Computers, Materials & Continua
DOI:10.32604/cmc.2022.020103
Article

Tech Science Press

A Quantum Algorithm for Evaluating the Hamming Distance

Mohammed Zidan[1,2,*], Manal G. Eldin[3], Mahmoud Y. Shams[4], Mohamed Tolan[5,6], Ayman Abd-Elhamed[2,7] and Mahmoud Abdel-Aty[8]

[1]Department of Artificial Intelligence, Hurghada Faculty of Computers and Artificial Intelligence, South Valley University, Egypt
[2]Faculty of Engineering, King Salman International University, South Sinai, Egypt
[3]Department of Mathematics and Computer Science, Faculty of Science, Beni-Suef University, Beni-Suef, Egypt
[4]Department of Machine Learning and Information Retrieval, Faculty of Artificial Intelligence, Kafrelsheikh University, Egypt
[5]Mechanical Department, Faculty of Technology and Education, Suez University, Suez, Egypt
[6]Faculty of Technological Industries, King Salman International University, South Sinai, Egypt
[7]Faculty of Engineering at Mataria, Helwan University, Cairo, Egypt
[8]Department of Mathematics, Faculty of Sciences, Sohag University, 82524 Sohag, Egypt
[*]Corresponding Author: Mohammed Zidan. Email: comsi2014@gmail.com
Received: 09 May 2021; Accepted: 29 July 2021

Abstract: We present a novel quantum algorithm to evaluate the hamming distance between two unknown oracles via measuring the degree of entanglement between two ancillary qubits. In particular, we use the power of the entanglement degree based quantum computing model that preserves at most the locality of interactions within the quantum model structure. This model uses one of two techniques to retrieve the solution of a quantum computing problem at hand. In the first technique, the solution of the problem is obtained based on whether there is an entanglement between the two ancillary qubits or not. In the second, the solution of the quantum computing problem is obtained as a function in the concurrence value, and the number of states that can be generated from the Boolean variables. The proposed algorithm receives two oracles, each oracle represents an unknown Boolean function, then it measures the hamming distance between these two oracles. The hamming distance is evaluated based on the second technique. It is shown that the proposed algorithm provides exponential speedup compared with the classical counterpart for Boolean functions that have large numbers of Boolean variables. The proposed algorithm is explained via a case study. Finally, employing recently developed experimental techniques, the proposed algorithm has been verified using IBM's quantum computer simulator.

Keywords: Quantum computing; quantum algorithm; quantum circuit

1 Introduction

Quantum algorithms have enormous technological and recent progress to solve the problem that needs high-performance computing on traditional computers [1–3]. Nowadays, quantum

technologies stand at the crossroads between many areas of study, such as quantum information, combinatorics, computational complexity, and statistical mechanics [4–7].

Boolean functions play a critical role in cryptography, particularly in the design of symmetric key algorithms. Analyzing these functions can be done using many techniques, such as spectral techniques. The Hamming distance $H(f,g)$ is the natural distance between two binary strings. In 2014, De et al. [6] showed a quantum algorithm based on the Chow parameters problem of any n- bit linear threshold function f given that a high prodigality in the Hamming distance which runs in time $O(n^2).\left(\frac{1}{\epsilon}\right)^{O\left(\log^2\left(\frac{1}{\epsilon}\right)\right)}$.

Xie et al. [8] have calculated $H(f,g)$ with n inputs that require $O(1)$ with probability at least $8/\pi^2$ in some special cases by taking advantage of Walsh transform. Moreover, they proposed an optimal algorithm which requires $\theta(2^n)$ the exact query complexity with accuracy $O\left(\frac{N\nabla.\epsilon^2}{t+1}\right)$ classically. Other researchers proposed algorithms based on development of two Hamming distance using unlike types of inner products like gnomic quantum classifier [9]. In the context of quantum communication complexity, Doriguello et al. [10] proposed an efficient quantum communication protocol to approximately measure the Hamming distance between two n bit strings in the SMP model with some relative error ϵ. Their protocol uses $O\left(\frac{logn}{\epsilon^5}\right)$qubits of communication.

