# Computational complexity in quantum computing

Koji Nagata,[1] Do Ngoc Diep,[2,3] and Tadao Nakamura[4]

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon, Korea*
*E-mail:* ko_mi_na@yahoo.co.jp

[2] *TIMAS, Thang Long University, Nghiem Xuan Yem road, Hoang Mai district, Hanoi, Vietnam*

[3] *Institute of Mathematics, VAST, 18 Hoang Quoc Viet road, Cau Giay district, Hanoi, Vietnam*

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

( Dated: November 3, 2021)

**Abstract**

Our aim is of studying the efficiency of two typical arithmetic calculations [T. Nakamura and K. Nagata, Int. J. Theor. Phys. **60**, 70 (2021)] using the principle of quantum mechanics. We demonstrate some evaluations of three two-variable functions which are elements of a boolean algebra composed of the four-atom set utilizing the Bernstein–Vazirani algorithm. This is faster than a classical apparatus, which would require $2^{12} = 4096$ evaluations. Finally, using the three two-variable functions evaluated here, we demonstrate two typical arithmetic calculations in the binary system. Hence, our calculations are faster than a classical apparatus, which would require $2^{12} = 4096$ evaluations.

PACS numbers: 03.67.Ac, 03.67.Lx, 03.65.Ca

Keywords: Quantum algorithms, Quantum computation, Formalism

## I. INTRODUCTION

Between the articles of research for constructing theoretical quantum algorithms [1] it may be mentioned as follows: In 1985, the Deutsch algorithm was introduced and constructed for the function property problem [2–4]. In 1993, the Bernstein–Vazirani algorithm was proposed for identifying linear functions [5, 6]. In 1994, Simon's algorithm [7] and Shor's algorithm [8] were discussed for period finding of periodic functions. In 1996, Grover [9] provided an algorithm for unordered object finding and the motivation for exploring the computational possibilities offered by quantum mechanics.

A simple algorithm for complete factorization of an $N$-partite pure quantum state is proposed by Mehendale and Joag [10]. Fujikawa, Oh, and Umetsu discuss a classical limit of Grover's algorithm induced by dephasing: coherence versus entanglement [11]. Quantum dialogue protocol based on Grover's search algorithms is presented by Yin, He, and Fan [12]. Some relations between a boolean algebra and quantum computing are discussed and proposed by Nagata and Nakamura. They show all the boolean functions are set into the quantum computer just like the electronic computer. This fact means that all performances in logic of computing and control of itself are available even in quantum computers. Therefore, we could design any quantum-gated computer using the traditional design ways in logic of existing electronic computers [13].

Further they prove that the quantum computer can operate just like the electronic computer fundamentally through the operation of addition of two $n$-digit numbers. Therefore, the quantum computer can solve all the four basic operations of arithmetic, addition, subtraction, multiplication, and division. Further it can be said that this quantum computer naturally operates not only arithmetic but also logic in terms of boolean logic [14]. As a result, the theory proposed by Refs. [13, 14] can build a very true quantum-gated computer that is driven and operated by all software (all programs) used on existing electronic computers. A quantum algorithm for a FULL adder operation based on registers of the CPU in a quantum-gated computer is disscussed [15]. Here, we point out how the argumentations are efficient when we compare our quantum computer with a classical apparatus.

A specific example is more understandable than the abstract structure when we study quantum computing theory. We investigate the concrete and specific example of the argumentations in Ref. [14]. Surprisingly, the concrete and specific calculation is faster than that of a classical apparatus, which would require $2^{12} = 4096$ evaluations when we introduce the full adder operation [16]. Another concrete and specific calculation is faster than that of a classical apparatus, which would require $2^8 = 256$ evaluations when we introduce only the half adder operation [16].

In this article, we study an efficiency for operating a full adder/half adder by quantum-gated computing. Fortunately, we have two typical arithmetic calculations in Ref. [14]. We demonstrate some evaluations of three two-variable functions which are elements of a boolean algebra composed of the four-atom set utilizing the Bernstein–Vazirani algorithm. This is faster than that of a classical apparatus, which would require $2^{12} = 4096$ evaluations. Using the three two-variable functions evaluated here, we demonstrate a typical arithmetic calculation in the binary system using the full adder operation. Surprisingly, the typical arithmetic calculation is faster than that of a classical apparatus, which would require $2^{12} = 4096$ evaluations when we introduce the full adder operation. Another typical arithmetic calculation is faster than that of a classical apparatus, which would require at least $2^8 = 256$ evaluations when we introduce only the half adder operation. The quantum advantage increases when two numbers we treat become very large.

