International Journal of Theoretical Physics (2019) 58: 136–142
https://doi.org/10.1007/s10773-018-3917-x

Necessary and Sufficient Condition for Quantum Computing

Koji Nagata[1] · Tadao Nakamura[2] · Ahmed Farouk[3] · Do Ngoc Diep[4,5]

Received: 1 June 2018 / Accepted: 5 October 2018 / Published online: 11 October 2018

Abstract
A necessary and sufficient condition for quantum computing performed with, for example, the Deutsch-Jozsa algorithm or the Bernstein-Vazirani algorithm, has theoretically been investigated. Assume a $2N$ qubit-quantum computing which starts with the state $|\overbrace{0, 0, ..., 0, 1}^{N}\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle$ as follows: $U_f|0, 0, ..., 0, 1\rangle|1, 1, ..., 1\rangle = |0, 0, ..., 0, 1\rangle|\overline{f(0, 0, ..., 0, 1)}\rangle$. Surprisingly the relation $f(x) = f(-x)$ is the necessary and sufficient condition of holding this fundamental relation if local unitary operations can be used.

Keywords Quantum algorithms · Quantum computation

1 Introduction

Quantum computing is explained as follows [1]: —The design and theory of computer systems that depend on quantum effects for their operation. On one level, this can be the use of small components, at the atomic or molecular level, to store or process information. An example would be a storage system that used two different spin states of atoms to store bits of information, or a logic gate that depends on the movement or spin of a single electron. Systems of this type are studied in nanocomputing. At a more fundamental level, the term 'quantum computing' implies the use of quantum effects that have no classical analogue to process information. In a 'classical' computer information is held in bits, which can have two alternative values (0 and 1). In a quantum computer the 0 and 1 values are held simultaneously in a superposition state. This unit of information is called a quantum bit (or qubit).

✉ Koji Nagata
ko_mi_na@yahoo.co.jp

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 Department of Physics and Computer Science, Faculty of Science, Wilfrid Laurier University, Waterloo, Canada

4 TIMAS, Thang Long University, Nghiem Xuan Yem road, Hoang Mai district, Hanoi, Vietnam

5 Institute of Mathematics, VAST, 18 Hoang Quoc Viet road, Cau Giay district, Hanoi, Vietnam

Much more information can be held in this way and, in principle, it is possible to do parallel processing of the information. Quantum computers would be much faster than conventional machines and capable of performing calculations that could not realistically be done otherwise. Ion traps, cavity QED, and spin measurements have been used in research in this area.

Articles on the history of research into quantum computing are mentioned as follows. An implementation of a quantum algorithm to solve Deutsch's problem [2–4] on a nuclear magnetic resonance quantum computer is reported [5]. An implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is reported [6]. Oliveira et al. implements Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [7]. A single-photon Bell states are prepared and measured [8]. The decoherence-free implementation of Deutsch's algorithm is introduced by using such a single-photon and by using two logical qubits [9]. A one-way based experimental implementation of Deutsch's algorithm is reported [10].

In 1993, the Bernstein-Vazirani algorithm was published [11, 12]. By utilizing a Boolean-valued function, it is extended to determine the values of the function [13]. In 1994, Simon's algorithm [14] and Shor's algorithm [15] were discussed. In 1996, Grover [16] provided the motivation for exploring the computational possibilities offered by quantum mechanics. An implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement in an ensemble quantum computer is mentioned [17]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits is discussed [18]. The question whether or not quantum learning is robust against noise is a subject of a study [19].

A quantum algorithm for approximating the influences of Boolean functions and its applications are studied [20]. Quantum computation with coherent spin states and the close Hadamard problem are reported [21]. Transport implementation of the Bernstein-Vazirani algorithm with ion qubits is studied [22]. Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers are discussed [23]. The dynamical analysis of Grover's search algorithm in arbitrarily high-dimensional search spaces is studied [24]. A method of computing many functions simultaneously by using many parallel quantum systems is reported [25]. An algorithm for fast determining a homogeneous linear function is proposed [26]. A method of calculating a multiplication by using the generalized Bernstein-Vazirani algorithm is studied [27]. A new mathematical structure for quantum algorithms in case of a special function is reported [28]. Efficient quantum algorithm for the parity problem of a certain function is given [29].