Recently, it was proposed that the degree of entanglement can be used efficiently to develop new quantum computing model [7]. A generalized version of the Deutsch-Jozsa problem was solved based on this quantum computing model [11]. Also, this model was used to propose quantum machine leaning algorithms based on this quantum computing model to perform competitive learning quantum mechanically [12,13]. Moreover, based on symmetric matrices in quantum stabilizer codes, a construction of binary and non-binary quantum stabilizer codes is presented by [14,15]. In this paper, a novel quantum algorithm computes the Hamming distance *Ham(f, g)* between two unknown Boolean functions. Concretely, it is proposed based on adding four ancilla qubits, and two extra CNOT gates in addition to the degree of entanglement-based quantum computing model [7]. The proposed algorithm retrieves *Ham(f, g)* between two given oracles U_f and U_g. Then, the complexity of the proposed algorithm is compared with the classical algorithm. Finally, the proposed algorithm is verified using IBM's quantum computer simulator.

The next part of this paper is organized, as follows: In Section 2, the methodology that is used to propose the algorithm is explained. Section 3 shows the problem statement, the proposed algorithm and analysis of the performance of the proposed algorithm via a case study. Also, the complexity of the proposed algorithm compared with classical algorithm is investigated in Section 3. Verification of the proposed algorithm on IBM's quantum computer simulator, and results discussion is performed in Section 4. Finally, main conclusions are discussed in Section 5.

2 Methodology

Recently, quantum computing model based on the degree of entanglement has been proposed [7]. This model utilizes concurrence measure to find the solution of some quantum problems based on the degree of entanglement C between two auxiliary qubits in a quantum system of n + 2, where n $\geq$ 0 [7,11–13]. In this model, the concurrence value C is estimated quantum mechanically via the operator Mz. Therefore, the solution of the quantum computing problems is obtained based on C. Moreover, it was proved that the operator Mz has the potential to distinguish between non-orthogonal states in the form $a_0|0\rangle + b_0|1\rangle$ by quantifying the degree of

entanglement between two qubits [12]. Suppose we have an arbitrary qubit in the state presented in Eq. (1) and demonstrated in Fig. 1.

$$|f(x)\rangle = a_0\ |0\rangle + b_0\ |1\rangle, \quad |a_0|^2 + |b_0|^2 = 1. \tag{1}$$

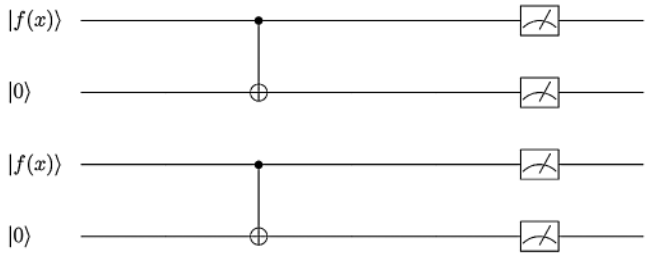


Figure 1: The circuit model of the operator $\boldsymbol{M_Z}$ that creates entanglement between the qubits |f(x)⟩ and |s⟩. Then, it measures the concurrence value quantum mechanically via $\boldsymbol{C} = \sqrt{2(\boldsymbol{P}_{0011} + \boldsymbol{P}_{1100})}$

Mz operator receives two decoupled replicas of two inputs. The first input is the qubit $|f(x)\rangle$ which has a state described by Eq. (1). The second input is a qubit $|s\rangle$ which is initialized in the state $|0\rangle$ while the operator Mz applies two operations.

In the first operation, the operator Mz creates entanglement between each replica of the two qubits |f(x)⟩ and |s⟩ individually and simultaneously. Hence, the state of each replica is defined by the state presented in Eq. (2).

$$|f(x)s\rangle = a_0\ |00\rangle + b_0\ |11\rangle. \tag{2}$$

This operation is achieved by applying $CNOT$ on each replica of the two qubits $|f(x)\rangle$ and |s⟩ individually and simultaneously, where the control and the target qubits are $|f(x)\rangle$ and |s⟩, respectively. The concurrence value C for the state described by Eq. (2) is defined as in Eq. (3) [12]:

$$C = 2|a_0 b_0|. \tag{3}$$

In the second operation, the operator Mz measures C between the two qubits |f(x)s⟩ by measuring the following two replica $|f(x)s\rangle \otimes |f(x)s\rangle$. Then, the concurrence value C between the two qubits $|f(x)\rangle$ and $|s\rangle$ is quantified on a quantum chip as shown in Eq. (4).

$$C = \sqrt{2(P_{0011} + P_{1100})}, \tag{4}$$

where $P0011$, $P1100$ are the probabilities of the states $|0011\rangle, |1100\rangle$, respectively. Therefore, the first technique of this computing model [12] finds the solution of the problem at hand based on the degree of entanglement C.

