Contents lists available at ScienceDirect

Results in Physics

journal homepage: www.elsevier.com/locate/rinp

A quantum algorithm based on entanglement measure for classifying Boolean multivariate function into novel hidden classes

Mohammed Zidan[a,b,*], Abdel-Haleem Abdel-Aty[c,d], Duc Manh Nguyen[e], Ahmed S.A. Mohamed[a,f], Yazeed Al-Sbou[g], Hichem Eleuch[h,i], Mahmoud Abdel-Aty[a,b,j]

[a] *University of Science and Technology, Zewail City of Science and Technology, October Gardens 12578, 6th of October City, Giza, Egypt*
[b] *Center for Photonics and Smart Materials (CPSM), Zewail City of Science and Technology, October Gardens, 6th of October City, Giza 12578, Egypt*
[c] *Department of Physics, College of Sciences, University of Bisha, Bisha 61922, P.O. Box 344, Saudi Arabia*
[d] *Physics Department, Faculty of Science, Al-Azhar University, 71524 Assiut, Egypt*
[e] *Coding and Information Theory Lab, University of Ulsan, Ulsan 44610, South Korea*
[f] *Department of Engineering Mathematics and Physics, Faculty of Engineering, Cairo University, Giza 12613, Egypt*
[g] *Deanship of Research and Graduate Studies, Applied Science University, P.O. Box 5055, 55222 Manama, Bahrain*
[h] *Department of Applied Sciences and Mathematics, College of Arts and Sciences, Abu Dhabi University, Abu Dhabi, United Arab Emirates*
[i] *Institute for Quantum Science and Engineering, Texas A&M University, College Station, TX 77843, USA*
[j] *Department of Mathematics, Faculty of Science, Sohag University, Sohag, Egypt*

ARTICLE INFO

Keywords:
Quantum information
Quantum algorithm
Deutsch-Jozsa algorithm
Quantum entanglement measure

ABSTRACT

In this paper, we propose a novel algorithm that solves a generalized version of the Deutsch-Jozsa problem. The proposed algorithm has the potential to classify an oracle U_F, that represents an unknown Boolean function on n Boolean variables, to one of 2^n different classes instead of only two classes which are constant and balanced classes in the case of Deutsch-Jozsa algorithm. The proposed algorithm is based on the use of entanglement measure to explore $2^n - 2$ additional classes compared to the standard Deutsch-Jozsa algorithm. In addition, the comparison between the proposed quantum algorithm and the classical one is investigated in details. The comparison shows that the proposed algorithm is faster when the number of Boolean variables exceed 14 variables.

1. Introduction

Quantum processing devices have proved powerful capabilities in solving the factorization problem used by the RSA algorithm, searching from unordered sets, and distributing encryption key with unconditional security [1]. The algorithms based on quantum computing devices have a better efficiency than the best algorithm in classical computing devices [2]. The notation of quantum computing was first proposed in 1982 by Richard Feynman [3]. A classical computer has a memory made up of bits, where each bit is either a zero or a one. In contrast, quantum computer maintains a sequence of qubits, which can represent a one, zero, or any quantum superposition state [4]. Subsequently, quantum evolution, and quantum measurements are involved [5] and became the most important parts in quantum systems [6–13].

In 1994, Peter Shor proposed quantum algorithm for integer factorization [14]. The algorithm runs on polynomial time, which is faster than the best classical algorithm and promises to defeat the best secured RSA cryptography system by implementing it in the large quantum computer. In addition, the quantum search algorithm is proposed by Grover [15], which could implement the search of an N-item database in $O(\sqrt{N})$ steps; in contrast, the classical algorithm must spend $O(N)$ steps. Therefore, the performance of quantum algorithms has significant improvements in comparison with the best classical algorithm. Since many quantum algorithms have been considered, in 1992, Deutsch and Jozsa proposed an algorithm which is specially designed to be easy for a quantum algorithm and hard for any deterministic classical algorithm [16]. It was also shown that the Deutsch-Jozsa algorithm can be applied to construct the quantum key distribution protocol [17]. Subsequently, secure quantum key distribution based on a special Deutsch-Jozsa algorithm using an entangled state [18], using a special function [19], and generalization in d-level quantum system [20,21] was explored.

One of the important features of quantum mechanics is quantum entanglement [22–24,39]. Since quantum entanglement is a physical phenomenon that occurs when two or more particles are interacted in the way such that the quantum state of each particle can not be

[*] Corresponding author.
E-mail address: comsi2014@gmail.com (M. Zidan).

https://doi.org/10.1016/j.rinp.2019.102549
Received 20 May 2019; Received in revised form 29 July 2019; Accepted 29 July 2019
Available online 09 August 2019

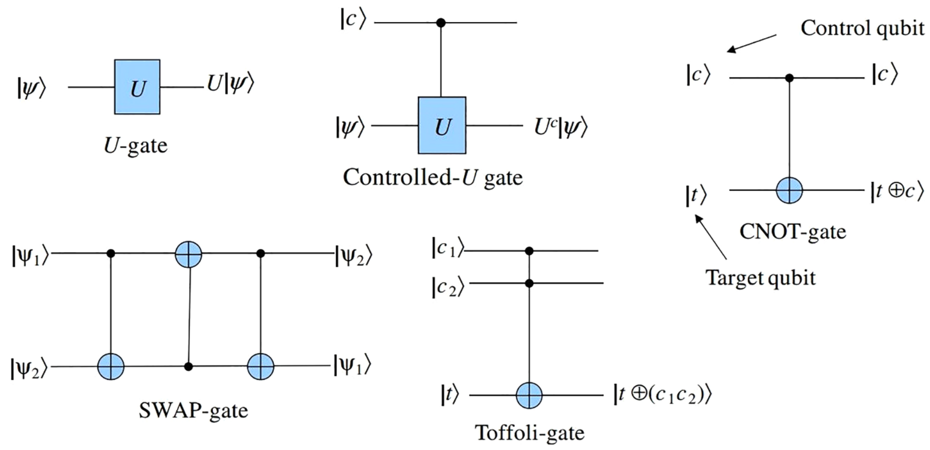

Fig. 1. Important quantum gates and their actions.

