Necessary and sufficient conditions for the root-finding problem

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

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*
E-mail: ko_mi_na@yahoo.co.jp

[2] *Institute of Mathematics, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet road, Cau Giay district, Hanoi, Vietnam*

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

(Dated: June 24, 2024)

Necessary and sufficient conditions for finding all the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$ are studied in term of quantum computing. We hope our discussions give some insight for future studies for root-finding problem.

PACS numbers: 03.67.-a, 03.67.Ac, 03.67.Lx, 03.65.Ca
Keywords: Quantum information; Quantum algorithms, protocols, and simulations; Quantum computation architectures and implementations; Formalism

I. INTRODUCTION

The great success of quantum mechanics (cf. [1–7]) is recognized by the scientific community for physical theories. Between the articles of research for constructing theoretical quantum algorithms [8] it may be mentioned as follows. In 1985, the Deutsch algorithm was introduced and constructed for the function property problem [9–11]. In 1993, the Bernstein–Vazirani algorithm was proposed for identifying linear functions [12, 13]. Generalization of the Bernstein–Vazirani algorithm beyond qubit systems is reported [14]. In 1994, Simon's algorithm [15] and Shor's algorithm [16] were discussed for period finding of periodic functions. In 1996, Grover [17] provided an algorithm for unordered object finding and the motivation for exploring the computational possibilities offered by quantum mechanics. In 2020, a parallel computation for all of the combinations of values in variables of a logical function was proposed by Nagata and Nakamura [18, 19].

Continuous-variable quantum information is the area of quantum information science that makes use of physical observables, such as the strength of an electromagnetic field, whose numerical values belong to continuous intervals. In 1998, Braunstein studied error correction for continuous quantum variables [20] and quantum error correction for communication with linear optics [21]. In 1999, Lloyd and Braunstein proposed quantum computation over continuous variables [22]. The same year, Ralph considered continuous-variable quantum cryptography [23]. In 2000, Hillery discussed quantum cryptography with squeezed states [24], while Reid described quantum cryptography with a predetermined key using continuous-variable Einstein-Podolsky-Rosen correlations [25].

In 2001, secure quantum key distribution using squeezed states was studied by Gottesman and Preskill [26]. A year later, continuous-variable quantum cryptography using coherent states was first proposed by Grosshans and Grangier [27]. Efficient classical simulation of continuous-variable quantum information processes is studied by Bartlett, Sanders, Braunstein, and Nemoto [28]. Continuous-variable quantum computing and its applications to cryptography are discussed by Diep, Nagata, and Wong [29].

Recently, Nagata and Nakamura discuss a quantum algorithm of finding the roots of a polynomial function by using the generalized Bernstein–Vazirani algorithm [30]. However, they restrict themselves to an assumption that all the roots are in the integers **Z**. Here, all the roots considered here are in the complex numbers **C**. How do we find all the roots of the polynomial function? It is a very difficult mathematical problem and we will not discuss how to solve it. Instead, we discuss necessary and sufficient conditions for finding all the roots of a polynomial function. We hope our discussions give some insight for future studies for root-finding problem.

In this paper, necessary and sufficient conditions for finding all the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$ are studied in term of quantum computing. We hope our discussions give some insight for future studies for root-finding problem.

II. NECESSARY AND SUFFICIENT CONDITIONS FOR THE ROOT-FINDING PROBLEM

Let us consider necessary and sufficient conditions for finding the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$. Here the roots are in the complex numbers; $|r_1| \le |r_2| \le ... \le |r_m|, r_j \in \mathbf{C}$, $f(x) \in \mathbf{C}$, $x \in \mathbf{C}$, and $a_j \in \mathbf{R}$. Here, $|r_j| = \sqrt{(\Re r_j)^2 + (\Im r_j)^2}$. Suppose the following relation:

$$d \ge |a_0| = |r_1||r_2|...|r_m| \ge |r_m|, \tag{1}$$

where $|a_0|$ is the absolute value of the constant of the polynomial function, $|r_m|$ is the largest absolute value of the roots of the function, and d is a very large natural number. Here the problem is of searching necessary and sufficient conditions for finding the roots of the polynomial function.

