Int J Theor Phys (2018) 57:2546–2555
https://doi.org/10.1007/s10773-018-3776-5

Efficient Quantum Algorithms of Finding the Roots of a Polynomial Function

Koji Nagata[1] · **Tadao Nakamura**[2] · **Han Geurdes**[3] · **Josep Batle**[4] · **Ahmed Farouk**[5] · **Do Ngoc Diep**[6,7] · **Santanu Kumar Patro**[8]

Received: 16 February 2018 / Accepted: 8 May 2018 / Published online: 18 May 2018

Abstract Two quantum algorithms of finding the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ are discussed by using the Bernstein-Vazirani algorithm. One algorithm is presented in the modulo 2. The other algorithm is presented in the modulo d. Here all the roots are in the integers $\mathbf{Z}$. The speed of solving the problem is shown to outperform the best classical case by a factor of m in both cases.

Keywords Quantum computation · Quantum algorithms

✉ 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 Geurdes Datascience, KvK 64522202, C vd Lijnstraat 164, 2593 NN, Den Haag, Netherlands

4 Departament de Física, Universitat de les Illes Balears, 07122 Palma de Mallorca, Balearic Islands, Spain

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

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

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

8 Department of Mathematics, Berhampur University, Berhampur, 760007, Odisha, India

1 Introduction

Quantum mechanics (cf. [1–6]) is successful in explaining and predicting many physical phenomena. One of the interesting applications of quantum principles is the application to information theory [6] leading to quantum computing.

Looking at studies of quantum computing, implementation of a quantum algorithm to solve Deutsch's problem [7–9] on a nuclear magnetic resonance quantum computer is reported firstly [10]. An implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer is also reported [11]. There are several attempts to use single-photon two-qubit states for quantum computing. Oliveira et al. implements Deutsch's algorithm with polarization and transverse spatial modes of the electromagnetic field as qubits [12]. In addition, single-photon Bell states are prepared and measured [13]. The decoherence-free implementation of Deutsch's algorithm is introduced by using such a single-photon and by using two logical qubits [14]. A one-way based experimental implementation of Deutsch's algorithm is reported [15].

For a number of recent algorithmic developments we mention the following. In 1993, the Bernstein-Vazirani algorithm was published [16, 17]. This work can be considered an extension of the Deutsch-Jozsa algorithm. In 1994, Simon's algorithm [18] and Shor's algorithm [19] were discussed. In 1996, Grover [20] provided the highest motivation for exploring the computational possibilities offered by quantum mechanics. Implementation of a quantum algorithm to solve the Bernstein-Vazirani parity problem without entanglement in an ensemble quantum computer can be mentioned as an important quantum algorithm [21]. Fiber-optics implementation of the Deutsch-Jozsa and Bernstein-Vazirani quantum algorithms with three qubits was also discussed in the recent past [22]. The question whether or not quantum learning is robust against noise is a subject of intense study [23].

A quantum algorithm for approximating the influences of Boolean functions and its applications are recently studied [24]. In addition, quantum computation with coherent spin states and the close Hadamard problem [25] are reported. Transport implementation of the Bernstein-Vazirani algorithm with ion qubits is studied [26]. Quantum Gauss-Jordan elimination and simulation of accounting principles on quantum computers are discussed [27]. We mention that the dynamical analysis of Grover's search algorithm in arbitrarily high-dimensional search spaces is studied [28]. A method of computing many functions simultaneously by using many parallel quantum systems is reported [29]. An algorithm for fast determining a homogeneous linear function is proposed [30]. A method of calculating a multiplication by using the generalized Bernstein-Vazirani algorithm is studied [31].

On the other hand, we may wonder if we need all the previously mentioned studies to reach a good quantum computer. In 2015, it was discussed that the Deutsch-Jozsa algorithm can be used for quantum key distribution [32]. In 2017, it was discussed that secure quantum key distribution based on Deutsch's algorithm using an entangled state [33]. Subsequently, a highly speedy secure quantum cryptography based on the Deutsch-Jozsa algorithm is proposed [34]. The relation between quantum computer and secret sharing with the use of quantum principles is discussed [35].