## II. REVIEW OF THE BERNSTEIN–VAZIRANI ALGORITHM

Suppose that

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

is a function with an $N$-bit domain and a 1-bit range. We assume the following case:

$$f(x) = a \cdot x = \sum_{i=1}^{N} a_i x_i (\text{mod } 2) = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \cdots \oplus a_N x_N, \tag{2}$$

where $a \in \{0,1\}^N$. The goal is of determining $f(x)$. Here, the number of functions is $2^N$. The Bernstein–Vazirani algorithm determines what function is true by one step. Thus, the efficiency of the Bernstein–Vazirani algorithm is $2^N$. Let us follow the quantum states through the Bernstein–Vazirani algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle. \tag{3}$$

After the componentwise Hadamard transformations on the input state, we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{4}$$

Next, the function $f$ is evaluated using

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle \tag{5}$$

in giving, by the phase kickback formation,

$$|\psi_2\rangle = \pm \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^N}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{6}$$

Here $y \oplus f(x)$ is the bitwise XOR (exclusive OR) of $y$ and $f(x)$.

We have

$$H^{\otimes N}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}}, \tag{7}$$

where $x \cdot z$ is the bitwise inner product of $x$ and $z$, modulo 2.

Using (7) and (6), we can now evaluate $|\psi_3\rangle$

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^N} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{8}$$

Thus, we have

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + a\cdot x}|z\rangle}{2^N} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{9}$$

Notice that

$$\sum_x (-1)^{x\cdot z + a\cdot x} = 2^N \delta_{a,z}. \tag{10}$$

Thus, we have

$$\begin{aligned}
|\psi_3\rangle &= \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + a\cdot x}|z\rangle}{2^N} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \pm \sum_z \frac{2^N \delta_{a,z}|z\rangle}{2^N} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \pm |a\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \pm |a_1 a_2 a_3 \cdots a_N\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
\end{aligned} \tag{11}$$

Alice now observes $|a_1 a_2 a_3 \cdots a_N\rangle$. In summary, if Alice measures $|a_1 a_2 a_3 \cdots a_N\rangle$, then the function is

$$f(x_1, x_2, ..., x_N) = a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus \cdots \oplus a_N x_N. \tag{12}$$

This shows that the quantum algorithm is superior to its classical counterpart by a factor of $2^N$.

## III. QUANTUM ALGORITHM FOR STORING SIMULTANEOUSLY ALL THE MAPPINGS OF THREE LOGICAL FUNCTIONS

We introduce the following three logical functions [16]:

$$\begin{aligned}
f_1(x,y) &= A \wedge B, \\
f_6(x,y) &= \text{Exclusive OR}(A, B), \\
f_7(x,y) &= A \vee B,
\end{aligned} \tag{13}$$

for all $x$ and $y$, that is,

$$\begin{aligned}
&f_1(0,0)=0, f_1(0,1)=0, f_1(1,0)=0, f_1(1,1)=1,\\
&f_6(0,0)=0, f_6(0,1)=1, f_6(1,0)=1, f_6(1,1)=0,\\
&f_7(0,0)=0, f_7(0,1)=1, f_7(1,0)=1, f_7(1,1)=1.
\end{aligned} \tag{14}$$

We can construct a FULL adder operation using these three logical functions.

Suppose that

$$f:\{0,1\}^{12}\rightarrow\{0,1\} \tag{15}$$

is a function with a 12-bit domain and a 1-bit range. We assume the following function:

$$\begin{aligned}
&f(x)=a\cdot x=\sum_{i=1}^{12}a_i x_i (\mathrm{mod}\ 2)\\
&=f_1(0,0)x_1\oplus f_1(0,1)x_2\oplus f_1(1,0)x_3\oplus f_1(1,1)x_4\\
&\oplus f_6(0,0)x_5\oplus f_6(0,1)x_6\oplus f_6(1,0)x_7\oplus f_6(1,1)x_8\\
&\oplus f_7(0,0)x_9\oplus f_7(0,1)x_{10}\oplus f_7(1,0)x_{11}\oplus f_7(1,1)x_{12},
\end{aligned} \tag{16}$$

where $a_i\in\{0,1\}$, $x_i\in\{0,1\}$, $x=x_1x_2...x_{12}\in\{0,1\}^{12}$, and

$$\begin{aligned}
&a=a_1a_2...a_{12}\\
&=f_1(0,0)f_1(0,1)f_1(1,0)f_1(1,1)f_6(0,0)f_6(0,1)f_6(1,0)f_6(1,1)f_7(0,0)f_7(0,1)f_7(1,0)f_7(1,1)\in\{0,1\}^{12}.
\end{aligned} \tag{17}$$