3 The Proposed Algorithm

In this section, we investigate the proposed algorithm for measuring the hamming distance between two functions including the problem statement, proposed algorithm, and performance analysis of the proposed algorithm by presenting a case study as in the following subsections.

3.1 Problem Statement

The Hamming distance between two functions f and g, each acting on n-variable provided via two black-boxes, is defined according to the following definition:

- **Definition:** The Hamming distance $Ham(f, g)$ between two Boolean functions $f(x)$ and $g(x)$ of $n-$ Boolean variables is defined as:-

  $Ham(f(x), g(x)) = |\{x \in \{0,1\}^n : f(x) \neq g(x)\}|$

The abstract problem of this paper can be defined, as follows:

- **Given:** Given two oracles represent two unknown Boolean functions such that

  $U_f : \{0,1\}^n \to \{0,1\}, and\ \ U_g : \{0,1\}^n \to \{0,1\}.$

- **Goal:** Retrieve the Hamming distance $Ham_\epsilon(f, g)$ *between* $f(x)$ *and* $g(x)$ such that:

  $(1-\epsilon)Ham(f,g) \leq Ham_\epsilon(f,g) \leq (1+\epsilon)Ham(f,g).$

3.2 The Proposed Algorithm

Now, the proposed algorithm that solves the above problem can be described, as follows:

(1) Step 1: Initialize the quantum register $|\psi\rangle$ of size n qubits, two disentangled qubits namely: $|y_f\rangle, |y_g\rangle$, and a two-qubit register $|\phi\rangle$. All of them are initialized in the vacuum state, $|0\rangle$, as follows:

$|\zeta_0\rangle = |\psi\rangle^{\otimes n} \otimes |y_f, y_g, \phi\rangle = |0\rangle^{\otimes n} \otimes |0,0,00\rangle.$

(2) Step 2: Apply the Hadamard gates to the first n qubits.

$$|\zeta_1\rangle = (H^{\otimes n} \otimes I^{\otimes 4})|\zeta_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0,0,00\rangle,$$

(3) Step 3: Apply the oracle U_f and on the first n qubits and the qubit $|y_f\rangle$, then the oracle U_g and on the first n qubits and the qubit $|y_g\rangle$:

$U_f|x, y_f\rangle = |x\rangle|y_f \oplus f(x)\rangle = |x\rangle|0 \oplus f(x)\rangle = |x\rangle|f(x)\rangle,$

$U_g|x, y_g\rangle = |x\rangle|y_g \oplus g(x)\rangle = |x\rangle|0 \oplus g(x)\rangle = |x\rangle|g(x)\rangle.$

So, the state of the system is as follows:

$$|\zeta_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x), g(x), 00\rangle.$$

(4) Step 4: Apply the CNOT gate twice, as follows:

$|\zeta_3\rangle = CNOT_{y_f\phi_1} CNOT_{y_g\phi_1} |\zeta_2\rangle.$

(5) Step 5: Repeat steps 1, 2, 3 and 4 to get a novel decoupled copy of the system $|\zeta_3\rangle$.

(6) Step 6: Apply Mz between on the two replica of the two qubits $|\phi_1\rangle\, and\, |\phi_2\rangle$,

If $P_{0000}>P_{1111}$, then $Ham(f(x),g(x))$ as in Eq. (5).

$$Ham(f(x),g(x))=\frac{N}{2}\left(1-\sqrt{1-C^2}\right). \tag{5}$$

If $P_{1111}\geq P_{0000}$, then $Ham(f(x),g(x))$ as in Eq. (6).

$$Ham(f(x),g(x))=\frac{N}{2}\left(1+\sqrt{1-C^2}\right), \tag{6}$$

where C is determined as in Eq. (4).

3.3 Performance Analysis of the Proposed Algorithm: Case Study

Here, we analyze the performance of the proposed algorithm via a case study. Assume we have the two Boolean functions $f(x)$ *and* $g(x)$, such that n = *2*, and corresponding results are defined as in Eq. (7).

$$\begin{aligned} &f(00)=0,\quad f(01)=0,\quad f(10)=1,\quad \text{and}\quad f(11)=1,\\ &g(00)=0,\quad g(01)=1,\quad g(10)=0,\quad \text{and}\quad g(11)=1. \end{aligned} \tag{7}$$

To determine the Hamming distance between $f(x)$ and $g(x)$, the steps of the proposed algorithm act, as follows: In Step1, because the number of Boolean variables is 2, so the size of the register $|\psi\rangle$ is n = 2 qubits. Consequently, the whole quantum system is in the following state: $|\zeta_0\rangle=|\psi\rangle^{\otimes n=2}\otimes|y_f,y_g,\phi\rangle=|\psi\rangle^{\otimes 2}\otimes|y_f,y_g,\phi\rangle=|00,0,0,00\rangle$.