The Bernstein-Vazirani algorithm determines a bit-strings. It is extended to determining the values of a function [36]. The values of the functions are restricted in $\{0, 1\}$. By using the method, we can consider important mathematical problems (for example [31]). In this paper, we consider root-finding problem.

By extending the Bernstein-Vazirani algorithm more, we present an algorithm of determining the values of a function that are extended to the natural numbers $\mathbf{N}$. That is, the extended algorithm determines a natural-number-strings instead of a bit-strings [30]. By using the method, we can consider the same important mathematical problem (root-finding problem).

Here, we propose two quantum algorithms of finding the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$. Here $x \in \mathbf{R}$ and the roots are in the integers; $|r_1| \leq |r_2| \leq ... \leq |r_m|, r_j \in \mathbf{Z}$. One algorithm is presented in the modulo 2. Another algorithm is presented in the modulo d. Given $2S(= N)$ absolute values of the function

$$|f(-S)|, ..., |f(-2)|, |f(-1)|,$$
$$|f(1)|, |f(2)|, ..., |f(S)| \tag{1}$$

all the unknown roots of the function shall be found, simultaneously. In the best classical case, we need m steps, whereas, in the quantum case we need a query. The speed of finding the roots is shown to outperform the classical case by a factor of m. Our algorithm combines quantum superposition with a property of quantum mechanics known as interference.

One method is based on the generalized Bernstein-Vazirani algorithm in the modulo 2 [36]. Another method is based on the generalized Bernstein-Vazirani algorithm in the modulo d [30].

2 Quantum Algorithm of Finding the Roots of a Polynomial Function: Part 1

In this section, the method is based on the generalized Bernstein-Vazirani algorithm in the modulo 2 [36].

Let us now introduce a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$. Assume we are given natural numbers

$$1, 2, ..., S \geq |a_0| = |r_1||r_2|...|r_m| \geq |r_m| \tag{2}$$

where $|a_0|$ is the absolute value of the constant and $|r_m|$ is the largest absolute value of the roots. Here the problem is of searching the roots of the function by a query. One step is of determining the following values

$$|f(-S)|, ..., |f(-2)|, |f(-1)|,$$
$$|f(1)|, |f(2)|, ..., |f(S)|. \tag{3}$$

Recall that in the classical case, we need N queries, that is, N separate evaluations of the values of the function (3). In our quantum algorithm, we shall require a single query. Suppose now that we introduce another function

$$g : \mathbf{R} \to \{0, 1\}. \tag{4}$$

The relation between the functions $f(x)$ and $g(x)$ is defined as follows

$$g(x) = \begin{cases} 1 \text{ if } f(x) \neq 0 \\ 0 \text{ if } f(x) = 0. \end{cases} \tag{5}$$

Our aim is of knowing the values x such that $f(x) = 0$ because they are the roots of $f(x)$. So our aim is equivalently of knowing the values x such that $g(x) = 0$ because they are the roots of $f(x)$. One step is, therefore, of determining the following N values

$$g(-S), ..., g(-2), g(-1),$$
$$g(1), g(2), ..., g(S). \tag{6}$$

We construct the following function

$$\begin{aligned} h(x) &= g(b)\cdot x = \sum_{i=1}^{N} g(b_i)x_i\,(\mathrm{mod}2) \\ &= g(b_1)x_1 \oplus g(b_2)x_2 \oplus g(b_3)x_3 \oplus \cdots \oplus g(b_N)x_N \\ &\quad x_i \in \{0,1\},\, g(b_i) \in \{0,1\}, \\ b_1 &= -S, ..., b_{N-1} = S-1, b_N = S. \end{aligned} \tag{7}$$