The string

$$a_1,a_2,a_3,a_4 \tag{18}$$

corresponds to

$$f_1(0,0),f_1(0,1),f_1(1,0),f_1(1,1), \tag{19}$$

respectively. The string

$$a_5,a_6,a_7,a_8 \tag{20}$$

corresponds to

$$f_6(0,0),f_6(0,1),f_6(1,0),f_6(1,1), \tag{21}$$

respectively. The string

$$a_9,a_{10},a_{11},a_{12} \tag{22}$$

corresponds to

$$f_7(0,0),f_7(0,1),f_7(1,0),f_7(1,1), \tag{23}$$

respectively. Here, $x\oplus y$ is the bitwise XOR (exclusive OR) of $x$ and $y$. Also, $a\cdot x$ is the bitwise inner product of $a$ and $x$, modulo 2. The goal is of storing the logical functions $f_1(x,y)$, $f_6(x,y)$, and $f_7(x,y)$ in a boolean algebra for all $x$ and $y$ into an output quantum state as the coefficients of $f(x)$. Let us follow the quantum states through the Bernstein–Vazirani algorithm.

The input state is

$$|\psi_0\rangle=|0\rangle^{\otimes 12}|1\rangle. \tag{24}$$

After the componentwise Hadamard transformations on the state (24), we have

$$|\psi_1\rangle=\sum_{x\in\{0,1\}^{12}}\frac{|x\rangle}{\sqrt{2^{12}}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{25}$$

Next, the function $f$ is stored into a quantum state using

$$U_f|x,y\rangle=|x,y\oplus f(x)\rangle \tag{26}$$

in giving, by the phase kickback formation,

$$|\psi_2\rangle = \pm \sum_{x\in\{0,1\}^{12}} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^{12}}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{27}$$

After the componentwise Hadamard transformations on the first 12 qubits in the state $|\psi_2\rangle$, we can now evaluate $|\psi_3\rangle$

$$|\psi_3\rangle = \pm \sum_{z\in\{0,1\}^{12}} \sum_{x\in\{0,1\}^{12}} \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{2^{12}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{28}$$

where $z_i \in \{0,1\}$ and $z = z_1 z_2 ... z_{12} \in \{0,1\}^{12}$. Using $f(x) = a \cdot x$, we have

$$|\psi_3\rangle = \pm \sum_{z\in\{0,1\}^{12}} \sum_{x\in\{0,1\}^{12}} \frac{(-1)^{x\cdot z+a\cdot x}|z\rangle}{2^{12}} \frac{|0\rangle - |1\rangle}{\sqrt{12}}. \tag{29}$$

Notice that

$$\sum_{x\in\{0,1\}^{12}} (-1)^{x\cdot z+a\cdot x} = 2^{12}\delta_{a,z}. \tag{30}$$

Thus, we have

$$\begin{aligned}
|\psi_3\rangle &= \pm \sum_{z\in\{0,1\}^{12}} \sum_{x\in\{0,1\}^{12}} \frac{(-1)^{x\cdot z+a\cdot x}|z\rangle}{2^{12}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \pm \sum_{z\in\{0,1\}^{12}} \frac{2^{12}\delta_{a,z}|z\rangle}{2^{12}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \pm |a_1 ... a_{12}\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \pm |f_1(0,0)f_1(0,1)f_1(1,0)f_1(1,1)\rangle \otimes |f_6(0,0)f_6(0,1)f_6(1,0)f_6(1,1)\rangle \\
&\otimes |f_7(0,0)f_7(0,1)f_7(1,0)f_7(1,1)\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
\end{aligned} \tag{31}$$

Thus, in summary, we store $f_1$, $f_6$, and $f_7$ into a single quantum state as

$$|f_1(0,0)f_1(0,1)f_1(1,0)f_1(1,1)\rangle \otimes |f_6(0,0)f_6(0,1)f_6(1,0)f_6(1,1)\rangle \otimes |f_7(0,0)f_7(0,1)f_7(1,0)f_7(1,1)\rangle \tag{32}$$

and the results of measurements are

$$\begin{aligned}
&f_1(0,0) = 0, f_1(0,1) = 0, f_1(1,0) = 0, f_1(1,1) = 1, \\
&f_6(0,0) = 0, f_6(0,1) = 1, f_6(1,0) = 1, f_6(1,1) = 0, \\
&f_7(0,0) = 0, f_7(0,1) = 1, f_7(1,0) = 1, f_7(1,1) = 1.
\end{aligned} \tag{33}$$

According to the first supposition, we are succeeding to store correctly them.