In Step 2, the proposed algorithm applies 2 Hadamard gates on the first two qubits of the system $|\zeta_0\rangle$, so the state of the system is transformed to the following state:

$$|\zeta_1\rangle=(H^{\otimes 2}\otimes I^{\otimes 4}|\zeta_0\rangle=\sqrt{\frac{1}{4}}(|00,0,0,00\rangle+|01,0,0,00\rangle+|10,0,0,00\rangle+|11,0,0,00\rangle).$$

This step generates the whole domain of the two Boolean functions $f(x)$ and $g(x)$.

In Step 3, the proposed algorithm applies the oracle U_f on the first n qubits and the qubit $|y_f\rangle$, and applies the oracle U_g and on the first n qubits and the qubit $|y_g\rangle$ at the same time. Therefore, the state of the system after applying the Oracle U_f is as in Eq. (8).

$$\begin{aligned} |\zeta_2\rangle&=|x_0x_1,y_f\oplus f(x_0x_1),0,00)=\frac{1}{\sqrt{2}}\sum_{x=0}^{3}|x_0x_1,|f(x),0,00\rangle\\ &=\sqrt{\frac{1}{4}}[|00,0,0,00\rangle+|01,0,0,00\rangle+|10,1,0,00\rangle+|11,1,0,00\rangle]. \end{aligned} \tag{8}$$

Similarly, the state of the system after applying the Oracle U_g is as in Eq. (9).

$$\begin{aligned} |\zeta_2\rangle&=|x_0x_1,f(x),\ y_g\oplus g(x_0x_1),00)=\frac{1}{\sqrt{2}}\sum_{x=0}^{3}|x_0x_1,|f(x),g(x),00\rangle\\ &=\sqrt{\frac{1}{4}}[|00,0,0,00\rangle+|01,0,1,00\rangle+|10,1,0,00\rangle+|11,1,1,00\rangle]. \end{aligned} \tag{9}$$

In Step 4, the proposed algorithm applies 2 CNOT gates simultaneously as follows:

$|\zeta_3'\rangle = CNOT_{y_f\phi_1} CNOT_{y_g\phi_1}, |\zeta_2\rangle.$

By applying the $CNOT_{y_g\phi_1}$ gate, the control qubit $|y_g\rangle$ and the target qubit $|\phi_1\rangle$. Therefore the state of the entire system is evolved as shown in Eq. (10).

$$|\zeta_3''\rangle = \sqrt{\frac{1}{4}}[|00,0,0,00\rangle + |01,0,1,10\rangle + |10,1,0,00\rangle + |11,1,1,10\rangle] \tag{10}$$

At the same time, by applying the $CNOT_{y_f\phi_1}$ gate between the control qubit $|y_f\rangle$ and the target qubit $|\phi_1\rangle$. Then, the state of the system is described as in Eq. (11).

$$|\zeta_3\rangle = \sqrt{\frac{1}{4}}[|00,0,0,00\rangle + |01,0,1,10\rangle + |10,1,0,10\rangle + |11,1,1,00\rangle] \tag{11}$$

Now, it is clear from Eq. (11) that step 4 evolves the state of the qubit $|\phi_1\rangle$ to be in state $|1\rangle$ only if the two functions $f(x_i) \neq g(x_i)$. On other hand, the state of the qubit $|\phi_1\rangle$ is the state $|0\rangle$ only if $f(x_i) = g(x_i)$ for x_i. In Step 5, the steps 1–4 are repeated to construct another decoupled replica of the system $|\zeta_3\rangle$, because Mz operator works on two decoupled copies of the register $|\phi\rangle$ to quantify the degree of entanglement between the two qubits: $|\phi_1\rangle$ and $|\phi_2\rangle$ (see Section 2). In Step 6, the proposed algorithm applies the two operations of the operator Mz between the two qubits $|\phi_1\rangle$ and $|\phi_2\rangle$, for each replica, in the system defined by Eq. (11). In the first operation, the operator Mz applies the $CNOT_{\varphi 1\varphi 2}$ gate on each replica, where the $|\phi_1\rangle$ is the control qubit and $|\phi_2\rangle$ is the target qubit. In the general case, n Boolean variables, the state of each replica after applying the first operation of the operator Mz is described as in Eq. (12):

