

A generalization of the Bernstein-Vazirani algorithm

Opinion

In this short contribution we present a generalization of the Bernstein-Vazirani algorithm. Given the set of real values $\{a_1, a_2, a_3, \dots, a_N\}$ and the function $g: \mathbb{R} \rightarrow \{0, 1\}$, we shall determine the following values $\{g(a_1), g(a_2), g(a_3), \dots, g(a_N)\}$ simultaneously. We are thus generalizing the Bernstein-Vazirani algorithm. We recover the usual algorithm when $g: a_i \rightarrow a_i$. The speed of determining the N values will be shown to outperform the classical case by a factor of N . PACS numbers: 03.67.Lx (Quantum computation architectures and implementations), 03.67.Ac (Quantum algorithms, protocols, and simulations).

Quantum mechanics¹⁻⁶ provides exact and frequently remarkably accurate numerical predictions, as reported for over a century. There has been a remarkable link in recent decades between the quantum theory and information theory, given rise to the rich field of quantum information theory (QIT), which novel proposals that outperform classical tasks or simply have no classical counterpart.⁶ One case that involves both quantum theory and information theory that can be found in the foundations of the quantum theory is the Leggett-type non-local variables theory,⁷ which has been experimentally explored.⁸⁻¹⁰ These experiments report that quantum theory does not accept a Leggett-type non-local variables interpretation, although some controversy remains around the conclusions and interpretations of the experimental outcomes.¹¹⁻¹³ Applications of QIT also include the implementation of quantum algorithms. One such case is provided for stance by the Deutsch's problem,¹⁴ first experimentally realized on a nuclear magnetic resonance proof-of-principle quantum computer.¹⁵ Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer has also been achieved.¹⁶ There have been, as well, several other attempts to use single-photon two qubit states for quantum computing. Oliveira et al. implemented the Deutsch's algorithm with polarization and transverse electromagnetic spatial modes as qubits.¹⁷ Other achievements also include single-photon Bell states preparation and measurement,¹⁸ a decoherence free implementation of Deutsch's algorithm using single photon and using two logical qubits¹⁹ and, more recently, a one-way quantum computing implementation of the algorithm.²⁰ These achievements involving the Deutsch-Jozsa algorithm are very well related to the so-called Bernstein-Vazirani algorithm,^{21,22} which can be considered as an extended version of the previous one. After these two algorithms, Simon's algorithm²³ was discovered, among others. There has been an experimental implementation of a quantum algorithm that solves the Bernstein-Vazirani parity problem without entanglement.²⁴ Additionally, fiber-optics implementations of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits have been realized.²⁵ Also, a variant of the algorithm for quantum learning being robust against noise has been introduced,²⁶ as well as a quantum algorithm for approximating the influences of Boolean functions and its applications.²⁷ The Bernstein-Vazirani growth has been also versatile in quantum key distribution²⁸ and transport implementation with ion qubits.²⁹ In the present work we shall extend the Bernstein-Vazirani algorithm a bit further. In what follows, we present in full detail our generalization and some conclusions are drawn. Let us suppose that we are given the following sequence of real values

Volume 2 Issue 1 - 2017

Nagata K,¹ Resconi G,² Nakamura T,³ Batle J,⁴ Abdalla S,⁵ Farouk F⁶

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

²Department of Mathematics and Physics, Catholic University, Italy

³Department of Information and Computer Science, Keio University, Japan

⁴Departament de Física, Universidad de les Illes Balears, Spain

⁵Department of Physics, King Abdulaziz University Jeddah, Saudi Arabia

⁶Information Technology Department, Al-Zahra College for Women, Egypt

Correspondence: Nagata K, Department of Physics, Advanced Institute of Science and Technology, Daejeon 305-701, Korea, Email ko-mi-na@yahoo.co.jp

Received: February 02, 2017 | **Published:** February 09, 2017

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

Let us now introduce the function

$$g: \mathbb{R} \rightarrow \{0, 1\}. \tag{2}$$

Our goal is to determine the following values:

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

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

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

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

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

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

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

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

$$|\psi_1\rangle = \bigoplus^N |1\rangle \tag{7}$$

After the Hadamard transform on the state, we have

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \tag{8}$$

Next, the function f is evaluated using

$$Uf : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle \tag{9}$$

Giving

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \tag{10}$$

After the Hadamard transform, using the previous equation and (10) we can now evaluate $|\psi_3\rangle$

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \tag{11}$$

Thus,

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x \cdot z + g(a) \cdot x} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \tag{12}$$

$$\sum_x (-1)^{x \cdot z + g(a) \cdot x} = 2^N \delta_{g(a), z} \tag{13}$$

Thus,

$$\begin{aligned} |\psi_3\rangle &= \pm \sum_z \sum_x \frac{(-1)^{x \cdot z + g(a) \cdot x} |z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ &= \pm \sum_z \frac{2^{N\delta} g(a) \cdot z}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ &= \pm |g(a)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ &= \pm |g(a_1)g(a_2)...g(a_N)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \end{aligned} \tag{14}$$

from which

$$|g(a_1), g(a_2)...g(a_N)\rangle \tag{15}$$

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

$$g(a_1), g(a_2), g(a_3), \dots, g(a_N) \tag{16}$$

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 receive the Bernstein-Vazirani algorithm when $g : ai \rightarrow ai$

In the present work we have presented a generalization of the Bernstein-Vazirani algorithm. The advantage that is promised over its classical counterpart is $O(N)$, much like in the vein of quantum

parallelism, where the N coefficients of a pure state $|\psi_N\rangle$ can be known in one single quantum query.