In 2015, it was discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [30]. In 2017, it was discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [31]. A highly speedy secure quantum cryptography based on the Deutsch-Jozsa algorithm is proposed [32]. The relation between quantum computer and secret sharing with the use of quantum principles is discussed [33]. An application of quantum Gauss-Jordan elimination code to quantum secret sharing code is studied [34]. Designing quantum circuit by one step method and similarity with neural network are discussed [35]. Efficient quantum algorithms of finding the roots of a polynomial function are discussed [36, 37].

There are many researches concerning quantum computing, quantum algorithm, and their experiments. However, a complete understanding of a fundamental structure of quantum computing is not given. There is a meaningful motivation of looking for a condition of obtaining the success of a quantum computing experiment. Namely, it is useful for experimental investigations for judging if the experiments are success. For example, the

Bernstein-Vazirani algorithm in a noisy environment is studied [22, 31] and a success probability is given. Here an all-versus-nothing theorem is investigated.

Assume a $2N$ qubit-quantum computing which starts with the state $|\overbrace{0, 0, ..., 0, 1}^{N}\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle$ as follows: $U_f|0, 0, ..., 0, 1\rangle|1, 1, ..., 1\rangle = |0, 0, ..., 0, 1\rangle|\overline{f(0, 0, ..., 0, 1)}\rangle$. Recently, it is shown that the relation $f(x) = f(-x)$ is a necessary condition of holding this fundamental relation of quantum computing performed with, for example, the Deutsch-Jozsa algorithm or the Bernstein-Vazirani algorithm if we assume $|-x\rangle = -|x\rangle$ [28, 29]. It is interesting to study whether the relation $f(x) = f(-x)$ is also a sufficient condition.

In this contribution, a necessary and sufficient condition for quantum computing is proposed. Surprisingly the relation $f(x) = f(-x)$ is the necessary and sufficient condition of holding this fundamental relation if local unitary operations can be used. A quantum algorithm (computing) experiment is success if $f(x) = f(-x)$, otherwise the experiment is not success.

The argumentations for finding this evenness: $f(x) = f(-x)$ of the function $f(x)$ is assumed to a practical use in combination together with quantum error correction algorithms for qubits/qudits (or even topological anyons in topological quantum error correction). See [38] and [39]. After an error correction the problem is protected from any kinds of bit flip or spin flip actions and the argumentations work well.

The rest of the paper is organized as follows:

In Section 2, a necessary and sufficient condition for quantum computing is given. Finally, the conclusion is drawn in Section 3.

2 A Necessary and Sufficient Condition for Quantum Computing

In this section, a necessary and sufficient condition for quantum computing is proposed. Assume $|-x\rangle = -|x\rangle$. This is realized as follows:

- Prepare $|-x\rangle$.
- Introduce the flip operator $\sigma_x = |-x\rangle\langle x| + |x\rangle\langle -x|$.
- Notice $\sigma_x|-x\rangle = |x\rangle$.
- Operate $-I$ to $|x\rangle$ in giving $-|x\rangle$.

Notice

- Prepare $-|x\rangle$.
- Introduce the flip operator $\sigma_x = |-x\rangle\langle x| + |x\rangle\langle -x|$.
- Notice $\sigma_x(-|x\rangle) = -|-x\rangle$.
- Operate $-I$ to $-|-x\rangle$ in giving $|-x\rangle$.

Therefore, transformations $|-x\rangle$ to $-|x\rangle$ and $-|x\rangle$ to $|-x\rangle$ are realised by using local unitary operations. In the following, local unitary operations can be used in order to justify the assumption $|-x\rangle = -|x\rangle$. Roughly speaking, the entire argumentations are held under the assumption that local unitary operations can be used.

Assume that the following function is given

$$f : \{-(2^N - 1), -(2^N - 2), \ldots, 2^N - 2, 2^N - 1\} \rightarrow \{0, 1, \ldots, 2^N - 2, 2^N - 1\}. \quad (1)$$

Assume that $f(y) \geq 0$. Introduce a function $g(x)$ that transforms binary strings into an integer. Define $g^{-1}(f(g(x))) = F(x)$. The construction of $F(x)$ is independent of the choice of the function g. Assume such a function $F(x)(= g^{-1}(f(g(x))))$ and such a function g indeed exist, for example to make precise, choose the function g such that for any string $x = (x_N, \ldots, x_0)$, $g(x) = x_N 2^N + \cdots + x_1 2^1 + x_0$. This function g is invertible and g^{-1} converts the integer $x = x_N 2^N + \cdots + x_1 2^1 + x_0$ back to the bit-string $(x_N, \ldots, x_1, x_0)$. $y = g(x)$ is the integer representation of the binary string x. For example, $x = (1, 1)$ if $y = 3$. Assume that the given function f is even. Namely,

$$F(x) = F(-x) \in \{0, 1\}^N, \tag{2}$$

where $x \in \{0, 1\}^N$. The condition (2) is a sufficient condition for quantum computing as shown below.