Here $g(b)$ symbolizes

$$g(b_1)...g(b_{N-1})g(b_N) = g(-S)...g(S-1)g(S). \tag{8}$$

Let us follow the quantum states through our algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle \tag{9}$$

where $|0\rangle^{\otimes N} = \overbrace{|0\rangle \otimes |0\rangle \otimes ... \otimes |0\rangle}^{N}$. After the componentwise Hadamard transforms on the state (9)

$$\overbrace{H|0\rangle \otimes H|0\rangle \otimes ... \otimes H|0\rangle}^{N} \otimes H|1\rangle \tag{10}$$

we have

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^N} \frac{|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{11}$$

Next, the function h is evaluated using

$$U_h : |x, y\rangle \to |x, y \oplus h(x)\rangle \tag{12}$$

in giving

$$|\psi_2\rangle = \pm \sum_{x} \frac{(-1)^{h(x)}|x\rangle}{\sqrt{2^N}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{13}$$

Here $y \oplus h(x)$ is the bitwise XOR (exclusive OR) of y and $h(x)$. By checking the cases $x = 0$ and $x = 1$ separately, we see that for a single qubit

$$H|x\rangle = \sum_{z} (-1)^{xz}|z\rangle/\sqrt{2}. \tag{14}$$

Thus we have

$$H^{\otimes N}|x_1, \ldots, x_N\rangle = \frac{\sum_{z_1,\ldots,z_N} (-1)^{x_1 z_1 + \cdots + x_N z_N}|z_1, \ldots, z_N\rangle}{\sqrt{2^N}}. \tag{15}$$

This can be summarized more succinctly in the very useful equation

$$H^{\otimes N}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^N}} \tag{16}$$

where $x \cdot z$ is the bitwise inner product of x and z, modulo 2. Using the (16) and (13), we can now evaluate $H^{\otimes N}|\psi_2\rangle = |\psi_3\rangle$

$$|\psi_3\rangle = \pm \sum_{z}\sum_{x} \frac{(-1)^{x\cdot z + h(x)}|z\rangle}{2^N} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{17}$$

Thus we have

$$|\psi_3\rangle = \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + g(b)\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{18}$$

Because we have

$$\sum_x (-1)^x = 0 \tag{19}$$

we can see that

$$\sum_x (-1)^{x\cdot z + g(b)\cdot x} = 2^N \delta_{g(b),z}. \tag{20}$$

Therefore, the sum is zero if $z \neq g(b)$ and is 2^N if $z = g(b)$. Thus we have

$$\begin{aligned}
|\psi_3\rangle &= \pm \sum_z \sum_x \frac{(-1)^{x\cdot z + g(b)\cdot x}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\
&= \pm \sum_z \frac{2^N \delta_{g(b),z}|z\rangle}{2^N}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\
&= \pm |g(b)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\
&= \pm |g(b_1)g(b_2)\cdots g(b_N)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \qquad (21)
\end{aligned}$$

from which

$$|g(b_1)g(b_2)\cdots g(b_N)\rangle. \tag{22}$$

can be obtained. That is to say, if we measure $|g(b_1)g(b_2)\cdots g(b_N)\rangle$ then we can retrieve the following values

$$g(b_1), g(b_2), g(b_3), \ldots, g(b_N) \tag{23}$$

using a single query. If $g(-3) = 0$, $g(5) = 0$, ..., $g(S-2) = 0$, the function $f(x)$ can be factorized as follows

$$f(x) = (x+3)(x-5)...(x-(S-2)). \tag{24}$$

Therefore we can find the m roots of the function. All we have to do is of performing one quantum measurement. The speed to determine the m roots improves by a factor of m as compared to the best classical counterpart.

3 Quantum Algorithm of Finding the Roots of a Polynomial Function: Part 2

In this section, the method is based on the generalized Bernstein-Vazirani algorithm in the modulo d [30].