In classical case we require $2^{12} = 4096$ steps. In quantum case here we require just only one step.

## IV. TYPICAL ARITHMETIC CALCULATIONS

We have used the Bernstein–Vazirani algorithm with the usual phase kickback formation to develop the overbridging between usual quantum mechanics (and then quantum computing) and a boolean algebra. In this, we have confirmed that usual quantum operations are useful, beyond the quantum computing only for quantum mechanics operations, for mathematical evaluations just like an arithmetic operation. We demonstrate two typical arithmetic calculations in the binary system.

As an example of a simple addition 1 + 1 in the binary system, we are going to develop the process of how to calculate this:

To solve it, fortunately we have a formula here

$$f_6(x,y) = \text{Exclusive OR}(A,B). \tag{34}$$

$$f_1(x,y) = A \wedge B. \tag{35}$$

$$1 + 1 = ?? \tag{36}$$
$$\text{Sum} = \text{Exclusive OR}(1, 1) = 0. \tag{37}$$
$$\text{Carry} = 1 \wedge 1 = 1. \tag{38}$$

Hence we have very clearly

$$1 + 1 = 10 \tag{39}$$

according to the algorithm for addition in the binary system. The concrete and specific calculation (1+1) is faster than that of a classical apparatus, which would require $2^8 = 256$ steps when we introduce only the half adder operation.

In more details, we must use the rule of a half adder that is composed of by using some formulae in the boolean algebra [16]. In the half adder, the function of it is the SUM and a Carry to the next digit position. The circuit consists of two boolean functions (37) and (38).

Further, we could mention a little bit complicated example. It is $2 + 3$ in the decimal system.

In addition of the half adder operation, we need one more operation the full adder [16]. As for the full adder, it is by the two half adders and the "OR" operation $A \vee B$ $(A, B \in \{0, 1\})$ in the boolean algebra to take out the result from the previous digit. The operation is left here because it is obvious mathematically. Anyhow we can obtain the result 5 in the decimal system.

To solve it, fortunately we have a formula here

$$f_6(x, y) = \text{Exclusive OR}(A, B). \tag{40}$$
$$f_1(x, y) = A \wedge B. \tag{41}$$
$$f_7(x, y) = A \vee B. \tag{42}$$

$$10 + 11 = ??? \tag{43}$$
$$\text{Sum} = \text{Exclusive OR}(0, 1) = 1. \tag{44}$$
$$\text{Carry} = 0 \wedge 1 = 0. \tag{45}$$

Thus we have

$$10 + 11 = ??1. \tag{46}$$

Also we see

$$\text{Carry C}_\text{i} = 0. \tag{47}$$

Our second aim is of calculating $1 + 1$ considering Carry $\text{C}_\text{i} = 0$ by using a full adder. The first half adder says

$$\text{Exclusive OR}(1, 1) = 0. \tag{48}$$
$$\text{Carry} = 1 \wedge 1 = 1. \tag{49}$$

The second half adder says

$$\text{Sum} = \text{Exclusive OR}(\text{Carry C}_\text{i}, \text{Exclusive OR}(1, 1)) = 0. \tag{50}$$
$$\text{Carry} = \text{Carry C}_\text{i} \wedge \text{Exclusive OR}(1, 1) = 0. \tag{51}$$

Thus we see $10 + 11 = ?01$. We have finally the carry Carry $\text{C}_0$ as follows: (This is (49) $\vee$ (51)).

$$\text{Carry C}_0 = 0 \vee 1 = 1. \tag{52}$$

Hence we have very clearly

$$10 + 11 = 101 \tag{53}$$

according to the algorithm for addition in the binary system. The concrete and specific calculation $(2 + 3)$ is faster than that of a classical apparatus, which would require $2^{12} = 4096$ steps when we introduce the full adder operation. The quantum advantage increases when two numbers we treat become very large. Toward practical quantum-gated computers, experimental demonstrations of our argumentations are going to be interested.