What the function $f(x)$ does in (1) is to map a set of discrete values onto another one. In (2), assume that x is the binary representation of an integer. x will be given by a binary string belonging to the Cartesian product $\overbrace{\{0, 1\} \times \{0, 1\} \times \ldots \times \{0, 1\}}^{N}$, for instance, $x = (0, 1, 1, 0, 0, 1, \ldots, 1)$. Define $-x$ as $-(0, 1, 1, 0, 0, 1, \ldots, 1)$.

Throughout the discussion, any normalization factors are omitted. The input state is

$$|\psi_1\rangle = |\overbrace{0, 0, \ldots, 0, 1}^{N}\rangle|\overbrace{1, 1, \ldots, 1}^{N}\rangle. \tag{3}$$

The function F is evaluated by using the following unitary $2N$ qubit gate

$$U_F : |x, z\rangle \rightarrow |x, z + F(x)\rangle \tag{4}$$

with

$$\begin{aligned} U_F : \quad & |x, z\rangle \rightarrow |x, z + F(x)\rangle \\ \Leftrightarrow\ & -|x, z\rangle \rightarrow -|x, z + F(x)\rangle \\ \Leftrightarrow\ & |-x, z\rangle \rightarrow |-x, z + F(x)\rangle \\ \Leftrightarrow\ & |-x, z\rangle \rightarrow |-x, z + F(-x)\rangle \end{aligned} \tag{5}$$

employing the fact that $F(x) = F(-x)$. Here, $z + F(x) = (z_1 \oplus F_1(x), z_2 \oplus F_2(x), \ldots, z_N \oplus F_N(x))$ (the symbol $\oplus$ indicates addition modulo 2). And, $\overline{F(x)} = (1 \oplus F_1(x), 1 \oplus F_2(x), \ldots, 1 \oplus F_N(x))$. For example, $F(0, 0, ..., 0, 1) = (0, 1, 1, 0, 0, 1, \ldots, 1)$ if $\overline{F(0, 0, ..., 0, 1)} = (1, 0, 0, 1, 1, 0, \ldots, 0)$.

The state $|\psi_1\rangle$ (3) can be decomposed as follows:

$$|\psi_1\rangle = \sum_{x=-(2^N-1)}^{-2} |x\rangle|\overbrace{1, 1, \ldots, 1}^{N}\rangle + \sum_{x=+1}^{2^N-1} |x\rangle|\overbrace{1, 1, \ldots, 1}^{N}\rangle. \tag{6}$$

Start the discussion from the following

$$\begin{aligned} & U_F|\psi_1\rangle = |\psi_2\rangle \\ & = \sum_{x=-(2^N-1)}^{-2} |x\rangle|\overline{F(x)}\rangle + \sum_{x=+1}^{2^N-1} |x\rangle|\overline{F(x)}\rangle \end{aligned} \tag{7}$$

and

$$|\psi_2\rangle = \sum_{x=-(2^N-1)}^{-2} |x\rangle|\overline{F(x)}\rangle + \sum_{x=+1}^{2^N-1} |x\rangle|\overline{F(x)}\rangle. \tag{8}$$

This implies for $x \to -x$, with $x \neq 0$ to the first term;

$$|\psi_2\rangle = \sum_{x=+2}^{2^N-1} |-x\rangle|\overline{F(-x)}\rangle + \sum_{x=+1}^{2^N-1} |x\rangle|\overline{F(x)}\rangle. \tag{9}$$

Therefore, using $\overline{F(x)} = \overline{F(-x)}$;

$$|\psi_2\rangle = \sum_{x=+2}^{2^N-1} |-x\rangle|\overline{F(x)}\rangle + \sum_{x=+1}^{2^N-1} |x\rangle|\overline{F(x)}\rangle. \tag{10}$$

Therefore, using $|-x\rangle = -|x\rangle$;

$$|\psi_2\rangle = -\sum_{x=+2}^{2^N-1} |x\rangle|\overline{F(x)}\rangle + \sum_{x=+1}^{2^N-1} |x\rangle|\overline{F(x)}\rangle. \tag{11}$$