described independently of the others, even when the particles are separated by a large distance. Entanglement has become the main phenomenon in a lot of applications of quantum computation and quantum information such as in teleportation [36], in entanglement-assisted quantum error correction codes [37,38], etc. Since entanglement can not be detected directly, entanglement measures were proposed to determine the degree of the entanglement in quantum system [40,44–46]. One of those measures is called concurrence, which can measure the degree of entanglement between two arbitrary qubits [45,46]. Originally, the purpose of the Deutsch-Jozsa algorithm is to classify an unknown Boolean function F, of n Boolean variables, that is provided through an orcale U_F into one of the two classes: balanced or constant, quantum algorithm solve this problem via only one query. Although there are 2^{2^n} possible Boolean functions can be generated for the n Boolean variables, but Deutsch-Jozsa algorithm can classify only two classes among these functions: constant Boolean functions class and balanced Boolean function class. In this paper, we propose a novel algorithm that can solve a more general form rather than Deutsch-Jozsa algorithm. The proposed algorithm harness the power of concurrence measure to quantify the degree of entanglement between two qubits in order to classify an unknown Boolean function F, of n Boolean variables, that is provided through an oracle U_F into one of 2^n different classes. Therefore, the proposed algorithm has the potential to classify an oracle U_F to one of 2^n different classes instead of only two classes which are constant and balanced classes in the case of Deutsch-Jozsa algorithm.

The organization of this paper is as follows. In Section 2, we briefly introduce the quantum state, quantum evolution, and some quantum gates. Section 3 shows the proposed entanglement measure operator that will be used to propose our algorithm. In Section 4, the original Deutsch-Jozsa algorithm is explained. The proposed algorithm and its analysis are explained in details in Section 5. The complexity of proposed algorithm is analyzed in Section 6. Finally, the conclusions are presented in Section 7.

2. Preliminaries

Bit or binary digit is the basic unit of information used in classical computing and digital communication. The basic unit of quantum information is the quantum bit (*qubit*). But if *bit* has two basic state of 0 or 1, the qubit state is the superposition of two basic states. It is necessary to use the mathematical model of quantum information. For this purpose, we use the two-dimensional Hilbert space (H). The basic states are

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

and the superposition state is denoted as

$$|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = a\ |0\rangle + b\ |1\rangle,$$

where the complex numbers a and b are called the probability amplitudes satisfy $|a|^2 + |b|^2 = 1$. As a consequence, the information which is represented in quantum state is unlimited. Generally, the quantum register is formed by n qubits physical system where n times tensor product of two-dimensional Hilbert space. The state of a system of n qubits is denoted as:

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} a_i\ |i\rangle.$$

Quantum system requires the unitary transformations on quantum states. Each transformation operator is a combination of the Pauli matrices. We can consider the Pauli operator as the non-phase form as following:

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ \mathbf{Y} = \mathbf{iXZ}.$$

Pauli matrices includes **X** (bit flip), **Z** (phase flip), and **Y** (the combination of bit and phase flips). The Pauli group P_1 for one qubit is closed under multiplication, which formed by **X**, **Z** and **Y**. We have: $P_1 = \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$. Generally, the n-qubit Pauli group, P_n is the n-times tensor product of Pauli group P_1. P_n has the following property: any two vectors in P_n are either commutative or anti-commutative. Therefore, all the quantum evolutions, such as phase shift, swap, controlled-NOT, Toffoli gates, are defined as the combination of all the elements of Pauli matrices. In addition, the Hadamard gate plays an important role in the quantum evolution. Since Hadamard gate changes the basis states into the superposition quantum states and a quantum superposition state can also be reverted to basis states by Hadamard gate, which is involved in all most quantum algorithm and quantum protocol. In classical evolution, AND and NOT gates form the set of the classical logical gates. In quantum evolution, phase-shift gate, Hadamard, and controlled-NOT form the set of quantum logical gates. Some of those quantum gates and their action are listed in Fig. 1.

3. Methodology: Entanglement measure

Entanglement is a type of the quantum correlations [7–11,13,41–43] that distinguishes the behavior of quantum mechanics. A two-qubit system becomes an entangled state if the state of one qubit cannot be separated from the state of the other. Entanglement cannot be detected directly, so entanglement measures [25–27] were proposed to determine the degree of entanglement in a quantum system. They measure the strength of the entanglement between two-qubit or multiple-qubit systems such as concurrence, witness, and

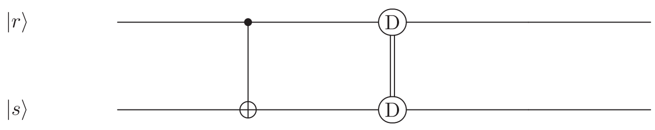

Fig. 2. Quantum circuit of M_z operator when applied on two qubits $|r\rangle$ and $|s\rangle$, where $|r\rangle$ is the control qubit and $|s\rangle$ is the target qubit.

