Quantum computing determining a homogeneous linear function

Koji Nagata,[1] Tadao Nakamura,[2] Han Geurdes,[3] Josep Batle,[4]
Soliman Abdalla,[5] Ahmed Farouk,[6] and Do Ngoc Diep[7,8]

[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] *Department of Physics, Faculty of Science, King Abdulaziz University Jeddah, P.O. Box 80203, Jeddah 21589, Saudi Arabia*
[6] *Computer Sciences Department, Faculty of Computers and Information, Mansoura University*
[7] *Institute of Mathematics, VAST, 18 Hoang Quoc Viet road, 10307, Hanoi Vietnam*
[8] *TIMAS, Thang Long University, Nghiem Xuan Yem, Dai Kim, Hoang Mai, Hanoi, Vietnam*

(Dated: September 1, 2017)

We present a method of highly speedy determining a homogeneous linear function $f(x) := s.x = s_1x_1+s_2x_2+\cdots+s_nx_n$ from $\{0,1,\ldots,d-1\}^n$ with coefficients $s = (s_1,\ldots,s_n)$. Here $x = (x_1,\ldots,x_n)$ and $x_j \in \mathbf{R}$. Given the interpolation values $f(1), f(2), ..., f(N)$, we shall determine the unknown coefficients $s = (s_1,\ldots,s_n)$ of the linear function, simultaneously. The speed of determining the values is shown to outperform the classical case by a factor of N.

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

I. INTRODUCTION

Quantum mechanics (cf. [1–6]) gives approximate and at times remarkably accurate numerical predictions. Quantum mechanics is successful in explaining and predicting many phenomena. Therefore there are many reasons to be convinced of the correctness of quantum mechanics. One of the interesting applications of quantum principles is its application to to information theory [6] leading to the quantum computer.

A quantum computer is a device for computation that makes direct use of superposition of states and entanglement, to perform operations on data. Quantum computers are different from digital computers based on transistor gates. Whereas digital computers require data to be encoded into binary digits (bits). Quantum computation utilizes quantum properties of e.g. molecules to represent data and subsequently perform operations on these representations of data [7]. A theoretical model is the quantum Turing machine, also known as the universal quantum computer. Quantum computers share theoretical similarities with non-deterministic and probabilistic computers, like the ability to be in more than one state simultaneously. The field of quantum computing was first introduced by Richard Feynman in 1982 [8, 9].

The Deutsch-Jozsa algorithm is a quantum algorithm, proposed by David Deutsch and Richard Jozsa in 1992 [10] with improvements by Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca in 1998 [11]. Although of little practical use, it is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm. It is also a deterministic algorithm, meaning that it always produces an answer, and that answer is always correct.

The Deutsch-Jozsa algorithm generalizes earlier (1985) work by David Deutsch, which provided a solution for the simple case. Specifically we are given a boolean function whose input is 1 bit, $f : \{0, 1\} \to \{0, 1\}$ and asked if it is constant [12].

The algorithm as Deutsch has originally proposed it is not, in fact, deterministic. The algorithm is successful with a probability of one half. In 1992, Deutsch and Jozsa produced a deterministic algorithm which was generalized to a function which takes N bits for its input. Unlike Deutsch's algorithm, this algorithm requires two function evaluations instead of only one.

Further improvements to the Deutsch-Jozsa algorithm are made by Cleve *et al.*, [11] resulting in an algorithm that is both deterministic and requires only a single query of f. This algorithm is still referred to as Deutsch-Jozsa algorithm in honour of the groundbreaking techniques they employed [11].

The Deutsch-Jozsa algorithm provides inspiration for Shor's algorithm and Grover's algorithm, two of the most revolutionary quantum algorithms [13, 14].

Looking at studies of quantum computing, implementation of a quantum algorithm to solve Deutsch's problem [10–12] on a nuclear magnetic resonance quantum computer is reported firstly [15]. An 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.* implements Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [17]. In addition, single-photon Bell states are prepared and measured [18]. Also the decoherence-free implementation of Deutsch's algorithm is introduced by using such single-photon and by using two logical qubits [19]. A one-way based experimental implementation of Deutsch's algorithm is reported [20].

For a number of recent algorithmic developments we mention the following. In 1993, the Bernstein-Vazirani algorithm was published [21, 22]. This work can be considered an extension of the Deutsch-Jozsa algorithm. In 1994, Simon's algorithm was published [23]. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement in an ensemble quantum computer can be mentioned as an important quantum algorithm [24]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits was also discussed in the recent past [25]. The question whether or not quantum learning is robust against noise is a subject of intense study [26].