We introduce a positive integer $d(> S)$. Throughout the section, we consider the problem in the modulo d. Assume the following

$$\overbrace{|f(-S)|, ..., |f(-1)|, |f(1)|, ..., |f(S)|}^{N} \leq d-1 \tag{25}$$

where $f(j) \in \{0, 1, ..., d-1\}$, and we define

$$f(\overline{N}) = (|f(-S)|, ..., |f(-1)|, |f(1)|, ..., |f(S)|) \tag{26}$$

where each entry of $f(\overline{N})$ is a natural number in the modulo d. Here $f(\overline{N}) \in \{0, 1, ..., d-1\}^N$. We define $f_{f(\overline{N})}(x)$ as follows

$$\begin{aligned} f_{f(\overline{N})}(x) &= f(\overline{N}) \cdot x \bmod d \\ &= |f(-S)|x_1 + |f(1-S)|x_2 + \cdots + |f(S)|x_N \bmod d \end{aligned} \tag{27}$$

where $x = (x_1, ..., x_N) \in \{0, 1, ..., d-1\}^N$. Let us follow the quantum states through the algorithm. The input state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|d-1\rangle \tag{28}$$

where $|0\rangle^{\otimes N}$ means $\overbrace{|0, 0, ..., 0\rangle}^{N}$. We discuss the Fourier transform of $|0\rangle$

$$|0\rangle \to \sum_{y=0}^{d-1} \frac{\omega^{y\cdot 0}|y\rangle}{\sqrt{d}} = \sum_{y=0}^{d-1} \frac{|y\rangle}{\sqrt{d}} \tag{29}$$

where we have used $\omega^0 = 1$. Subsequently let us define the wave function $|\phi\rangle$ as follows

$$|\phi\rangle = \frac{1}{\sqrt{d}}(\omega^d|0\rangle + \omega^{d-1}|1\rangle + \cdots + \omega|d-1\rangle) \tag{30}$$

where $\omega = e^{2\pi i/d}$. In the following, we discuss the Fourier transform of $|d-1\rangle$

$$\begin{aligned} |d-1\rangle \to \sum_{y=0}^{d-1} \frac{\omega^{y\cdot(d-1)}|y\rangle}{\sqrt{d}} &= \sum_{y=0}^{d-1} \frac{\omega^{yd-y}|y\rangle}{\sqrt{d}} \\ &= \sum_{y=0}^{d-1} \frac{\omega^{d-y}|y\rangle}{\sqrt{d}} = |\phi\rangle \end{aligned} \tag{31}$$

where we have used $\omega^{yd} = \omega^d = 1$. The Fourier transform of $|x_1...x_N\rangle$ is as follows

$$\begin{aligned} &|x_1...x_N\rangle \\ &\to \sum_{z_1=0}^{d-1} \cdots \sum_{z_N=0}^{d-1} \frac{\omega^{z_1x_1}|z_1\rangle}{\sqrt{d}} \cdots \frac{\omega^{z_Nx_N}|z_N\rangle}{\sqrt{d}} \\ &= \sum_{z\in K} \frac{\omega^{z\cdot x}|z\rangle}{\sqrt{d^N}} \end{aligned} \tag{32}$$

where $K = \{0, 1, 2, ..., d-1\}^N$ and z is $(z_1, z_2, ..., z_N)$. Hence, for completeness, $\sum_{z\in K}$ is a shorthand to the compound sum

$$\sum_{z_1\in\{0,1,..,d-1\}} \sum_{z_2\in\{0,1,..,d-1\}} \cdots \sum_{z_N\in\{0,1,..,d-1\}} . \tag{33}$$

After the componentwise Fourier transforms on the state (28)

$$\overbrace{F|0\rangle \otimes F|0\rangle \otimes ... \otimes F|0\rangle}^{N} \otimes F|d-1\rangle \tag{34}$$

we have

$$|\psi_1\rangle = \sum_{x\in K} \frac{|x\rangle}{\sqrt{d^N}}|\phi\rangle. \tag{35}$$