negativity among others [26,28,29]. The strength of entanglement in a two-qubit system is often measured using concurrence measure [26,27]. For an arbitrary pure two-qubit state that is defined as follows:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle,$$

its concurrence C is calculated by [45]:

$$C = 2|ad - bc|,$$

where $0 \leqslant C \leqslant 1$. Suppose there is given a two-qubit system has the state

$$|\psi\rangle = a|00\rangle + d|11\rangle, \quad (1)$$

the concurrence value C becomes[30]

$$C = 2|ad|. \quad (2)$$

In 2018, Zidan et al. [31] proposed to use concurrence measure operator, denoted M_z that has the circuit model shown in Fig. 2, to solve some quantum computation problems. Then, some researchers used this operator to propose novel quantum computation and quantum machine learning algorithms [32–34]. According to the circuit model which is shown in Fig. 2, the operator M_z is a unitary operator that applies the *CNOT* gate between the qubits $|r\rangle$ and $|s\rangle$ followed by measuring the degree of entanglement in between through the operator D using concurrence measure. The main objective of the M_z is to distinguish between the states $a|0\rangle + d|1\rangle$ and $|0\rangle$. In sense that, if the state of the qubit $|r\rangle$ is $|r\rangle = a|0\rangle + d|1\rangle$, then the M_z operator creates the entangled state $a|00\rangle + d|11\rangle$ by applying the *CNOT* gate between the qubits $|r\rangle$ and $|s\rangle$, where the qubit $|s\rangle$ is always initialized in the state $|s\rangle = |0\rangle$. Then M_z measures the concurrence between the qubits $|r\rangle$ and $|s\rangle$ as $C > 0$ through the operator D. On the other hand, the M_z leaves them disentangled in the state $|rs\rangle = |00\rangle$ and measures the concurrence value in between as $C = 0$ through the operator D only if the given qubit $|r\rangle$ is in the state $|r\rangle = |0\rangle$. The operator D can be implemented using experimental setups [27,30,35], however, here, we propose a novel circuit model that implements the operator D that quantifies the concurrence value C for the two-qubit pure state given by Eq. (1). This circuit requires two decoupled copies of the two-qubit pure state $|\psi\rangle \otimes |\psi\rangle$ given by Eq. (1) as shown in Fig. 4, and it performs according to the following steps:

1. Prepare two decoupled copies of the two-qubit state given by Eq. (1) as follows:

   $$|\eta\rangle = |\psi\rangle \otimes |\psi\rangle = (a|00\rangle + d|11\rangle) \otimes (a|00\rangle + d|11\rangle).$$

   Therefore, the state of the system is as follows:

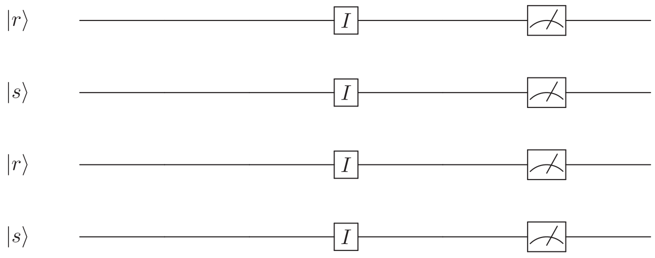

Fig. 3. The proposed circuit model of the operator D that measures the concurrence value between two arbitrary qubits $|r\rangle$ and $|s\rangle$.

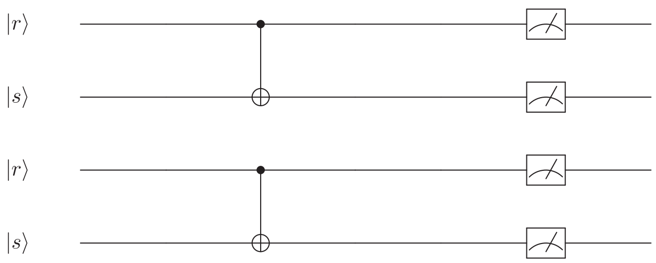

Fig. 4. The circuit model of the operator M_z that distinguishes between the state of the qubit $|r\rangle$ either in the state $|r\rangle = a|0\rangle + d|1\rangle$ or $|r\rangle = |0\rangle$ based on the degree of entanglement ($0 < C \leqslant 1$) or the absence of entanglement ($C = 0$) between two qubits $|r\rangle|s\rangle$, respectively.

$$|\eta\rangle = a^2|0000\rangle + ad|0011\rangle + ad|1100\rangle + d^2|1111\rangle. \quad (3)$$

2. Measure the system and estimate the probability of the state $|0011\rangle$ or $|1100\rangle$ and calculate the concurrence value C using Eq. (4), which can be obtained by comparing Eqs. (2) and (3), we obtain

   $$C = 2\sqrt{P_{0011}} \quad or \quad C = 2\sqrt{P_{1100}}, \quad (4)$$

   where P_{0011} and P_{1100} are the success probabilities for obtaining the state $|0011\rangle$ and $|1100\rangle$, respectively.

By implementing the operator D, given in Fig. 2, into the circuit model depicted in Fig. 3, the new circuit model of the M_z operator becomes as shown in Fig. 4. It is obvious that M_z operator applies two main operations. In the first operation, the *CNOT* gate is applied on each replica of the two-qubit systems $|r\rangle$ and $|s\rangle$ as the control qubit and as a target qubit, respectively. Accordingly, there are two cases:

(i) The state of each replica of the two-qubit $|rs\rangle$ system will be entangled, $|rs\rangle = a|00\rangle + d|11\rangle$, only if $|r\rangle = a|0\rangle + d|1\rangle$. Consequently, the second operation of the operator M_z applies the operator D on the state $|rs\rangle \otimes |rs\rangle$ as shown in Fig. 4. Therefore, the state of the system is described by Eq. (3) and the concurrence can be estimated using one of the formulas shown in Eq. (4).

(ii) On the other hand, the state of the system will be separable in the state $|rs\rangle = |00\rangle$ only if the state of the qubit $|r\rangle$ is $|0\rangle$. Again, when the second operation of the operator M_z applies the operator D on the state $|rs\rangle \otimes |rs\rangle$ as shown in Fig. 4. Therefore, the state of the system is as follows:

$$|\eta\rangle = |0000\rangle.$$

So, in this case the concurrence value is $C = 0$. Eventually, it is clear that the operator D in M_z is a unitary operator that measures the concurrence value C between the two qubits $|r\rangle$ and $|s\rangle$, by estimating the probability of the state $|0011\rangle$ or $|1100\rangle$ according to Eq. (4). M_z is used in the last step into the proposed algorithm (see Section 5.2).