Let us discuss the structure of quantum computing. To this end, we introduce the transformation U_f defined by the mapping

$$U_f|x\rangle|j\rangle = |x\rangle|(|f(x)| + j) \bmod d\rangle, \tag{2}$$

where $|f(x)| = \sqrt{(\Re f(x))^2 + (\Im f(x))^2}$. We define a quantum state $|\phi_d\rangle$ as follows:

$$|\phi_d\rangle = \frac{1}{\sqrt{d}} \int_0^d dj \omega(d)^{d-j}|j\rangle, \tag{3}$$

where $\omega(d) = e^{2\pi i/d}$. By the phase kickback [31] (See Appendix A) we have the following formula:

$$U_f|x\rangle|\phi_d\rangle = \omega(d)^{|f(x)|}|x\rangle|\phi_d\rangle. \tag{4}$$

Notice that

$$(U_f)^d|x\rangle|j\rangle = |x\rangle|(d|f(x)| + j) \bmod d\rangle = |x\rangle|j\rangle. \tag{5}$$

Therefore, the mapping U_f is a cyclic transformation.

Here, we define the input state as follows:

$$|\psi\rangle_d = \frac{1}{\sqrt{d}} \int_0^d dx|x\rangle|\phi_d\rangle. \tag{6}$$

By applying U_f, to $|\psi\rangle_d$, we obtain the following output state by the phase kickback:

$$U_f|\psi\rangle_d = \frac{1}{\sqrt{d}} \int_0^d dx \omega(d)^{|f(x)|}|x\rangle|\phi_d\rangle. \tag{7}$$

So, by looking at the state $U_f|\psi\rangle_d$, we see the phase factor $\omega(d)^{|f(x)|}$.

Again, we define the input state as follows (d and e are relatively prime and $d < e$):

$$|\psi\rangle_e = \frac{1}{\sqrt{e}} \int_0^e dx|x\rangle|\phi_e\rangle. \tag{8}$$

By applying U_f, to $|\psi_0\rangle$, we obtain the following output state by the phase kickback:

$$U_f|\psi\rangle_e = \frac{1}{\sqrt{e}} \int_0^e dx \omega(e)^{|f(x)|}|x\rangle|\phi_e\rangle. \tag{9}$$

So, by looking at the state $U_f|\psi\rangle_e$, we see the phase factor $\omega(e)^{|f(x)|}$.

We have several necessary and sufficient conditions for finding all the roots of a polynomial function.

$$\begin{aligned} & |f(r)| = 0 \\ & \Leftrightarrow \omega(d)^{|f(r)|} = 1 \wedge \omega(e)^{|f(r)|} = 1 \\ & \Leftrightarrow U_f = I \\ & \Leftrightarrow U_f|\psi\rangle_d = |\psi\rangle_d \wedge U_f|\psi\rangle_e = |\psi\rangle_e, \end{aligned} \tag{10}$$

where d and e are relatively prime and $d < e$.

Proposition 1

$$|f(r)| = 0 \Rightarrow \omega(d)^{|f(r)|} = 1 \wedge \omega(e)^{|f(r)|} = 1. \tag{11}$$

Proof: If $|f(r)| = 0$, then $\omega(d)^0 = 1$ and $\omega(e)^0 = 1$.
QED

Proposition 2

$$|f(r)| = 0 \Leftarrow \omega(d)^{|f(r)|} = 1 \wedge \omega(e)^{|f(r)|} = 1. \tag{12}$$

Proof: If $\omega(d)^{|f(r)|} = 1$, then $|f(r)| = 0$ or $|f(r)| = dp, (p = 1, 2, 3, ...)$. If $\omega(e)^{|f(r)|} = 1$, then $|f(r)| = 0$ or $|f(r)| = eq, (q = 1, 2, 3, ...)$. d and e are relatively prime and $d < e$. Thus $|f(r)| = dp$ and $|f(r)| = eq$ are not realized. Therefore, $\omega(d)^{|f(r)|} = 1 \wedge \omega(e)^{|f(r)|} = 1$ implies $|f(r)| = 0$.
QED