$$\begin{aligned} |\zeta_4\rangle &= (I^{\otimes n+2} \otimes CONT)|\zeta_3\rangle \\ &= \sqrt{\frac{t_1}{2^n}} \left(\frac{1}{\sqrt{t_1}} \sum_{x=\{x|f(x)=g(x)\}} \sum_{y_f y_g=\{00,11\}} |x\rangle|y_f y_{fg}\rangle \right) |00\rangle \\ &+ \sqrt{\frac{t_2}{2^n}} \left(\frac{1}{\sqrt{t_2}} \sum_{x=\{x|f(x)\neq g(x)\}} \sum_{y_f y_g=\{01,10\}} |x\rangle|y_f y_{fg}\rangle \right) |11\rangle \end{aligned} \tag{12}$$

Let,

$$\begin{aligned} &|\beta_1\rangle = \sum_{x=\{x|f(x)=g(x)\}} \sum_{y_f y_g=\{00,11\}} |x\rangle|y_f y_{fg}\rangle, \quad |\beta_2\rangle = \sum_{x=\{x|f(x)=g(x)\}} \sum_{y_f y_g\neq\{01,10\}} |x\rangle|y_f y_{fg}\rangle \\ &a_0 = \sqrt{\frac{t_1}{2^n}}, \quad \text{and} \quad b_0 = \sqrt{\frac{t_2}{2^n}}. \end{aligned} \tag{13}$$

Thus, Eqs. (12)–(13), the state system is summarized in Eq. (14).

$$|\xi^4\rangle = a_0|\beta_1\rangle|00\rangle + b_0|\beta_2\rangle|11\rangle. \tag{14}$$

According to Eq. (14), the first operation of the operator Mz applies the $CNOT_{\varphi 1\varphi 2}$ to entangle the two qubits: $|\phi_1\rangle$ and $|\phi_2\rangle$, where the degree of entanglement in between depends on the value of the hamming distance among the two-function $f(x)$ and $g(x)$ $(Ham(f(x), g(x)) > 0)$.

Conversely, the operator Mz maintains the two qubits: $|\phi_1\rangle$ and $|\phi_2\rangle$ separable only if the hamming distance among the two-function $f(x)$ and $g(x)$ $(Ham(f(x), g(x)) = 0)$.

Now, for this case study at hands, n = 2 and $|\zeta_3\rangle$ is defined by Eq. (11). The state of each replica after applying the first operation of the operator Mz is described according to Eq. (11) and Eqs. (12)–(14), as in Eq. (15).

$$\begin{aligned}
|\zeta_4\rangle &= \sqrt{\frac{1}{4}}[|00,0,0,00\rangle + |01,0,1,11\rangle + |10,1,0,11\rangle + |11,1,1,00\rangle]. \\
&= \sqrt{\frac{t_1}{2^n}}\left(\frac{1}{\sqrt{t_1}} \sum_{x=\{x|f(x)=g(x)\ \}} \sum_{y_f y_g=\{00,11\}} |x\rangle|y_f y_g\rangle\right)|00\rangle \\
&\quad + \sqrt{\frac{t_2}{2^n}}\left(\frac{1}{\sqrt{t_2}} \sum_{x=\{x|f(x)\neq g(x)\ \}} \sum_{y_f y_g=\{01,10\}} |x\rangle|y_f y_g\rangle\right)|11\rangle \\
&= \sqrt{\frac{2}{4}}\left(\frac{1}{\sqrt{2}} \sum_{x=\{00,11\ \}} \sum_{y_f y_g=\{00,11\}} |x\rangle|y_f y_g\rangle\right) \\
&\quad + \sqrt{\frac{2}{4}}\left(\frac{1}{\sqrt{2}} \sum_{x=\{01,10\ \}} \sum_{y_f y_g=\{01,10\}} |x\rangle|y_f y_g\rangle\right)|11\rangle \\
&= \sqrt{\frac{2}{4}}\ |\beta_1\rangle|00\rangle + \sqrt{\frac{2}{4}}\ |\beta_2\rangle|11\rangle.
\end{aligned} \tag{15}$$

