f(x)} |x\rangle |\phi\rangle.
\]
(23)
Therefore, the relation (17) holds.

We have \( |\psi_2\rangle \) by operating \( SUM_f(x) \) to \( |\psi_1\rangle \)
\[
SUM_f(x)|\psi_1\rangle = |\psi_2\rangle = \sum_{x \in K} \frac{\omega^{f(x)} |x\rangle}{\sqrt{2d-1}^N} |\phi\rangle.
\]
(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

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

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

(25)

Because we have

$$
\sum_{z \in K} (\omega)^z = 0
$$

(26)

we may notice

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

$$
= (2d-1)^N \delta_{z,-g(a)}.
$$

(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

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

$$
= \sum_{z \in K} \frac{(2d-1)^N \delta_{z,-g(a)}|z\rangle}{(2d-1)^N} |\phi\rangle
$$

$$
= -(|g(a_1), g(a_2), g(a_3), \ldots, g(a_N))|\phi\rangle
$$

(28)

from which

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

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

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

(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 $g : R \rightarrow Z$, 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.

---