A quantum algorithm for approximating the influences of Boolean functions and its applications is recently studied [27]. In addition, Quantum computation with coherent spin states and the close Hadamard problem [28] and the transport implementation of the Bernstein-Vazirani algorithm with ion qubits are studied [29]. Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers are discussed [30]. We mention that the dynamical analysis of Grover's search algorithm in arbitrarily high-dimensional search spaces is studied [31]. A method of computing many functions simultaneously by using many parallel quantum systems is reported [32].

On the other hand, we may wonder if we need all the previously mentioned studies to reach a good quantum computer. The earliest quantum algorithm, the Deutsch-Jozsa algorithm, is representative to show that quantum computation is faster than its classical counterpart. Its magnitude grows exponentially with the number of qubits. In 2015, it was discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [33]. In 2017, it was discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [34]. Subsequently, a highly speedy secure quantum cryptography based on the Deutsch-Jozsa algorithm was proposed [35].

The relation between quantum computer and secret sharing with the use of quantum principles is discussed [36].

However, it can be stated that quantum computers presently are "quantum estimators". There are many open problems that we cannot solve them by using quantum estimators. By a case, quantum estimators cannot solve a problem that classical computers can solve correctly. Therefore, we need more rigorous quantum devices for computation of solving such a problem. Motivated by this conjecture, let us discuss the arbitrary high-dimensional quantum computer. And we solve very wide problem by using a new quantum device proposed here. It is first step to a true quantum computer.

In this paper, we present a method of determining a homogeneous linear function $f(x) := s.x = s_1x_1 + s_2x_2 + \cdots + s_nx_n$ from $\{0, 1, \ldots, d-1\}^n$ with coefficients $s = (s_1, \ldots, s_n)$. Here $x = (x_1, \ldots, x_n)$ and $x_j \in \mathbf{R}$. Our quantum algorithm overcomes a classical counterpart by a factor of $O(N)$.

II. THE GENERALIZED BERNSTEIN-VAZIRANI ALGORITHM TO QUDIT SYSTEMS

In this section, we review [37] an algorithm to solve the Bernstein-Vazirani problem for a d-dimensional system. Our algorithm combines quantum parallelism with a property of quantum mechanics known as interference. Here the problem changes to finding an unknown string $s \in \{0, 1, ..., d-1\}^N$ by querying a quantum state.

We define $f_s(x)$ as follows;

$$f_s(x) = s \cdot x \bmod d = s_1x_1 + s_2x_2 + \cdots + s_Nx_N \bmod d \tag{1}$$

where $x \in \{0, 1, ..., d-1\}^N$

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

$$|\psi_0\rangle = |0\rangle^{\otimes N}|d-1\rangle. \tag{2}$$

We define $|\phi\rangle$ as follows;

$$|\phi\rangle = \frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle) \tag{3}$$

In the following, we discuss the Fourier transform of $|d-1\rangle$;

$$|d-1\rangle \to \sum_{z=0}^{d-1} \frac{\omega^{z\cdot(d-1)}|z\rangle}{\sqrt{d}} = \sum_{z=0}^{d-1} \frac{\omega^{zd-z}|z\rangle}{\sqrt{d}} = \sum_{z=0}^{d-1} \frac{\omega^{d-z}|z\rangle}{\sqrt{d}} = |\phi\rangle \tag{4}$$

After the $N+1$ Fourier transforms on the state, we have

$$|\psi_1\rangle = \sum_{x=0}^{d-1} \frac{|x\rangle}{\sqrt{d^N}} \frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle) \tag{5}$$

We introduce $SUM_{f_s(x)}$ gate;

$$|x\rangle|j\rangle \to |x\rangle|(f_s(x) + j) \bmod d\rangle \tag{6}$$

Here,

$$SUM_{f_s(x)} = SUM_{s\cdot x} \tag{7}$$

We have

$$SUM_{s\cdot x}|x\rangle|\phi\rangle = \omega^{s\cdot x}|x\rangle|\phi\rangle \tag{8}$$

In what follows, we discuss the reason of the above relation (8).

Now consider applying the SUM gate to the state $|x\rangle|\phi\rangle$. Each term in $|\phi\rangle$ is of the form $\omega^{d-j}|j\rangle$. We see

$$SUM\omega^{d-j}|x\rangle|j\rangle \to \omega^{d-j}|x\rangle|(j + s\cdot x) \bmod d\rangle \tag{9}$$

We introduce k such as $s \cdot x + j = k \Rightarrow d - j = d + s \cdot x - k$.