Consequently, the state of the system which consists of the two replicas, after applying the first operation of the operator Mz, is in Eq. (16).

$$|\xi\rangle = |\xi^4\rangle \otimes |\xi^4\rangle = \frac{2}{4}|\beta_1\rangle^{\otimes 2}|0000\rangle + \frac{2}{4}|\beta_1\rangle|\beta_2\rangle|0011\rangle \quad + \quad \frac{2}{4}|\beta_2\rangle|\beta_1\rangle|1100\rangle + \frac{2}{4}|\beta_1\rangle^{\otimes 2}|1111\rangle \tag{16}$$

In the second operation of the operator Mz, the last four qubits in Eq. (16), are measured and the probabilities P_{0000}, P_{1100}, P_{0011}, and P_{1111} are estimated. Then, the degree of entanglement C among the two qubits of the register $|\phi\rangle$ is quantified using Eq. (4) (see Section 2). In this case study, the concurrence value C according to the Eqs. (4) and (16) is $C = \sqrt{2(P_{0011} + P_{1100})}$. Therefore, $C = \sqrt{2\left(\frac{4}{16} + \frac{4}{16}\right)} = 1$. It is obvious from Eq. (16), that $P_{0000} = P_{1111}$ after measuring operation. So, according to step 6 in the proposed algorithm (see Section (3.2)), the Hamming distance between the Boolean functions $f(x)$ and $g(x)$ is investigated as follows

$$Ham(f(x), g(x)) = \frac{N}{2}\left(1 + \sqrt{1 - c^2}\right) = \frac{4}{2}\left(1 + \sqrt{1 - 1}\right) = 2.$$

which can be verified from Eq. (7).

3.4 Complexity

Here, the complexity of the proposed algorithm is investigated. In quantum computing, the complexity of algorithms is calculated from the number of the oracle calls. It is evident from Eqs. (5)–(6) that the Hamming distance between the oracles U_f, and U_g depends on the value of the concurrence value C. This value can be determined based on the probabilities of states $|0011\rangle$,

and $|1100\rangle$, for the last four qubits, $|\phi\rangle \otimes |\phi\rangle$, in Eq. (16). The proposed algorithm computes the probabilities of these states based on recall the oracles: U_f, and U_g via $2M$ times, where M is the number of measurements. Therefore, C is quantified by Eq. (4) with max error $\epsilon = \frac{1}{\sqrt{2M}}$. In IBM's real quantum computer [16], the number of measurements is M = 8192. Hence, the proposed algorithm needs to recall the oracles: U_f, *and* U_g with 2 M = 2(8192) = 2^{14} times on this real quantum computer. Fig. 2 shows a comparison between the complexity of the proposed algorithm and that of classical algorithm. The elaboration of this Figure can be shown as follows: (i) It is evident from Fig. 2 that if the number of variables in the two oracles U_f, and U_g is $1 \leq n \leq 12$, then time-cost of the proposed quantum algorithm is higher than the classical algorithm. (ii) If the number of variables in the two oracles U_f, and U_g is n = 13, then complexity of the proposed quantum algorithm and the classical algorithm is the same. (iii) It is evident from Fig. 2 that if the number of variables in the two oracles U_f, and U_g is n > 13, then the speed of the proposed algorithm increases dramatically compared with classical algorithm. The speed up of the proposed algorithm seems to be exponential when n > 18 if the max target error is 0.01.