4. Original Deutsch-Jozsa algorithm

We consider the function F: $\{0, 1\}^n \rightarrow \{0, 1\}$. Function F receives the binary string of length n and returns the values 0 or 1. The domain of function F can be considered as the integer numbers in $0, 1, \ldots, 2^{n-1}$. Hence, the function F is called to be *balanced* if a half of the inputs returns value 0 and a half of the inputs returns the value 1. When all the inputs return the value 0 or 1, we call the function F to be *constant*. The Deutsch-Jozsa algorithm aims to solve the problem: assume the function F is given and it can be evaluated via an oracle U_F. In this case, it is sure that F is in the type of balanced or constant; which is the best way to determine the type of function F. In classical computation, we must evaluate function F on the different inputs. The best case gives us only

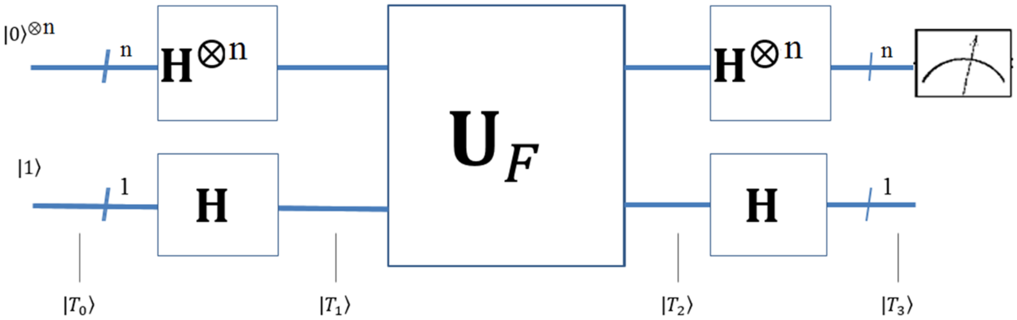

Fig. 5. Quantum circuit of Deutsch-Jozsa algorithm.

two queries to conclude the type of function. In contrast, the worst case requires $2^{n-1}+1$ queries which is more than a half of the possible inputs to ensure that the function type is constant or not.

In quantum computation, we can evaluate the type of function F in only one query. The quantum evolutions are given in Fig. 5. The details of the system after each step is explained as follows:
Step 1: The initial qubit state:

$$|T_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle \tag{5}$$

Step 2: We apply the Hadarmard evolution on the $n+1$ qubits to get the superposition with the same probability:

$$|T_1\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{i=\{0,1\}^n} |i\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]\right) \tag{6}$$

Step 3: The type of function F is applied by using the unitary evolution $\mathbf{U}_F$: $|x, y\rangle \to |x, y \oplus F(x)\rangle$, we have:

$$|T_2\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{i=\{0,1\}^n} (-1)^{F(i)}|i\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]\right) \tag{7}$$

Step 4: Then, we use again Hadamard evolution to the top n qubits to decode superposition state into basis states.

$$|T_3\rangle = \left(\frac{1}{2^n} \sum_{i=\{0,1\}^n} (-1)^{F(i)}|0\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]\right). \tag{8}$$

The top n qubits of $|T_3\rangle$ become

$$\frac{1}{2^n} \sum_{i=\{0,1\}^n} (-1)^{F(i)}|\mathbf{0}\rangle = \begin{cases} -1\ |\mathbf{0}\rangle & \text{if} F \text{is} \textit{constant} \text{ at} 1, \\ +1\ |\mathbf{0}\rangle & \text{if} F \text{is} \textit{constant} \text{ at} 0. \\ 0\ |\mathbf{0}\rangle & \text{If} F \text{is} \textit{balance}. \end{cases} \tag{9}$$

Step 5: Measurement: We now do measurements on the top qubits of $|T_3\rangle$. If the result is 0s, we conclude that the type of function F is *constant*. Otherwise, we conclude that the type of function is *balanced*.

5. Extended Deutsch-Jozsa Problem

5.1. Problem statement

Deutsch-Jozsa algorithm is the extension of the original Deutsch algorithm from one variable to n variables, which can determine the type of a given function (that is defined by an oracle U_F) constant or balanced exponentially speed-up rather than classical algorithms. Indeed, for n variables there are 2^{2^n} possible functions. Deutsch-Jozsa algorithm classifies two functions of those as a constant function and has the ability to classify only the balanced functions among the remaining $2^{2^n}-2$ possible functions. Here, we propose a more general form of Deutsch-Jozsa algorithm according to the following definition.

Definition. For an oracle U_F, it represents an unknown Boolean function F: $\{0, 1\}^n \to \{0, 1\}$. There exists a number r_c of the possible values of the Boolean variables $(x_1, x_2, \ldots, x_n)$ which satisfy $F(x_1, x_2, \ldots, x_n) = 1$. If $r_c = \frac{N}{2}$, then this Boolean function F is called a balanced Function. But If $r_c = 0$ or $r_c = N = 2^n$, then this Boolean function F is called a constant function. Otherwise, the Boolean function F belongs to the class label r_c.

In this paper, we define the balanced function as the function that maps half possible 2^n inputs to output 1. Our proposed problem classifies a given oracle U_F into one of three classes. The first class contains two constant functions. The second class contains $\frac{N!}{\left(\frac{N}{2}!\right)^2}$ balanced functions. While each class r_c, $0 < r_c < N$, $r_c \neq \frac{N}{2}$, of the rest $N-2$ classes contains $\frac{N!}{r_c!(N-r_c)!}$ possible Boolean functions, for example Table (1) shows the possible class labels $r_c = 2^2$ of two Boolean variables.

The abstract problem can be defined as follows:

- Given: An oracle U_F represents an unknown Boolean function F: $\{0, 1\}^n \to \{0, 1\}$.
- Goal: Return the class label r_c that contains the oracle U_F.