We introduce $SUM_{f_{f(\overline{N})}(x)}$ gate

$$|x\rangle|j\rangle \to |x\rangle|(f_{f(\overline{N})}(x) + j) \bmod d\rangle \tag{36}$$

where

$$f_{f(\overline{N})}(x) = f(\overline{N}) \cdot x \bmod d. \tag{37}$$

We have

$$SUM_{f(\overline{N})\cdot x}|x\rangle|\phi\rangle = \omega^{f(\overline{N})\cdot x}|x\rangle|\phi\rangle. \tag{38}$$

In what follows, we will discuss the reasonable behind of the above relation (38). Now consider applying the $SUM_{f(\overline{N})\cdot x}$ gate to the state $|x\rangle|\phi\rangle$. Each term in $|\phi\rangle$ is of the form $\omega^{d-j}|j\rangle$. We see

$$\begin{aligned} &SUM_{f(\overline{N})\cdot x}\omega^{d-j}|x\rangle|j\rangle \\ &\to \omega^{d-j}|x\rangle|(j + f(\overline{N}) \cdot x) \bmod d\rangle. \end{aligned} \tag{39}$$

We introduce k such as $f(\overline{N}) \cdot x + j = k \Rightarrow d - j = d + \big(f(\overline{N}) \cdot x\big) - k$. Hence (39) becomes

$$\begin{aligned} &SUM_{f(\overline{N})\cdot x}\omega^{d-j}|x\rangle|j\rangle \\ &\to \omega^{f(\overline{N})\cdot x}\omega^{d-k}|x\rangle|k \bmod d\rangle. \end{aligned} \tag{40}$$

Now, when $k < d$ we have $|k \bmod d\rangle = |k\rangle$ and thus, the terms in $|\phi\rangle$ such that $k < d$ are transformed as follows

$$SUM_{f(\overline{N})\cdot x}\omega^{d-j}|x\rangle|j\rangle \to \omega^{f(\overline{N})\cdot x}\omega^{d-k}|x\rangle|k\rangle. \tag{41}$$

Also, as $f(\overline{N}) \cdot x$ and j are bounded above by $d - 1$, k is strictly less than $2d$. Hence, when $d \le k < 2d$ we have $|k \bmod d\rangle = |k - d\rangle$. Now, we introduce m such that $k - d = m$ then we have

$$\begin{aligned} \omega^{f(\overline{N})\cdot x}\omega^{d-k}|x\rangle|k \bmod d\rangle &= \omega^{f(\overline{N})\cdot x}\omega^{-m}|x\rangle|m\rangle \\ &= \omega^{f(\overline{N})\cdot x}\omega^{d-m}|x\rangle|m\rangle. \end{aligned} \tag{42}$$

Hence the terms in $|\phi\rangle$ such that $k \ge d$ are transformed as follows

$$SUM_{f(\overline{N})\cdot x}\omega^{d-j}|x\rangle|j\rangle \to \omega^{f(\overline{N})\cdot x}\omega^{d-m}|x\rangle|m\rangle. \tag{43}$$

Hence from (41) and (43) we have

$$SUM_{f(\overline{N})\cdot x}|x\rangle|\phi\rangle = \omega^{f(\overline{N})\cdot x}|x\rangle|\phi\rangle. \tag{44}$$

Therefore, the relation (38) holds. We have $|\psi_2\rangle$ by operating $SUM_{f_{f(\overline{N})}(x)}$ to $|\psi_1\rangle$

$$SUM_{f(\overline{N})\cdot x}|\psi_1\rangle = |\psi_2\rangle = \sum_{x\in K} \frac{\omega^{f(\overline{N})\cdot x}|x\rangle}{\sqrt{d^N}}|\phi\rangle. \tag{45}$$

After the Fourier transform on $|x\rangle$, using the previous (32) and (45) we can now evaluate $|\psi_3\rangle$ as follows

$$|\psi_3\rangle = \sum_{z\in K}\sum_{x\in K} \frac{(\omega)^{x\cdot z + f(\overline{N})\cdot x}|z\rangle}{d^N}|\phi\rangle. \tag{46}$$