Thus, the terms except for $x = 1$ cancel;

$$|\psi_2\rangle = |0, 0, \ldots, 0, 1\rangle|\overline{F(0, 0, \ldots, 0, 1)}\rangle. \tag{12}$$

The following fundamental relation in quantum computing is derived.

$$\begin{aligned} &U_F|\overbrace{0, 0, ..., 0, 1}^{N}\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle \\ &= |\overbrace{0, 0, ..., 0, 1}^{N}\rangle|\overline{F(0, 0, ..., 0, 1)}\rangle. \end{aligned} \tag{13}$$

Therefore, the relation $F(x) = F(-x)$ is a sufficient condition for the fundamental relation (13). The relation $F(x) = F(-x)$ is also a necessary condition for the fundamental relation (13) as shown below [28, 29].

From the definition in (5), notice

$$U_F|x\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle = |x\rangle|\overline{F(x)}\rangle. \tag{14}$$

This implies for $x \to -x$, with $x \neq 0$

$$U_F|-x\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle = |-x\rangle|\overline{F(-x)}\rangle. \tag{15}$$

Assume $|-x\rangle = -|x\rangle$. It follows that the minus sign on the left and right hand sides of (15) drops off. This implies

$$U_F|x\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle = |x\rangle|\overline{F(-x)}\rangle. \tag{16}$$

Assume such that

$$|P\rangle = |Q\rangle \Leftrightarrow P = Q. \tag{17}$$

Comparing (14) with (16), notice $|\overline{F(x)}\rangle = |\overline{F(-x)}\rangle$. Hence, the following property of the function in order to maintain a consistency for the fundamental relation (13) cannot be avoided.

$$\overline{F(x)} = \overline{F(-x)}. \tag{18}$$

The fact that the function under study is even is derived.

$$F(x) = F(-x). \tag{19}$$

Thus the relation $F(x) = F(-x)$ is a necessary condition for the fundamental relation (13).

It is indeed surprise to show the relation $f(x) = f(-x)$ is the necessary and sufficient condition of holding this fundamental relation if local unitary operations can be used. Again, a quantum algorithm (computing) experiment is success if $f(x) = f(-x)$, otherwise the experiment is not success. It is the all-versus-nothing theorem.

A quantum algorithm does not distinguish $f(-x)$ from $f(x)$. In other words, the minus sign does not change anything in the outcome of the quantum algorithm. This fact is due to the Galilean transformation that changes the Cartesian coordinate from x to $-x$. The non-relativistic quantum theory are invariant under the Galilean transformation. The all-versus-nothing theorem is explained as follows: the quantum algorithms is invariant under the Galilean transformation.

3 Conclusions

In conclusion, a necessary and sufficient condition for quantum computing has been proposed. Assume a $2N$ qubit-quantum computing which starts with the state $|\overbrace{0, 0, ..., 0, 1}^{N}\rangle|\overbrace{1, 1, ..., 1}^{N}\rangle$ as follows: $U_f|0, 0, ..., 0, 1\rangle|1, 1, ..., 1\rangle = |0, 0, ..., 0, 1\rangle |\overline{f(0, 0, ..., 0, 1)}\rangle$. Surprisingly the relation $f(x) = f(-x)$ has been the necessary and sufficient condition of holding this fundamental relation if local unitary operations can be used.

Acknowledgements We thank Professor Han Geurdes, Professor Shahrokh Heidari, Professor Hamed Daei Kasmaei, and Professor Mark Behzad Doost for valuable comments.