5.2. The proposed algorithm

Here, we proceed to show the steps of the proposed algorithm based on entanglement measure (the concurrence) as follows:

1.Register preparation: initialize the two quantum registers as a tensor product of the register $|\chi\rangle = |0\rangle^{\otimes n}$ and two ancillary qubits $|rs\rangle = |00\rangle$ as follows:

$$|\xi_0\rangle = |\chi\rangle \otimes |rs\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes 2}.$$

2.$|\xi_1\rangle = H^{\otimes n}|\chi\rangle \otimes I^{\otimes 2}|rs\rangle$.

Table 1
The 2^N possible Boolean functions F: $\{0, 1\}^2 \to \{0, 1\}$.

x_0	x_1	Constant $r_c = \{0, 4\}$		Balanced $r_c = 2$						Class $r_c = 1$				Class $r_c = 3$			
0	0	0	1	1	1	1	0	0	0	1	0	0	0	1	0	1	1
0	1	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	1
1	0	0	1	0	1	0	1	0	1	0	0	1	0	1	1	1	0
1	1	0	1	0	0	1	0	1	1	0	0	0	1	0	1	1	1

3.$|\xi_2\rangle = U_F|\chi, r\rangle \otimes I|s\rangle$.

4.Repeat the steps 1, 2, and 3 to get another copy of $|rs\rangle$ because M_z operator needs two copies of $|rs\rangle$ to quantify the degree of entanglement in between (see Section 3).

Remark: this step does not violate the non-cloning theorem [47] because when steps 1, 2, and 3 are repeated, a new different system is initialized in the first step and when the second and third steps are applied then a new copy of $|rs\rangle$ is created, independently, without cloning the original state.

5.Apply the operator M_z, shown in Fig. 4, on the two copies of the state $|rs\rangle$ and estimate P_{0011} or P_{1100} to quantify the concurrence value C according to Eq. (4) and estimate the P_{0000} and P_{1111}, where P_{0000}, P_{0011}, P_{1100} and P_{1111} are the probabilities of the states $|0000\rangle$, $|0011\rangle$, $|1100\rangle$ and $|1111\rangle$, respectively.

(i)If $P_{0000} > P_{1111}$ then $U_F \in$ the class label r_c,

$$r_c = \frac{N}{2}(1 - \sqrt{1 - C^2}).$$

(a)If $r_c = 0$ then U_F is the constant function $F(x_1, x_2, ..., x_n) = 0$.

(b)If $r_c = \frac{N}{2}$ then U_F is a balanced function.

(c)If $0 < r_c$ and $r_c \neq \frac{N}{2}$ then $U_F \in$ the class label r_c.

(ii)If $P_{0000} \leqslant P_{1111}$ then $U_F \in$ the class label r_c,

$$r_c = \frac{N}{2}(1 + \sqrt{1 - C^2}).$$

(a)If $r_c = N$ then U_F is the constant function $F(x_1, x_2, ..., x_n) = 1$.

(b)If $r_c = \frac{N}{2}$ then U_F is a balanced function.

(c)If $0 < r_c$ and $r_c \neq \frac{N}{2}$ then $U_F \in$ the class label r_c.

5.3. Analysis of the proposed algorithm

In Step 1, we initialize the system by the quantum registers $|\chi\rangle$ of size n qubit and two ancilla qubits $|r\rangle \otimes |s\rangle$, where all the qubits are initialized in the state $|0\rangle$. In Step 2, The Hadamard gate is applied on each qubit of the register $|\chi\rangle$ to generate a uniform superposition, that contains all possible values of the Boolean variables $(x_1, x_2, ..., x_n)$, therefore the state of the quantum system is as follows:

$$|\xi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|00\rangle.$$

In step 3, the oracle U_F is applied on the register $|\chi\rangle$ and the qubit $|r\rangle$ as U_f: $|\chi, r\rangle = |\chi, r \oplus F(\chi)\rangle$, so the state of the quantum system is as follows:

$$|\xi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k, 0 \oplus F(k)\rangle|0\rangle.$$

Here, the state of the qubit $|r\rangle$ can be described as follows:

$$|r\rangle = \sqrt{\frac{m_0}{N}}|0\rangle + \sqrt{\frac{r_c}{N}}|1\rangle, \tag{10}$$

where m_0 represents the number of the states that correspond to $F(k) = 0$, and r_c represents the number of the states that correspond to $F(k) = 1$, where $k = 0, 1, ..., 2^n - 1$, therefore

$$N = m_0 + r_c. \tag{11}$$

In step 4, the steps 1, 2 and 3 are repeated to generate a duplicate of the two-qubit system $|rs\rangle$. This step does not violate the no-cloning theorem [47], because M_z operator requires two copies to quantify the degree of entanglement between the qubits $|r\rangle$ and $|s\rangle$ as explained in Section 3. In other words, this step does not violate the non-cloning theorem [47] because when steps 1, 2 and 3 are repeated, a new different system is initialized in the first step and when the second and third steps are applied then a new copy of $|rs\rangle$ is created, independently, without cloning the original state. So, after this step, we have two replica of the two-qubit $|rs\rangle$ which is given as follows:

$$|rs\rangle = \sqrt{\frac{m_0}{N}}|00\rangle + \sqrt{\frac{r_c}{N}}|10\rangle. \tag{12}$$

Finally, in step 5, the M_z operator is applied on the two copies of $|rs\rangle$, which allows application of two consequence operations. In the first operation, the M_z operator applies the CNOT-gate between the two qubits $|r\rangle$ and $|s\rangle$ whose state is described by Eq. (12). After applying this operation, the state of $|rs\rangle$ is described as follows:

$$|rs\rangle = \sqrt{\frac{m_0}{N}}|00\rangle + \sqrt{\frac{r_c}{N}}|11\rangle. \tag{13}$$