Because we have

$$\sum_{x\in K}(\omega)^x = 0 \tag{47}$$

we may notice

$$\sum_{x\in K}(\omega)^{x\cdot(z+f(\overline{N}))} = d^N\delta_{z+f(\overline{N}),0} = d^N\delta_{z,-f(\overline{N})}. \tag{48}$$

Therefore, the above summation is zero if $z \neq -f(\overline{N})$ and the above summation is d^N if $z = -f(\overline{N})$. Thus we have

$$\begin{aligned} |\psi_3\rangle &= \sum_{z\in K}\sum_{x\in K} \frac{(\omega)^{x\cdot z + f(\overline{N})\cdot x}|z\rangle}{d^N}|\phi\rangle \\ &= \sum_{z\in K} \frac{d^N\delta_{z,-f(\overline{N})}|z\rangle}{d^N}|\phi\rangle \\ &= -|(|f(-S)|, ..., |f(-1)|, |f(1)|, ..., |f(S)|)\rangle|\phi\rangle \end{aligned} \tag{49}$$

from which

$$|(|f(-S)|, ..., |f(-1)|, |f(1)|, ..., |f(S)|)\rangle \tag{50}$$

can be obtained. That is to say, if we measure the first N qudits state of the state $|\psi_3\rangle$, that is, $|(|f(-S)|, ..., |f(-1)|, |f(1)|, ..., |f(S)|)\rangle$, then we can retrieve the following values

$$|f(-S)|, ..., |f(-1)|, |f(1)|, ..., |f(S)| \tag{51}$$

using a single query. If $|f(-3)| = 0, |f(5)| = 0, ..., |f(S-2)| = 0$, the function can be factorized as follows

$$f(x) = (x+3)(x-5)...(x-(S-2)). \tag{52}$$

Therefore we can find the m roots of the function. All we have to do is to perform one quantum measurement. The speed to determine the m roots improves by a factor of m as compared to the best classical counterpart.

4 Conclusions

In conclusion, two quantum algorithms of finding the roots of a polynomial function $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ have been proposed. Here $x \in \mathbf{R}$ and the roots have been in the integers $|r_1| \leq |r_2| \leq ... \leq |r_m|, r_j \in \mathbf{Z}$. One algorithm has been presented in the modulo 2. Another algorithm has been presented in the modulo d. Given absolute values of the function $|f(-S)|$, ..., $|f(-1)|$, $|f(1)|$, ..., $|f(S)|$, ($|a_0| \leq S$), all the unknown roots of the function shall have been found, simultaneously. The speed of finding the roots has been shown to outperform the best classical case by a factor of m in both cases.

Acknowledgements We thank Professor Germano Resconi and Professor Shahrokh Heidari for valuable comments.

