Necessary and sufficient conditions for the root-finding problem

Koji Nagata,¹ Do Ngoc Diep,² and Tadao Nakamura³

¹Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea
E-mail: ko_mi_na@yahoo.co.jp
²Institute of Mathematics, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet road, Cau Giay district, Hanoi, Vietnam
³Department 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 \( f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0 \) 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 \( \mathbb{Z} \). Here, all the roots considered here are in the complex numbers \( \mathbb{C} \). 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 \( f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0 \) 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 \( f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0 \). Here the roots are in the complex numbers; \( |r_1| \leq |r_2| \leq \ldots \leq |r_m|, r_j \in \mathbb{C}, \ f(x) \in \mathbb{C}, \ x \in \mathbb{C}, \) and \( a_j \in \mathbb{R} \). Here \( |r_j| = \sqrt{(\Re(r_j))^2 + (\Im(r_j))^2} \). Suppose the following relation:

\[
d \geq |a_0| = |r_1||r_2|\ldots|r_m| \geq |r_m|, \quad (1)
\]

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

$$U_f|x⟩|j⟩ = |x⟩|⟨f(x) + j⟩ \mod d⟩,$$

where $|f(x)| = \sqrt{(Rf(x))^2 + (3f(x))^2}$. We define a quantum state $|φ_d⟩$ as follows:

$$|φ_d⟩ = \frac{1}{\sqrt{d}} \int_0^d dx |x⟩|φ_d⟩.$$

Notice that

$$(U_f)^d|x⟩|j⟩ = |x⟩|⟨df(x) + j⟩ \mod d⟩ = |x⟩|j⟩.$$

Therefore, the mapping $U_f$ is a cyclic transformation. Here, we define the input state as follows:

$$|ψ_d⟩ = \frac{1}{\sqrt{d}} \int_0^d dx |x⟩|ψ_d⟩.$$

By applying $U_f$, to $|ψ_d⟩$, we obtain the following output state by the phase kickback:

$$U_f|ψ⟩d = \frac{1}{\sqrt{d}} \int_0^d dx |x⟩|ψ⟩d.$$

So, by looking at the state $U_f|ψ⟩d$, we see the phase factor $ω(d)|f(x)|$.

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

$$|ψ⟩e = \frac{1}{\sqrt{e}} \int_0^e dx |x⟩|ψ⟩e.$$

By applying $U_f$, to $|ψ0⟩$, we obtain the following output state by the phase kickback:

$$U_f|ψ⟩e = \frac{1}{\sqrt{e}} \int_0^e dx |x⟩|ψ⟩e.$$

So, by looking at the state $U_f|ψ⟩e$, we see the phase factor $ω(e)|f(x)|$.

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

$$|f(r)| = 0 \Rightarrow ω(d)|f(r)| = 1 \land ω(e)|f(r)| = 1.$$

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

QED

Proposition 2

$$|f(r)| = 0 \iff ω(d)|f(r)| = 1 \land ω(e)|f(r)| = 1.$$

Proof: If $ω(d)|f(r)| = 1$, 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, $ω(d)|f(r)| = 1 \land ω(e)|f(r)| = 1$ implies $|f(r)| = 0$.

QED

Proposition 3

$$ω(d)|f(r)| = 1 \land ω(e)|f(r)| = 1$$

Proof: Obvious.

Proposition 4

$$U_f I = U_f |ψ⟩d = |ψ⟩d \land U_f |ψ⟩e = |ψ⟩e.$$

Proof: Obvious.

Proposition 5

$$|f(r)| = 0 \Rightarrow U_f I.$$

Proof: If $|f(r)| = 0$, then $U_f|r⟩|j⟩ = |r⟩|(|f(r)| + j) \mod d⟩ = |r⟩|j⟩$.

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, Hann Gerunds, Preston Guynn, Shahrokhi Heidari, Wenliang Jin, Hamed Daei Kasmaei, Janusz Milek, Mosayeb Naseri, Santan 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]:

\[ U_f |x\rangle |\phi_d\rangle = \omega(d)^{|f(x)|} |x\rangle |\phi_d\rangle. \]  

(A1)

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

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

\[ U_f \omega^{d-j}|j\rangle = \omega^{d-j}|f(x)\rangle (|f(x)| + j) \bmod d. \]  

(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

\[ U_f \omega^{d-j}|x\rangle |j\rangle = \omega^{|f(x)|} \omega^{d-k}|x\rangle |k\rangle. \]  

(A3)

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

\[ U_f \omega^{d-j}|x\rangle |j\rangle = \omega^{|f(x)|} \omega^{d-k}|x\rangle |k\rangle. \]  

(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 \( d \leq k < 2d \), we have \(|k \bmod d| = |k - d|\). Let \( k - d = m \). We have

\[ \omega^{|f(x)|} \omega^{d-k}|x\rangle |m\rangle = \omega^{|f(x)|} \omega^{d-m}|x\rangle |m\rangle. \]  

(A5)

Hence, the terms in \(|\phi_d\rangle\) for which \( k \geq d \) are transformed as follows:

\[ U_f \omega^{d-j}|x\rangle |j\rangle = \omega^{|f(x)|} \omega^{d-m}|x\rangle |m\rangle. \]  

(A6)

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

\[ U_f |x\rangle |\phi_d\rangle = \omega^{|f(x)|} |x\rangle |\phi_d\rangle. \]  

(A7)

Therefore, the relation (A1) holds.

REFERENCES