Proposition 3

$$\begin{aligned} & \omega(d)^{|f(r)|} = 1 \wedge \omega(e)^{|f(r)|} = 1 \\ & \Leftarrow U_f|\psi\rangle_d = |\psi\rangle_d \wedge U_f|\psi\rangle_e = |\psi\rangle_e. \end{aligned} \tag{13}$$

Proof: Obvious.

Proposition 4

$$U_f = I \Rightarrow U_f|\psi\rangle_d = |\psi\rangle_d \wedge U_f|\psi\rangle_e = |\psi\rangle_e. \tag{14}$$

Proof: Obvious.

Proposition 5

$$|f(r)| = 0 \Rightarrow U_f = I. \tag{15}$$

Proof: If $|f(r)| = 0$, then $U_f|r\rangle|j\rangle = |r\rangle|(|f(r)| + j) \bmod d\rangle = |r\rangle|j\rangle$.
QED

We hope our discussions give some insight for future studies for root-finding problem.

III. CONCLUSIONS

Necessary and sufficient conditions for finding all the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ have been studied in term of quantum computing. We have hoped our discussions give some insight for future studies for root-finding problem.

ACKNOWLEDGMENTS

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

DECLARATIONS

Ethical approval

The authors are in an applicable thought to ethical approval.

Competing interests

The authors state that there is no conflict of interest.

Author contributions

Koji Nagata, Do Ngoc Diep, and Tadao Nakamura wrote and read the manuscript.

Funding

Not applicable.

Data availability

No data associated in the manuscript.

Appendix A: The phase kickback

We have the following formula by the phase kick-back [31]:

$$U_f|x\rangle|\phi_d\rangle = \omega(d)^{|f(x)|}|x\rangle|\phi_d\rangle. \tag{A1}$$

where $\omega(d) = e^{2\pi i/d}$ and $|f(x)| = \sqrt{(\Re f(x))^2 + (\Im f(x))^2}$.

In what follows, we discuss the rationale behind the above relation (A1). Consider the action of the U_f gate on the state $|x\rangle|\phi_d\rangle$. Each term in $|\phi_d\rangle$ is of the form $\omega^{d-j}|j\rangle$. We observe that

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{d-j}|x\rangle|(|f(x)| + j) \bmod d\rangle. \tag{A2}$$

A variable k is introduced such that $|f(x)| + j = k$, from which it follows that $d - j = d + |f(x)| - k$. Thus, (A2) becomes

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{|f(x)|}\omega^{d-k}|x\rangle|k \bmod d\rangle. \tag{A3}$$

If $k < d$ we have that $|k \bmod d\rangle = |k\rangle$ and thus the terms in $|\phi_d\rangle$ for which $k < d$ are transformed as follows:

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{|f(x)|}\omega^{d-k}|x\rangle|k\rangle. \tag{A4}$$

On the other hand, as both $|f(x)|$ and j are bounded from above by d, k is strictly less than $2d$. Thus, when $d \le k < 2d$, we have $|k \bmod d\rangle = |k - d\rangle$. Let $k - d = m$. We have

$$\begin{aligned}&\omega^{|f(x)|}\omega^{d-k}|x\rangle|k \bmod d\rangle = \omega^{|f(x)|}\omega^{-m}|x\rangle|m\rangle \\ &= \omega^{|f(x)|}\omega^{d-m}|x\rangle|m\rangle.\end{aligned} \tag{A5}$$

Hence, the terms in $|\phi_d\rangle$ for which $k \ge d$ are transformed as follows:

$$U_f\omega^{d-j}|x\rangle|j\rangle = \omega^{|f(x)|}\omega^{d-m}|x\rangle|m\rangle. \tag{A6}$$

Finally, regarding (A4) and (A6), we have

$$U_f|x\rangle|\phi_d\rangle = \omega^{|f(x)|}|x\rangle|\phi_d\rangle. \tag{A7}$$

Therefore, the relation (A1) holds.