## V. CONCLUSIONS AND DISCUSSIONS

In conclusion, we have studied an efficiency for operating a full adder/half adder by quantum-gated computing. Fortunately, we have had two typical arithmetic calculations in Ref. [14]. We have demonstrated some evaluations of three two-variable functions which are elements of a boolean algebra composed of the four-atom set utilizing the Bernstein-Vazirani algorithm. This has been faster than that of a classical apparatus, which would require $2^{12} = 4096$ evaluations. Using the three two-variable functions evaluated here, we have demonstrated a typical arithmetic calculation in the binary system using the full adder operation. Surprisingly, the typical arithmetic calculation has been faster than that of a classical apparatus, which would require $2^{12} = 4096$ evaluations when we introduce the full adder operation. Another typical arithmetic calculation has been faster than that of a classical apparatus, which would require at least $2^8 = 256$ evaluations when we introduce only the half adder operation. The quantum advantage has increased when two numbers we treat become very large. Toward practical quantum-gated computers, experimental demonstrations of our argumentations have been going to be interested.

## NOTE

On behalf of all authors, the corresponding author states that there is no conflict of interest.

## ACKNOWLEDGMENTS

We thank Soliman Abdalla, Jaewook Ahn, Josep Batle, Mark Behzad Doost, Ahmed Farouk, Han Geurdes, Shahrokh Heidari, Wenliang Jin, Hamed Daei Kasmaei, Janusz Milek, Mosayeb Naseri, Santanu Kumar Patro, Germano Resconi, and Renata Wong for valuable support.

---

[1] R. Rennie (Editor), *Oxford dictionary of physics* (Oxford University Press, 2015), Seventh ed.

[2] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer. Proc. R. Soc. Lond. A **400**, 97 (1985). https://doi.org/10.1098/rspa.1985.0070

[3] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation. Proc. R. Soc. Lond. A **439**, 553 (1992). https://doi.org/10.1098/rspa.1992.0167

[4] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Quantum algorithms revisited. Proc. R. Soc. Lond. A **454**, 339 (1998). https://doi.org/10.1098/rspa.1998.0164

[5] E. Bernstein and U. Vazirani, Quantum complexity theory. Proceedings of 25th Annual ACM Symposium on Theory of Computing (STOC '93), p. 11 (1993). https://doi.org/10.1145/167088.167097

[6] E. Bernstein and U. Vazirani, Quantum Complexity Theory. SIAM J. Comput. **26**, 1411 (1997). https://doi.org/10.1137/S0097539796300921

[7] D. R. Simon, On the power of quantum computation. Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, p. 116 (1994). https://doi.org/10.1109/SFCS.1994.365701

[8] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, p. 124 (1994). https://doi.org/10.1109/SFCS.1994.365700

[9] L. K. Grover, A fast quantum mechanical algorithm for database search. Proceedings of 28th Annual ACM Symposium on Theory of Computing, p. 212 (1996). https://doi.org/10.1145/237814.237866

[10] D. P. Mehendale and P. S. Joag, A Simple Algorithm for Complete Factorization of an $N$-Partite Pure Quantum State. Quantum Physics Letters, Vol. 6, No. 1, 73 (2017). https://doi.org/10.18576/qpl/060110

[11] K. Fujikawa, C. H. Oh, and K. Umetsu, A classical limit of Grover's algorithm induced by dephasing: Coherence versus entanglement. Modern Physics Letters A, Vol. 34, No. 07n08, 1950146 (2019). https://doi.org/10.1142/S0217732319501463

[12] A. Yin, K. He, and P. Fan, Quantum dialogue protocol based on Grover's search algorithms. Modern Physics Letters A, Vol. 34, No. 21, 1950169 (2019). https://doi.org/10.1142/S0217732319501694

[13] K. Nagata and T. Nakamura, Some Theoretically Organized Algorithm for Quantum Computers. Int. J. Theor. Phys. **59**, 611 (2020). https://doi.org/10.1007/s10773-019-04354-7

[14] T. Nakamura and K. Nagata, Physics' Evolution Toward Computing. Int. J. Theor. Phys. **60**, 70 (2021). https://doi.org/10.1007/s10773-020-04661-4

[15] K. Nagata and T. Nakamura, A quantum algorithm for a FULL adder operation based on registers of the CPU in a quantum-gated computer. Int. J. Theor. Phys. **60**, 2986 (2021). https://doi.org/10.1007/s10773-021-04894-x

[16] W. J. Gilbert and W. K. Nicholson, *Modern algebra with applications* (John Wiley and Sons, Inc. Second edition, 2004).