References

1. von Neumann, J.: Mathematical foundations of quantum mechanics. Princeton University Press, Princeton, New Jersey (1955)
2. Feynman, R.P., Leighton, R.B., Sands, M.: Lectures on physics, Volume III, quantum mechanics. Addison-Wesley Publishing Company (1965)
3. Redhead, M.: Incompleteness, nonlocality, and realism, 2nd edn. Clarendon Press, Oxford (1989)
4. Peres, A.: Quantum theory: concepts and methods. Kluwer Academic, Dordrecht, the Netherlands (1993)
5. Sakurai, J.J.: Modern quantum mechanics. Addison-Wesley Publishing Company, Revised ed (1995)
6. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, UK (2000)
7. Deutsch, D.: Proc. Roy. Soc. London Ser. A **400**, 97 (1985)
8. Deutsch, D., Jozsa, R.: Proc. Roy. Soc. London Ser. A **439**, 553 (1992)
9. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Proc. Roy. Soc. London Ser. A **454**, 339 (1998)
10. Jones, J.A., Mosca, M.: J. Chem. Phys. **109**, 1648 (1998)
11. Gulde, S., Riebe, M., Lancaster, G.P.T., Becher, C., Eschner, J., Häffner, H., Schmidt-Kaler, F., Chuang, I.L., Blatt, R.: Nature (London) **421**, 48 (2003)
12. de Oliveira, A.N., Walborn, S.P., Monken, C.H.: J. Opt. B: Quantum Semiclass. Opt. **7**, 288–292 (2005)
13. Kim, Y.-H.: Phys. Rev. A **67**(R), 040301 (2003)
14. Mohseni, M., Lundeen, J.S., Resch, K.J., Steinberg, A.M.: Phys. Rev. Lett. **91**, 187903 (2003)
15. Tame, M.S., Prevedel, R., Paternostro, M., Böhi, P., Kim, M.S., Zeilinger, A.: Phys. Rev. Lett. **140501**, 98 (2007)
16. Bernstein, E., Vazirani, U.: 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
17. Bernstein, E., Vazirani, U.: SIAM J. Comput. **26-5**, 1411–1473 (1997)
18. Simon, D.R.: Foundations of Computer Science. Proceedings., 35th Annual Symposium on: 116-123, retrieved 2011-06-06 (1994)
19. Shor, P.W.: Proceedings of the 35th IEEE Symposium on Foundations of Computer Science 124 (1994)
20. Grover, L.K.: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212 (1996)
21. Du, J., Shi, M., Zhou, X., Fan, Y., Ye, B.J., Han, R., Wu, J.: Phys. Rev. A **64**, 042306 (2001)
22. Brainis, E., Lamoureux, L.-P., Cerf, N.J., Emplit, P.h., Haelterman, M., Massar, S.: Phys. Rev. Lett. **90**, 157902 (2003)
23. Cross, A.W., Smith, G., Smolin, J.A.: Phys. Rev. A **92**, 012327 (2015)
24. Li, H., Yang, L.: Quantum Inf. Process. **14**, 1787 (2015)
25. Adcock, M.R.A., Hoyer, P., Sanders, B.C.: Quantum Inf. Process. **15**, 1361 (2016)
26. Fallek, S.D., Herold, C.D., McMahon, B.J., Maller, K.M., Brown, K.R., Amini, J.M.: New J. Phys. **18**, 083030 (2016)
27. Diep, D.N., Giang, D.H., Van Minh, N.: Int. J. Theor. Phys. **56**, 1948 (2017). https://doi.org/10.1007/s10773-017-3340-8
28. Jin, W.: Quantum Inf. Process **15**, 65 (2016)
29. Nagata, K., Resconi, G., Nakamura, T., Batle, J., Abdalla, S., Farouk, A., Geurdes, H.: Asian J. Math. Phys. **1**(1), 1–4 (2017)
30. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Abdalla, S., Farouk, A., Diep, D.N.: Int. J. Theor. Phys. (2017). https://doi.org/10.1007/s10773-017-3630-1
31. Nagata, K., Nakamura, T., Geurdes, H., Batle, J., Abdalla, S., Farouk, A.: Int. J. Theor. Phys. (2018). https://doi.org/10.1007/s10773-018-3687-5
32. Nagata, K., Nakamura, T.: Open Access Library Journal **2**, e1798 (2015). https://doi.org/10.4236/oalib.1101798

33. Nagata, K., Nakamura, T.: Int. J. Theor. Phys. **56**, 2086 (2017). https://doi.org/10.1007/s10773-017-3352-4
34. Nagata, K., Nakamura, T., Farouk, A.: Int. J. Theor. Phys. **56**, 2887 (2017). https://doi.org/10.1007/s10773-017-3456-x
35. Diep, D.N., Giang, D.H.: Int. J. Theor. Phys. **56**, 2797 (2017). https://doi.org/10.1007/s10773-017-3444-1
36. Nagata, K., Resconi, G., Nakamura, T., Batle, J., Abdalla, S., Farouk, A.: MOJ Ecology and Environmental Science **2**(1), 00010 (2017)