REFERENCES

[1] J. J. Sakurai, “Modern Quantum Mechanics,” (Addison-Wesley Publishing Company, 1995), Revised ed.

[2] A. Peres, “Quantum Theory: Concepts and Methods,” (Kluwer Academic, Dordrecht, The Netherlands, 1993).

[3] M. Redhead, “Incompleteness, Nonlocality, and Realism,” (Clarendon Press, Oxford, 1989), 2nd ed.

[4] J. von Neumann, “Mathematical Foundations of Quantum Mechanics,” (Princeton University Press, Princeton, New Jersey, 1955).

[5] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information,” (Cambridge University Press, 2000).

[6] A. S. Holevo, “Quantum Systems, Channels, Information, A Mathematical Introduction,” (De Gruyter, 2012). https://doi.org/10.1515/9783110273403

[7] K. Nagata, D. N. Diep, A. Farouk, and T. Nakamura, “Simplified Quantum Computing with Applications,” (IOP Publishing, Bristol, UK, 2022). https://doi.org/10.1088/978-0-7503-4700-6

[8] R. Rennie (Editor), “Oxford dictionary of physics,” (Oxford University Press, 2015), Seventh ed.

[9] 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

[10] 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

[11] 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

[12] 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

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

[14] K. Nagata, H. Geurdes, S. K. Patro, S. Heidari, A. Farouk, and T. Nakamura, “Generalization of the Bernstein-Vazirani algorithm beyond qubit systems,” Quantum Stud.: Math. Found. **7**, 17 (2020). https://doi.org/10.1007/s40509-019-00196-4

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] S. L. Braunstein, "Error Correction for Continuous Quantum Variables," Phys. Rev. Lett. **80**, 4084 (1998). https://doi.org/10.1103/PhysRevLett.80.4084

[21] S. L. Braunstein, "Quantum error correction for communication with linear optics," Nature (London) **394**, 47 (1998). https://doi.org/10.1038/27850

[22] S. Lloyd and S. L. Braunstein, "Quantum Computation over Continuous Variables," Phys. Rev. Lett. **82**, 1784 (1999). https://doi.org/10.1103/PhysRevLett.82.1784

[23] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303(R) (1999). https://doi.org/10.1103/PhysRevA.61.010303

[24] M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A **61**, 022309 (2000). https://doi.org/10.1103/PhysRevA.61.022309

[25] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," Phys. Rev. A **62**, 062308 (2000). https://doi.org/10.1103/PhysRevA.62.062308

[26] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**, 022309 (2001). https://doi.org/10.1103/PhysRevA.63.022309

[27] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Phys. Rev. Lett. **88**, 057902 (2002). https://doi.org/10.1103/PhysRevLett.88.057902

[28] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, "Efficient Classical Simulation of Continuous Variable," Quantum Information Processes. Phys. Rev. Lett. **88**, 097904 (2002). https://doi.org/10.1103/PhysRevLett.88.097904

[29] D. N. Diep, K. Nagata, and R. Wong, "Continuous-variable quantum computing and its applications to cryptography," Int. J. Theor. Phys. **59**, 3184 (2020). https://doi.org/10.1007/s10773-020-04571-5

[30] K. Nagata and T. Nakamura "Quantum algorithm for the root-finding problem," Quantum Studies: Mathematics and Foundations, Volume 6, Issue 1 (2019), pp. 135–139. https://doi.org/10.1007/s40509-018-0171-0

[31] K. Nagata, H. Geurdes, S. K. Patro, S. Heidari, A. Farouk, and T. Nakamura, "Quantum Algorithm for Determining a Complex Number String," Int. J. Theor. Phys. **58**, 3694 (2019). https://doi.org/10.1007/s10773-019-04239-9