Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(3):326-328**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

A New Mathematical Structure for Quantum Algorithms in Case of a Special Function

Koji Nagata[1], Tadao Nakamura[2]

[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

Abstract In this short contribution, we discuss a new mathematical structure for standard quantum algorithms. They say a certain property in case of a special function f that the relation $f(x) = f(-x)$ holds.

PACS numbers: 03.67.Ac, 03.67.Lx

Keywords Quantum algorithms, Quantum computation

1. Introduction

In 1985, the Deutsch-Jozsa algorithm was discussed [1, 2, 3]. In 1993, the Bernstein-Vazirani algorithm was published [4, 5]. This work can be considered an extension of the Deutsch-Jozsa algorithm. 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.

In this short contribution, we discuss a new mathematical structure for standard quantum algorithms. They say a certain property in case of a special function f that the relation $f(x) = f(-x)$ holds.

2. Mathematical structure for standard quantum algorithms

We discuss a new mathematical structure for standard quantum algorithms in case of a special function f.

Let us suppose that we are given the following function

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

We shall assume that $f(y)\geq 0$.

Let us introduce a function $g(x)$ that transforms binary strings into positive integers. We also define $g^{-1}(f(g(x))) = F(x)$. We shall assume, for the time being, that the given function is even. Thus, we have

$$\begin{aligned} F(x) &= F(-x)\in\{0,1\}^N \\ x &\in\{0,1\}^N. \end{aligned} \tag{2}$$

We see that the condition (2) holds in standard quantum algorithms.

What the function $f(x)$ does in (1) is to map a set of discrete values onto another one. In (2), we assume that x is the binary representation of one element. 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, $x=(0,1,1,0,0,1,\ldots,1)$. We then define $-x$ as $-(0,1,1,0,0,1,\ldots,1)$.

Throughout the discussion, we omit any normalization factor. Let us suppose $|-x\rangle = -|x\rangle$. 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 $2N$ qubits gate

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

with

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

and 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).

We have the following fact

$$\begin{aligned} &U_F|\overbrace{0,0,...,0,1}^{N}\rangle|\overbrace{1,1,...,1}^{N}\rangle \\ &=|\overbrace{0,0,...,0,1}^{N}\rangle|\overline{F(0,0,...,0,1)}\rangle. \end{aligned} \tag{6}$$

Here, for example, if we have $F(0,0,...,0,1)=(0,1,1,0,0,1,\ldots,1)$, then $\overline{F(0,0,...,0,1)}=(1,0,0,1,1,0,\ldots,0)$.

Surprisingly the relation $F(x)=F(-x)$ is necessary for the fundamental relation (6) as shown below.

From the definition in (??), we have

$$U_F|x\rangle|\overbrace{1,1,...,1}^{N}\rangle = |x\rangle|\overline{F(x)}\rangle. \tag{7}$$

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

$$U_F|-x\rangle|\overbrace{1,1,...,1}^{N}\rangle = |-x\rangle|\overline{F(-x)}\rangle. \tag{8}$$

We state that $|-x\rangle = -|x\rangle$. Then it follows that the minus sign on left and right hand side of (8) drop off. This implies

$$U_F|x\rangle|\overbrace{1,1,...,1}^{N}\rangle = |x\rangle|\overline{F(-x)}\rangle. \tag{9}$$

We furthermore assume such that

$$|P\rangle = |Q\rangle \Leftrightarrow P=Q. \tag{10}$$

Comparing (7) with (9) we see $|\overline{F(x)}\rangle = |\overline{F(-x)}\rangle$. Hence, we cannot avoid the following property of the function in order to maintain consistency for the fundamental relation (6)

$$\overline{F(x)} = \overline{F(-x)}. \tag{11}$$

That is, the function under study is even

$$F(x)=F(-x). \tag{12}$$

3. Conclusions

In conclusion, we have discussed a new mathematical structure for standard quantum algorithms. They have said a certain property in case of a special function f that the relation $f(x) = f(-x)$ holds.

Acknowledgements

We thank Professor Han Geurdes for valuable discussions.

References

[1]. D. Deutsch, *Proc. Roy. Soc. London Ser. A* 400, 97 (1985). https://doi.org/10.1098/rspa.1985.0070

[2]. D. Deutsch and R. Jozsa, *Proc. Roy. Soc. London Ser. A* 439, 553 (1992). https://doi.org/10.1098/rspa.1992.0167

[3]. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Proc. Roy. Soc. London Ser. A* 454, 339 (1998). https://doi.org/10.1098/rspa.1998.0164

[4]. E. Bernstein and U. Vazirani, Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC '93), pp. 11-20 (1993). https://doi.org/10.1145/167088.167097

[5]. E. Bernstein and U. Vazirani, SIAM J. Comput. 26-5, pp. 1411-1473 (1997). https://doi.org/10.1137/S0097539796300921

[6]. D. R. Simon, Foundations of Computer Science, (1994) Proceedings., 35th Annual Symposium on: 116-123, retrieved 2011-06-06.

[7]. P. W. Shor, Proceedings of the 35th IEEE Symposium on Foundations of Computer Science. 124 (1994).

[8]. L. K. Grover, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. 212 (1996).