Hence (9) becomes,

$$SUM\omega^{d-j}|x\rangle|j\rangle \to \omega^{s\cdot x}\omega^{d-k}|x\rangle|k \bmod d\rangle \tag{10}$$

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

$$SUM\omega^{d-j}|x\rangle|j\rangle \rightarrow \omega^{s\cdot x}\omega^{d-k}|x\rangle|k\rangle \tag{11}$$

Also, as $s \cdot x$ and j are bounded above by $d-1$, k is strictly less than $2d$. Hence, when $d \leq k < 2d$ we have $|k \bmod d\rangle = |k-d\rangle$.

Now, we introduce m such that $k - d = m$ then we have

$$\omega^{s\cdot x}\omega^{d-k}|x\rangle|k \bmod d\rangle = \omega^{s\cdot x}\omega^{-m}|x\rangle|m\rangle = \omega^{s\cdot x}\omega^{d-m}|x\rangle|m\rangle \tag{12}$$

Hence the terms in $|\phi\rangle$ such that $k \geq d$ is

$$SUM\omega^{d-j}|x\rangle|j\rangle \rightarrow \omega^{s\cdot x}\omega^{d-m}|x\rangle|m\rangle \tag{13}$$

Hence from (11) and (13) we have

$$SUM|x\rangle|\phi\rangle = \omega^{s\cdot x}|x\rangle|\phi\rangle \tag{14}$$

Therefore, the relation (8) holds.

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

$$SUM_{s\cdot x}|\psi_1\rangle = |\psi_2\rangle = \sum_{x=0}^{d-1}\frac{\omega^{s\cdot x}|x\rangle}{\sqrt{d^N}}\frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle) \tag{15}$$

The Fourier transform of $|x\rangle$ is as follows;

$$|x_0x_1...x_N\rangle \rightarrow \sum_{z_0=0}^{d-1}\sum_{z_1=0}^{d-1}\cdots\sum_{z_N=0}^{d-1}\frac{\omega^{z_0x_0}|z_0\rangle}{\sqrt{d}}\frac{\omega^{z_1x_1}|z_1\rangle}{\sqrt{d}}\cdots\frac{\omega^{z_Nx_N}|z_N\rangle}{\sqrt{d}} \tag{16}$$

Thus we have

$$|x\rangle \rightarrow \sum_{z=0}^{d-1}\frac{\omega^{z\cdot x}|z\rangle}{\sqrt{d^N}} \tag{17}$$

After the Fourier transform on $|x\rangle$, using the previous equation (15) and (17) we can now evaluate $|\psi_3\rangle$,

$$|\psi_3\rangle = \sum_{z=0}^{d-1}\sum_{x=0}^{d-1}\frac{(\omega)^{x\cdot z+s\cdot x}|z\rangle}{d^N}\frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle) \tag{18}$$

We notice

$$\sum_{x=0}^{d-1}(\omega)^{x(z+s)} = d\delta_{z+s,0} = d\delta_{z,-s}. \tag{19}$$

Thus,

$$\begin{aligned}|\psi_3\rangle &= \sum_{z=0}^{d-1}\sum_{x=0}^{d-1}\frac{(\omega)^{x\cdot z+s\cdot x}|z\rangle}{d^N}\frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle)\\ &= \sum_{z=0}^{d-1}\frac{d^N\delta_{z,-s}|z\rangle}{d^N}\frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle)\\ &= -|s_1s_2...s_N\rangle\frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle)\end{aligned} \tag{20}$$

from which

$$|s_1s_2...s_N\rangle. \tag{21}$$

can be obtained. That is to say, if we measure $|s_1s_2...s_N\rangle$ then we can retrieve the following values

$$s_1s_2...s_N \tag{22}$$

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

The speed to determine N values improves by a factor of N as compared to the classical counterpart. Notice that we recoiver the Bernstein-Vazirani algorithm when $d = 2$.

III. QUANTUM COMPUTING DETERMINING A HOMOGENEOUS LINEAR FUNCTION

Suppose f is a homogeneous linear function $f(x) := s.x = s_1x_1 + s_2x_2 + \cdots + s_nx_n$ from $\{0, 1, \ldots, d-1\}^n$ with coefficients $s = (s_1, \ldots, s_n)$, such that

$$0 \leq f(1), f(2), \ldots, f(N) \leq d-1. \tag{23}$$

Our goal is of determining the unknown coefficients $s_1, \ldots, s_n$ from knowing the interpolation values $f(1), f(2), ..., f(N)$, simultaneously. Because the function is linear, we need to know exactly N points $(1, f(1)), \ldots, (N, f(N))$ to interpolate the function in the classical case, i.e. we need N steps of computing. However as we will show in the quantum mechanical case, we need a query.