In the second operation, the M_z operator quantifies the concurrence value C between the two qubits $|r\rangle$ and $|s\rangle$ by estimating the probability of the state $|0011\rangle$ or $|1100\rangle$ and use Eq. (4) to quantify the concurrence value C. Taking into account Eq. (13), then Eq. (3) will be as follows:

$$|\eta\rangle = \frac{m_0}{N}|0000\rangle + \frac{\sqrt{m_0 r_c}}{N}|0011\rangle + \frac{\sqrt{m_0 r_c}}{N}|1100\rangle + \frac{r_c}{N}|1111\rangle. \tag{14}$$

Then from Eq. (14), Eq. (11), and Eq. (4) the concurrence value C is calculated as follows:

$$C = 2\sqrt{P_{0011}} = 2\sqrt{P_{1100}} = 2\frac{\sqrt{m_0 r_c}}{N} = 2\frac{\sqrt{(N - r_c)r_c}}{N}.$$

So, it is clear that this function is a quadratic equation in terms of r_c as follows:

$$r_c^2 - Nr_c + \frac{C^2N^2}{4} = 0.$$

which has the following two roots

$$r_c = \frac{N}{2}(1 \pm \sqrt{1 - C^2}), \tag{15}$$

one of these roots represents the number of states that make the oracle U_F satisfies $F(x_1, x_2, ..., x_n) = 1$. The other root represents the number of states which make the oracle U_F satisfies $F(x_1, x_2, ..., x_n) = 0$. According to the definition, to determine which root among Eq. (15) represents the class label r_c of the oracle U_F, we need to determine the most likelihood probability among the states $|0000\rangle$ and $|1111\rangle$ in the state defined by Eq. (14). If the number of states which make $F(x_1, x_2, ..., x_n) = 1$ is greater than the number of states which make $F(x_1, x_2, ..., x_n) = 0$, this makes the probability of the state $|1\rangle$ will be the most likelihood compared to the probability of the state $|0\rangle$ in Eq. (10). Consequently, the probability of the state $|1111\rangle$ will be the most likelihood compared to the probability of the state $|0000\rangle$ in Eq. (14). Therefore, the root $\frac{N}{2}(1 + \sqrt{1 - C^2})$ represents the class label r_c for the oracle U_F. On the other hand, if the number of states which make $F(x_1, x_2, ..., x_n) = 0$ is greater than the number of states which make $F(x_1, x_2, ..., x_n) = 1$, this implies that the probability of the state $|0\rangle$ will be the most likelihood compared with the probability of the state $|1\rangle$ in Eq. (10). Consequently, the probability of the state $|0000\rangle$ will be the most likelihood compared to the probability of the state $|1111\rangle$ in Eq. (14). Therefore, the root $\frac{N}{2}(1 - \sqrt{1 - C^2})$ represents the class label r_c of the oracle U_F. It is worth noting that, if all the states satisfy that $F(x_1, x_2, ..., x_n) = 0$, this implies that the probability of the state $|0\rangle$ is 1 in Eq. (10). Consequently, the probability of the state $|0000\rangle$ is 1 in Eq. (14) and theconcurrencevalue C vanishes according to Eq. (4). Therefore, the root $r_c = 0$ indicates that the oracle U_F represents the constant function $F(k) = 0, \forall\ k = 0, 1, ..., 2^n - 1$. Conversely, if all the states satisfy that $F(x_1, x_2, ..., x_n) = 1$, this implies that the probability of the state $|1\rangle$ is 1 in Eq. (10). Consequently, the probability of the state $|1111\rangle$ is 1 in Eq. (14) and the concurrence value C vanishes also according to Eq. (4). Therefore, the root $r_c = N$ indicates that the oracle U_F represents the constant function $F(k) = 1, \forall\ k = 0, 1, ..., 2^n - 1$. Finally, if the number of states which make $F(x_1, x_2, ..., x_n) = 1$ equals to the number of states

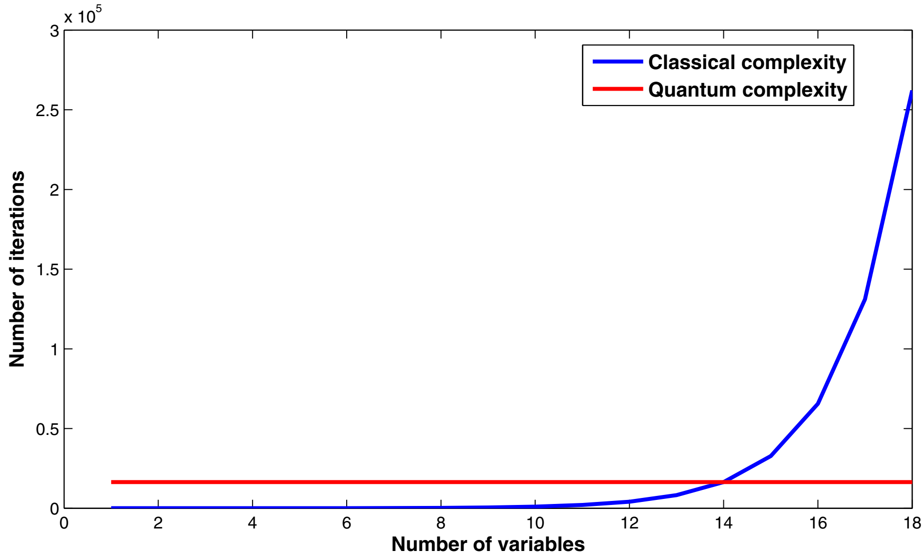

Fig. 6. The complexity comparison between proposed algorithm and classical algorithm to solve the proposed generalized version of Deutsch-Jozsa's problem as the number of Boolean variables $\leqslant 18$.