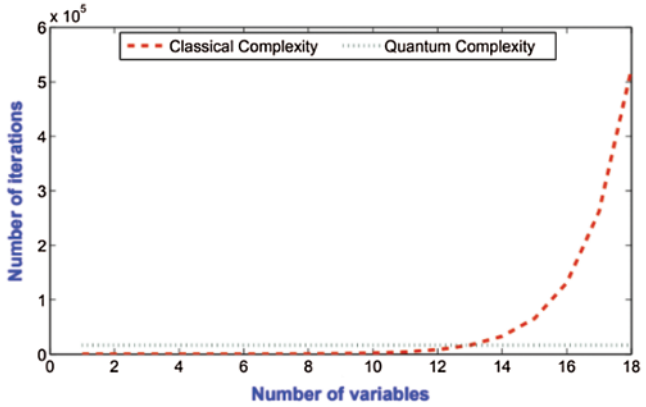


Figure 2: Comparison between the quantum complexity and the classical complexity

4 Experimental Verification of the Proposed Algorithm

4.1 Experimental Setup

To verify the proposed algorithm practically, we will conduct some experiments for measuring the hamming distance between two oracles on IBM's quantum computer simulator called Qiskit Aer [16]. Here, for verification purpose, it is assumed that these oracles are well known for the examiner but unknown for each body else. In the conducted experiments, the oracles, U_f and U_g, represent a Boolean function of two Boolean variables $f: \{0, 1\}^2 \rightarrow \{0, 1\}$ and g: $\{0, 1\}^2 \rightarrow \{0, 1\}$, respectively. Thus, the possible hamming distances between these two oracles are $Ham(f(x), g(x)) = \{0, 1, 2, 3, 4\}$. Therefore, five experiments are conducted. In the first simulation experiment, the two oracles U_f and U_g are implemented via the Boolean functions $f(x_0, x_1) = 1$ and $g(x_0, x_1) = 1$, respectively. The quantum circuits of these oracles are shown in Fig. 3. In the second simulation experiment, the two oracles U_f and U_g are implemented via the Boolean functions $f(x_0, x_1) = x_1$, and $g(x_0, x_1) = x_0x_1$, respectively. The quantum circuits of these oracles are shown in Fig. 4. In the third simulation experiment, the two oracles U_f and U_g are implemented via the Boolean functions $f(x_0, x_1) = x_0x_1$, and $g(x_0, x_1) = x_0x_1 \oplus x_1$, respectively. The quantum circuits of these

oracles are shown in Fig. 5. In the fourth simulation experiment, the two oracles U_f and U_g are implemented via the Boolean functions $f(x_0, x_1) = x_0 \oplus x_1$ and $g(x_0, x_1) = x_0x_1$, respectively. The quantum circuits of these oracles are shown in Fig. 6. In the last simulation experiment, the two oracles U_f and U_g are implemented via the Boolean functions $f(x_0, x_1) = 1$, and $g(x_0, x_1) = 0$, respectively. The quantum circuits of these oracles are shown in Fig. 7.

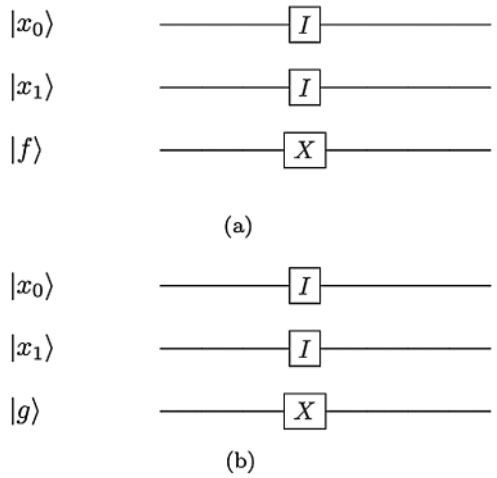


Figure 3: The quantum circuits for two different oracles U_f and U_g, respectively, the hamming distance in between is $Ham\ (f(x_0, x_1), g(x_0, x_1)) = 0$: (a) The quantum circuit of the oracle U_f that represents the Boolean function $f(x_0, x_1) = 1$. (b) The quantum circuit of the oracle U_g that represents the Boolean function $g(x_0, x_1) = 1$

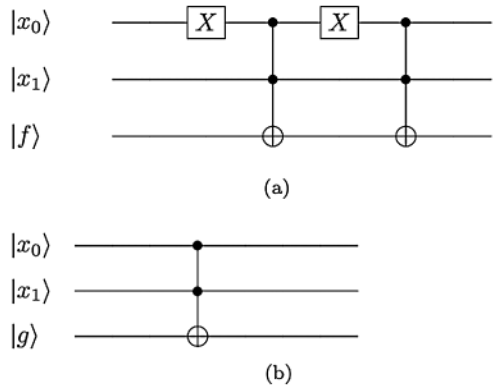


Figure 4: The quantum circuits for two different oracles U_f and U_g, respectively. The hamming distance in between is $Ham(f(x_0, x_1), g(x_0, x_1)) = 1$: (a) The quantum circuit of the oracle U_f that represents the Boolean function $f(x_0, x_1) = x1$. (b) The quantum circuit of the oracle U_g that represents the Boolean function $g(x_0, x_1) = x_0x_1$