References

1. Rennie, R. (ed.): Oxford dictionary of physics, 7th. Oxford University Press, Oxford (2015)
2. Deutsch, D.: Soc, Proc. Roy. London Ser. A **400**, 97 (1985)
3. Deutsch, D., Jozsa, R.: Proc. Roy. Soc. London Ser. A **439**, 553 (1992)
4. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Proc. Roy. Soc. London Ser. A **454**, 339 (1998)
5. Jones, J.A., Mosca, M.: J. Chem. Phys. **109**, 1648 (1998)
6. Gulde, S., Riebe, M., Lancaster, G.P.T., Becher, C., Eschner, J., Häffner, H., Schmidt-Kaler, F., Chuang, I.L., Blatt, R.: Nat. (London) **421**, 48 (2003)
7. de Oliveira, A.N., Walborn, S.P., Monken, C.H.: J. Opt. B: Quantum Semiclass. Opt. **7**, 288–292 (2005)
8. Kim, Y.-H.: Rev, Phys. A **67**(R), 040301 (2003)
9. Mohseni, M., Lundeen, J.S., Resch, K.J., Steinberg, A.M.: Phys. Rev. Lett. **91**, 187903 (2003)
10. Tame, M.S., Prevedel, R., Paternostro, M., Böhi, P., Kim, M.S., Zeilinger, A.: Phys. Rev. Lett. **98**, 140501 (2007)
11. Bernstein, E., Vazirani, U.: In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC '93), pp. 11–20 (1993)
12. Bernstein, E., Vazirani, U.: SIAM J. Comput. **26-5**, 1411–1473 (1997)
13. Nagata, K., Resconi, G., Nakamura, T., Batle, J., Abdalla, S., Farouk, A.: MOJ Ecol Environ Sci **2**(1), 00010 (2017)
14. Simon, D.R.: Foundations of computer science. In: Proceedings 35th Annual Symposium on: 116-123, retrieved 2011-06-06 (1994)

15. Shor, P.W.: In: Proceedings of the 35th IEEE Symposium on Foundations of computer science, p. 124 (1994)
16. Grover, L.K.: In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing, p. 212 (1996)
17. Du, J., Shi, M., Zhou, X., Fan, Y., Ye, B.J., Han, R., Wu, J.: Phys. Rev. A **64**, 042306 (2001)
18. Brainis, E., Lamoureux, L.-P., Cerf, N.J., Emplit, P.h., Haelterman, M., Massar, S.: Phys. Rev. Lett. **90**, 157902 (2003)
19. Cross, A.W., Smith, G., Smolin, J.A.: Phys. Rev. A **92**, 012327 (2015)
20. Li, H., Yang, L.: Quantum Inf. Process. **14**, 1787 (2015)
21. Adcock, M.R.A., Hoyer, P., Sanders, B.C.: Quantum Inf. Process. **15**, 1361 (2016)
22. Fallek, S.D., Herold, C.D., McMahon, B.J., Maller, K.M., Brown, K.R., Amini, J.M.: New J. Phys. **18**, 083030 (2016)
23. Diep, D.N., Giang, D.H., Van Minh, N.: Int. J. Theor. Phys. **56**, 1948 (2017)
24. Jin, W.: Quantum Inf. Process. **15**, 65 (2016)
25. Nagata, K., Resconi, G., Nakamura, T., Batle, J., Abdalla, S., Farouk, A., Geurdes, H.: Asian J. Math. Phys. **1**(1), 1–4 (2017)
26. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Abdalla, S., Farouk, A., Diep, D.N.: Int. J. Theor. Phys. **57**, 973 (2018)
27. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Abdalla, S., Farouk, A.: Int. J. Theor. Phys. **57**, 1605 (2018)
28. Nagata, K., Nakamura, T.: J Sci Eng Res **5**(3), 326–328 (2018)
29. Nagata, K., Nakamura, T., Batle, J., Farouk, A.: Int. J. Theor. Phys. **57**, 3098 (2018)
30. Nagata, K., Nakamura, T.: Open Access Library J. **2**, e1798 (2015)
31. Nagata, K., Nakamura, T.: Int. J. Theor. Phys. **56**, 2086 (2017)
32. Nagata, K., Nakamura, T., Farouk, A.: Int. J. Theor. Phys. **56**, 2887 (2017)
33. Diep, D.N., Giang, D.H.: Int. J. Theor. Phys. **56**, 2797 (2017)
34. Diep, D.N., Giang, D.H., Phu, P.H.: Int. J. Theor. Phys. **57**, 841 (2018)
35. Resconi, G., Nagata, K.: Intern. J. Gen. Eng. Technol. **7**(1), 1–20 (2018)
36. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Farouk, A., Diep, D.N., Patro, S.K.: Int. J. Theor. Phys. **57**, 2546 (2018)
37. Nagata, K., Nakamura, T.: Quantum algorithm for the root-finding problem, Quantum Stud.: Math. Found. https://doi.org/10.1007/s40509-018-0171-0 (2018)
38. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge University Press, Cambridge (2000)
39. Devitt, S.J., Munro, W.J., Nemoto, K.: Rep. Prog. Phys. **76**, 076001 (2013)