Acknowledgements

J. Batle acknowledges fruitful discussions with J. Rossell'o, Maria del Mar Batle and Regina Batle.

Conflict of interest

The author declares no conflict of interest.

References

1. Von Neumann J. *Mathematical foundations of quantum mechanics*. Princeton, New Jersey: Princeton University Press; 1995.
2. Feynman RP, Leighton RB, Sands M. *Lectures on physics. Quantum mechanics*. 3; 1965.
3. Redhead M. *Incompleteness, no locality, and realism*. 2nd ed. Clarendon Press, Canada: Oxford; 1989.
4. Peres A. *Quantum theory: concepts and methods*. Dordrecht, The Netherlands: Kluwer Academic; 1995.
5. Sakurai JJ. *Modern quantum mechanics*. Addison-wesley publishing company; 1995.
6. Nielsen MA, Chuang IL. *Quantum computation and quantum information*. Cambridge University Press; 2000.
7. Leggett J. *Found. Phys.* 2003;33:1469.
8. Groblacher S, Paterek T, Kaltenbaek R, et al. A physical basis for entanglement in a non-local hidden variable theory. *Nature(London)*. 2007;446:871.
9. Paterek T, Fedrizzi A, Groblacher S, et al. Experimental test of nonlocal realistic theories without the rotational symmetry assumption. *Phys Rev Lett.* 2007;99(21-23):210406.
10. Branciard C, Ling A, Gisin N, et al. Experimental falsification of leggett's nonlocal variable model. *Phys Rev Lett.* 2007;99(21-23):210407.
11. Suarez A. Nonlocal "Realistic" leggett models can be considered refuted by the before-before experiment. *Found Phys.* 2008;38(6):583-589.
12. Zukowski M. Comment on: nonlocal "Realistic" leggett models can be considered refuted by the before-before experiment. *Found Phys.* 2008;38(11):1070-1071.
13. A Suarez. On Bell, Suarez-Scarani, and leggett experiments: reply to a comment by marek Zukowski. *Found Phys.* 2009;39(2):156-159.
14. Deutsch D. Quantum theory, the church-turing principle and the universal quantum computer. *Proc Roy Soc London Ser A.* 1985;400(1818):97.
15. Jones JA, Mosca M. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *Chem Phys.* 1998;109:1648
16. Gulde S, Riebe M, Lancaster GPT, et al. Quantum information processing with trapped Ca+ ions. *Nature.* 2003;421:48.
17. De Oliveira N, Walborn SP, Monken CH. *Opt. B: Quantum Semi class. Opt.* 2005;7:288-292.
18. Kim YH. Experimental entanglement concentration and universal Bell-state synthesizer. *Physical Review A.* 2003;67:040301(R).
19. Mohseni M, Lundeen JS, Resch KJ, et al. Experimental application of Decoherence-free subspaces in an optical quantum-computing algorithm. *Phys. Rev. Lett.* 2003;91(18):187903.

20. Tame MS, Prevedel R, Paternostro M, et al. Experimental realization of a quantum game on a one-way quantum computer. *Phys Rev Lett.* 2007;98:140501.
21. Bernstein E, Vazirani U. *Proceedings of the twenty-fifth annual ACM symposium on theory of computing (STOC '93)*. 1993;11–20.
22. Bernstein E, Vazirani U. Quantum complexity theory. *SIAM J* 1997;26(5):1411–1473.
23. Simon DR. *On the power of quantum computation. Foundations of computer science proceedings 35th annual symposium on foundations of computer science*. 1994;116–123.
24. Du J, Shi M, Zhou X, Fan Y, Ye BJ, et al. *Phys Rev.* 2001;64: 042306.
25. Brainis E, Lamoureux LP, Cerf NC, et al. *Phys Rev Lett.* 2003;90:157902.
26. Cross W, Smith G, Smolin JA. Quantum learning robust to noise. *Phys. Rev.* 2015;92:012327.
27. Li H, Yang L. A quantum algorithm for approximating the influences of Boolean functions and its applications. *Quantum Inf Process.* 2015;14(6):1787–1797.
28. Nagata K, Nakamura T. *The Deutsch–Jozsa Algorithm Can Be Used for Quantum Key Distribution. Open Access Library Journal.* 2015; p. 1–6.
29. Fallek SD, Herold CD, McMahon BJ, et al. Transport implementation of the Bernstein–Vazirani algorithm with ion qubits. *New J. Phys.* 2016;18:083030.