Here we are given the interpolation values $f(1), f(2), ..., f(N)$

$$\begin{aligned} f(1) &= s_1a_1 + s_2a_2 + \cdots + s_na_n = y^1 \\ f(2) &= s_1b_1 + s_2b_2 + \cdots + s_nb_n = y^2 \\ &\cdots \\ f(N) &= s_1c_1 + s_2c_2 + \cdots + s_nc_n = y^n \end{aligned} \tag{24}$$

We are given the following values

$$\vec{y} = (y^1, y^2, ..., y^n) \tag{25}$$

Our aim is of determining the following values, simultaneously

$$s = (s_1(\vec{y}), s_2(\vec{y}), ..., s_n(\vec{y})) = (s_1, \ldots, s_n) \tag{26}$$

Following Kronecker's Theorem, the system (24) of linear equations has a unique solution $s = (s_1, \ldots, s_n)$ if and only if the augmented coefficient matrix

$$(A|\mathbf{b}) := \begin{pmatrix} a_1 & a_2 & \ldots & a_n & y^1 \\ b_1 & b_2 & \ldots & b_n & y^2 \\ .. & .. & ... & .. & .. \\ c_1 & c_2 & \ldots & c_n & y^n \end{pmatrix}$$

has rank n, i.e. the interpolation points $(a, y^1), (b, y^2), \ldots, (c, y^n)$ are in generic position. The problem can be solved by the generalized Bernstein-Vazirani algorithm to qudit systems.

Therefore, we arrived to the goal of finding out the unknown coefficients $s = (s_1, \ldots, s_n)$ from the given

$$(f(1), f(2), ..., f(N)) \tag{27}$$

So, we know the unknown coefficients $s = (s_1, \ldots, s_n)$ of the linear function $f(x) = s.x$, if we know the interpolation values $(f(1), f(2), ..., f(N))$.

IV. CONCLUSIONS

In conclusion, we have presented a method of determining a linear function $f(x) := s.x = s_1x_1 + s_2x_2 + \cdots + s_nx_n$ from $\{0, 1, \ldots, d-1\}^n$ with coefficients $s = (s_1, \ldots, s_n)$. Here $x = (x_1, \ldots, x_n)$ and $x_j \in \mathbf{R}$. Our quantum algorithm has overcome a classical counterpart by a factor of $O(N)$.

ACKNOWLEDGEMENTS

We thank Prof. Germano Resconi for valuable comments.

[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] "Quantum Computing with Molecules" article in Scientific American by Neil Gershenfeld and Isaac L. Chuang.
[8] Quantum computation. David Deutsch, Physics World, 1/6/92.
[9] Quantum computer - Wikipedia, the free encyclopedia
[10] D. Deutsch and R. Jozsa, *Proc. Roy. Soc. London Ser. A* **439**, 553 (1992).
[11] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Proc. Roy. Soc. London Ser. A* **454**, 339 (1998).
[12] D. Deutsch, *Proc. Roy. Soc. London Ser. A* **400**, 97 (1985).
[13] P. W. Shor, Proceedings of the 35th IEEE Symposium on Foundations of Computer Science. 124 (1994).
[14] L. K. Grover, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. 212 (1996).
[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] A. W. Cross, G. Smith, and J. A. Smolin, Phys. Rev. A **92**, 012327 (2015).
[27] H. Li and L. Yang, Quantum Inf. Process. **14**, 1787 (2015).
[28] M. R. A. Adcock, P. Hoyer, and B. C. Sanders, Quantum Inf. Process. **15**, 1361 (2016).
[29] S. D. Fallek, C. D. Herold, B. J. McMahon, K. M. Maller, K. R. Brown, and J. M. Amini, New J. Phys. **18**, 083030 (2016).
[30] D. N. Diep, D. H. Giang, and N. Van Minh, Int J Theor Phys (2017) 56: 1948. https://doi.org/10.1007/s10773-017-3340-8.
[31] W. Jin, Quantum Inf. Process. **15**, 65 (2016).
[32] K. Nagata, G. Resconi, T. Nakamura, J. Batle, S. Abdalla, A. Farouk, and H. Geurdes, Asian J. Math. Phys. 1 (1) (2017), 1-4.
[33] K. Nagata and T. Nakamura, Open Access Library Journal, 2: e1798 (2015). http://dx.doi.org/10.4236/oalib.1101798.
[34] K. Nagata and T. Nakamura, Int J Theor Phys (2017) 56: 2086. https://doi.org/10.1007/s10773-017-3352-4
[35] K. Nagata, T. Nakamura, and A. Farouk, Int J Theor Phys (2017). https://doi.org/10.1007/s10773-017-3456-x.
[36] D. N. Diep and D. H. Giang, Int J Theor Phys (2017). https://doi.org/10.1007/s10773-017-3444-1.
[37] R. Krishna, V. Makwana, A. P. Suresh, arXiv:1609.03185 [quant-ph] (2016).