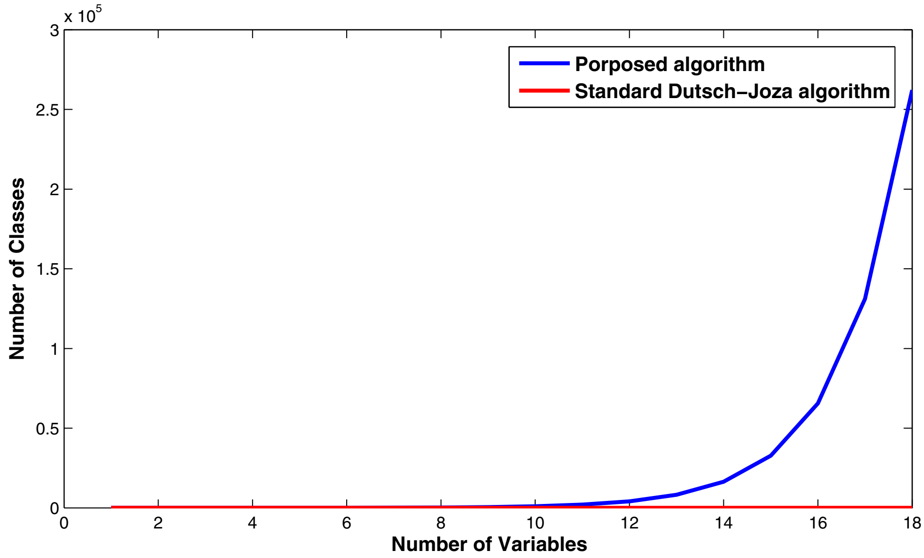

Fig. 7. Comparison between the number of classes which are classified via the proposed algorithm and the standard Deutsch-Jozsa algorithm as a function the number of Boolean variables.

which make $F(x_1, x_2, ..., x_n) = 0$, then the probability of the state $|1\rangle$ equals to the probability of the state $|0\rangle$ in Eq. (10). Consequently, the probability of the state $|1111\rangle$ equals to the probability of the state $|0000\rangle$ in Eq. (14). Hence, the concurrence is maximal ($C = 1$). Therefore, the root $r_c = \frac{N}{2}$ indicates that the oracle U_F belongs to the balanced Boolean functions class.

6. Complexity

In this section, we investigate the complexity of the proposed algorithm. It is clear from the proposed algorithm that recognizing the class label r_c to which the oracle U_F belongs depends on the value of the concurrence C. The concurrence value C can be quantified by estimating the probability of the state $|0011\rangle$ or $|1100\rangle$ according to Eq. (4). So, the oracle U_F should be recalled multiple times to estimate the probability of one of these states. The number of measurements which can be performed using IBM's real quantum computer is 1024, 4092 or 8192. Here, we consider that the proposed algorithm can be implemented on IBM's real quantum computer using its maximum number of measurements which is 8192. Then, the proposed algorithm needs to recall the oracle U_F with $2(8192) = 2^{14}$ times to perform 8192 measurements in order to estimate the concurrence value C via one of the states shown in Eq. (4). Therefore, we need to compare with the number of iterations that should be preformed to solve the same problem classically. It is clear from Fig. 6 that there are three remarks that can be recorded. First remark: as long as the number of variables is less than 14, the proposed algorithm is slower than classical computer taking into account that we consider the maximum number of practical quantum measurements to be 8192. Second remark: when the number of variables increases to be 14, then there is no difference between classical algorithms and the proposed algorithm. Third remark: we note that as the number of variables increases to be more than 14, the speed of the proposed algorithm increases dramatically compared with classical computers. It is lucid from Fig. 7 that the proposed algorithm classifies an oracle U_F to an exponential classes greater up compared with the standard Deutsch-Jozsa algorithm which always classifies the same oracle to only two classes even if the number of variables tends to be very huge. This concludes that the proposed algorithm is efficient when the number of variables is greater than 14 and can classify an exponential number of classes compared with the standard Deutsch-Jozsa algorithm. Finally, the realization of the proposed algorithm when the number of Boolean variables is 14 on IBM's real quantum computer requires 32 qubits which is not available for us today.

7. Conclusion

In this paper, we have proposed a novel algorithm that has the ability to solve a generalized version of Deustsh-Jozsa 's algorithm. We have also proposed novel circuit model for realization of M_z operator. This circuit is used as a key step in the proposed algorithm that can classify a black box U_F to 2^n different class labels. The analysis and the complexity of the proposed algorithm are investigated.

References

[1] Nielsen MA, Chuang IL. Quantum computation and quantum information. Cambridge, UK: Cambridge University Press; 2000.

[2] Von Neumann J. Mathematical foundations of quantum mechanics. Princeton, New Jersey: Princeton University Press; 1955.

[3] Feynman R. Simulating physics with computers. Int J Theor Phys 1982;21:467.

[4] Gaitan F. Quantum error correction and fault tolerant quantum computing. FL. USA: CRC Press. Inc., BocaRaton; 2007.

[5] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. J Cryptol 1992;5(1):3–28.

[6] Feynman RP, Leighton RB, Sands M. Lectures on Physics. Volume III. Quantum mechanics Addison-Wesley Publishing Company; 1965.

[7] Abdel-Aty M. Quantum information entropy and multi-qubit entanglement. Progress Quantum Electron 2007;31(1):1–49.

[8] Abdalla MS, Abdel-Aty M, Obada A-SF. Degree of entanglement for anisotropic coupled oscillators interacting with a single atom. J Opt B: Quantum Semiclassical Opt 2002;4(6). pp. 396-40.

[9] Luo S, Fu S. Geometric measure of quantum discord. Phys Rev 2010;82:034302.

[10] Huang ZM, Qiu DW. Geometric quantum discord under noisy environment. Quantum Inf Process 1979;2016:15.

[11] Mohamed AB. Non-local correlation and quantum discord in two atoms in the non-degenerate model. Ann Phys 2012;327:3130–7.

[12] Luo S. Using measurement-induced disturbance to characterize correlations as classical or quantum. Phys Rev 2008;77:022301.

[13] Sete EA, Svidzinsky AA, Rostovtsev YV, Eleuch H, Jha PK, Suckewer S, Scully MO. Using quantum coherence to generate gain in the XUV and X-ray: gain-swept superradiance and lasing without inversion. IEEE J Sel Top Quantum Electron 2012;18:541–53.

[14] Shor PW. Scheme for reducing decoherence in quantum computer memory. Phys Rev A 1995;52:2493.

[15] Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett 1997;79:325.

[16] Deutsch D, Jozsa R. Rapid solutions of problems by quantum computation. Proc R Soc London A 1992.

[17] Nagata K, Nakamura T. The Deutsch-Jozsa algorithm can be used for quantum key distribution. Open Access Library J 2015;2:e1798.

[18] Nagata K, Nakamura T, Farouk A. Quantum cryptography based on the Deutsch-Jozsa algorithm. Int J Theor Phys 2017;56:2887–97.

[19] Nagata K, Nakamura T, Geurdes H, Batle J, Abdalla S, Farouk A. Secure quantum key distribution based on a special Deutsch-Jozsa algorithm. Asian J Math Phys 2018;2:6–13.

[20] Nguyen DM, Kim S. Quantum key distribution protocol based on modified generalization of Deutsch-Jozsa algorithm in d-level quantum system. Int J Theor Phys 2019;58(1):71–82.

[21] Nguyen DM, Kim S. Multi-bits transfer based on the quantum three-stage protocol with quantum error correction codes. Int J Theor Phys 2019;58(6):2043–53.

[22] Hill S, Wootters WK. Entanglement of a pair of quantum bits. Phys Rev Lett 1997;78:5022.

[23] Wootters WK. Entanglement of formation of an arbitrary state of two qubits. Phys Rev Lett 1998;80:2245.

[24] Barzanjeh S, Eleuch H. Dynamical behavior of entanglement in semiconductor microcavities. Phys E 2010;42:2091–6.

[25] Hill S, Wootters WK. Entanglement of a pair of quantum bits. Phys Rev Lett 1997;78:5022.

[26] Wootters WK. Entanglement of formation of an arbitrary state of two qubits. Phys Rev Lett 1998;80:2245.

[27] Zhou L, Sheng YB. Concurrence measurement for the two-qubit optical and atomic states. Entropy 2015;17:4293.

[28] Vidal G, Werner RF. Computable measure of entanglement. Phys Rev 2002;65:032314.

[29] Islam R, Ma R, Preiss PM, Tai ME, Lukin A, Rispoli M, Greine M. Measuring entanglement entropy in a quantum many-body system. Nature 2015;528:48.

[30] Walborn SP, Ribeior PHS, Davidovich L, Mintert F, Buchleitner A. Experimental determination of entanglement with a single measurement. Nature 2006;440:1022.

[31] Zidan M, Abdel-Aty A, Younes A, Zanaty EA, El-khayat I, Abdel-Aty M. A novel algorithm based on entanglement measurement for improving speed of quantum algorithms. Appl Math Inf Sci 2018;12:265–9.

[32] El-Wazan K, Younes A, Doma SB. A Quantum algorithm for testing junta variables and learning Boolean functions via entanglement measure. arXiv 2017, arXiv:1710.10495.

[33] El-Wazan K. A quantum algorithm for testing junta variables and learning Boolean functions via entanglement measure. arXiv 2019, arXiv:1903.04762.

[34] Zidan M, Abdel-Aty A-H, El-shafei M, Feraig M, Al-Sbou Y, Eleuch H, Abdel-Aty M. Quantum classification algorithm based on competitive learning neural network and entanglement measure. Appl Sci 2019;9:1277.

[35] Hong-Fu W, Shou Z. Application of quantum algorithms to direct measurement of concurrence of a two-qubit pure state. Chin Phys B 2009;18:2642.

[36] Nguyen DM, Kim S. Quantum stabilizer codes construction from Hermitian self-orthogonal codes over GF(4). J Commun Networks 2018;20(3):309–15.

[37] Nguyen DM, Kim S. Minimal-entanglement entanglement-assisted quantum error correction codes from modified circulant matrices. Symmetry 2017;9(7):122.

[38] Nguyen DM, Kim S. New constructions of quantum stabilizer codes based on difference sets. Symmetry 2018;10(11):655.

[39] Zhou L, Sheng YB. Concurrence measurement for the two-qubit optical and atomic states. Entropy 2015;17:4293.

[40] Vidal G, Werner RF. Computable measure of entanglement. Phys Rev 2002;65:032314.

[41] Sete EA, Eleuch H, Das S. Semiconductor cavity QED with squeezed light: nonlinear regime. Phys. Rev. A 2011;84(5):053817.

[42] Eleuch H. Quantum trajectories and autocorrelation function in semiconductor microcavity. Appl Math Inf Sci 2009;3(2):185–96.

[43] Abdel-Aty M, Abdalla MS, Obada A-SF. Entropy and phase properties of isotropic coupled oscillators interacting with a single atom: one- and two-photon processes. J Opt B: Quantum Semiclassical Opt 2002;4(3):S133–41.

[44] Islam R, Ma R, Preiss PM, Tai ME, Lukin A, Rispoli M, Greine M. Measuring entanglement entropy in a quantum many-body system. Nature 2015;528:48.

[45] Romero G, Løpez CE, Lastra F, Solano E, Retamal JC. Direct measurement of concurrence for atomic two-qubit pure states. Phys Rev 2007;75:032303.

[46] Walborn SP, Ribeior PHS, Davidovich L, Mintert F, Buchleitner A. Experimental determination of entanglement with a single measurement. Nature 2006;440:1022.

[47] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature 1982;299:802–3.