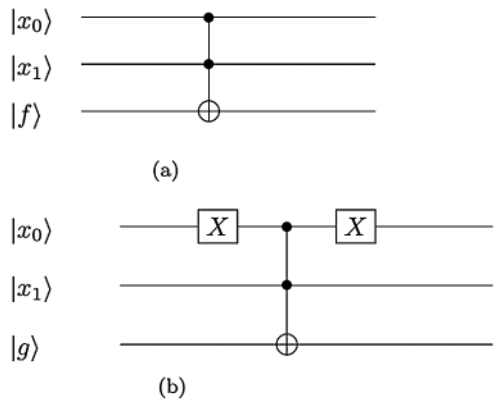


Figure 5: The quantum circuits for two different oracles U_f and U_g, respectively. The hamming distance in between is $Ham(f(x_0, x_1), g(x_0, x_1)) = 2$: (a) The quantum circuit of the oracle U_f that represents the Boolean function $f(x_0, x_1) = x_0x_1$. (b) The quantum circuit of the oracle U_g that represents the Boolean function $g(x_0, x_1) = x_0x_1 \oplus x_1$

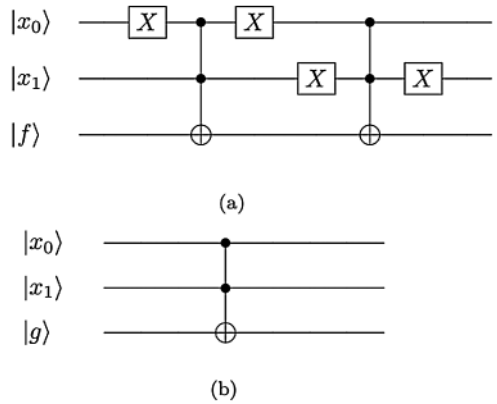


Figure 6: The quantum circuits for two different oracles U_f and U_g, respectively. The hamming distance in between is $Ham(f(x_0, x_1), g(x_0, x_1)) = 3$: (a) The quantum circuit of the oracle U_f that represents the Boolean function $f(x_0, x_1) = x_0 \oplus x_1$. (b) The quantum circuit of the oracle Ug that represents the Boolean function $g(x_0, x_1) = x_0x_1$

4.2 Results Discussion

It is clear from Section 3.2 that the proposed algorithm measures $Ham(f(x), g(x))$ between two given oracles U_f and U_g based on the concurrence value C by measuring the last four qubits of the system described by Eq. (16). The outcomes of this measurement process estimate the probabilities P_{0000}, P_{0011}, P_{1100}, and P_{1111} after M shots of measurement. Then, C is calculated quantum mechanically using Eq. (4). The estimated probabilities P_{0000}, P_{0011}, P_{1100}, and P_{1111} for the five conducted experiments are depicted in Figs. 8a–8e. The blue histograms represent the estimation of these probabilities by IBM's simulator and the green histograms represent the theoretical estimation. The results of the first simulation experiment that measures $Ham(f(x), g(x))$ between the Boolean functions $f(x_0, x_1) = 1$ and $g(x_0, x_1) = 1$ are shown in Fig. 8a. It shows that

both the simulation results of estimating the probabilities P_{0000}, P_{0011}, P_{1100}, and P_{1111} match the theoretical values exactly with fidelity $F = 1$. Theoretically, the Hamming distance between the Boolean functions $f(x_0, x_1) = 1$, and $g(x_0, x_1) = 1$ from their truth tables is $Ham(f(x), g(x)) = 0$. Practically, it is clear from Fig. 8a that the probabilities P_{0011}, P_{1100} are zero; this implies that $C = 0$ from Eq. (4). According to Fig. 8a, it is obvious that $P_{0000} > P_{1111}$.

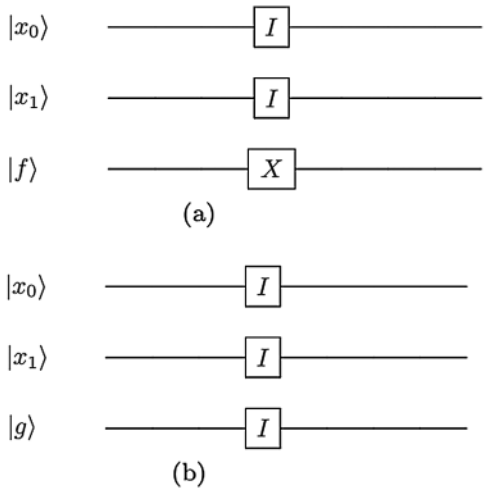
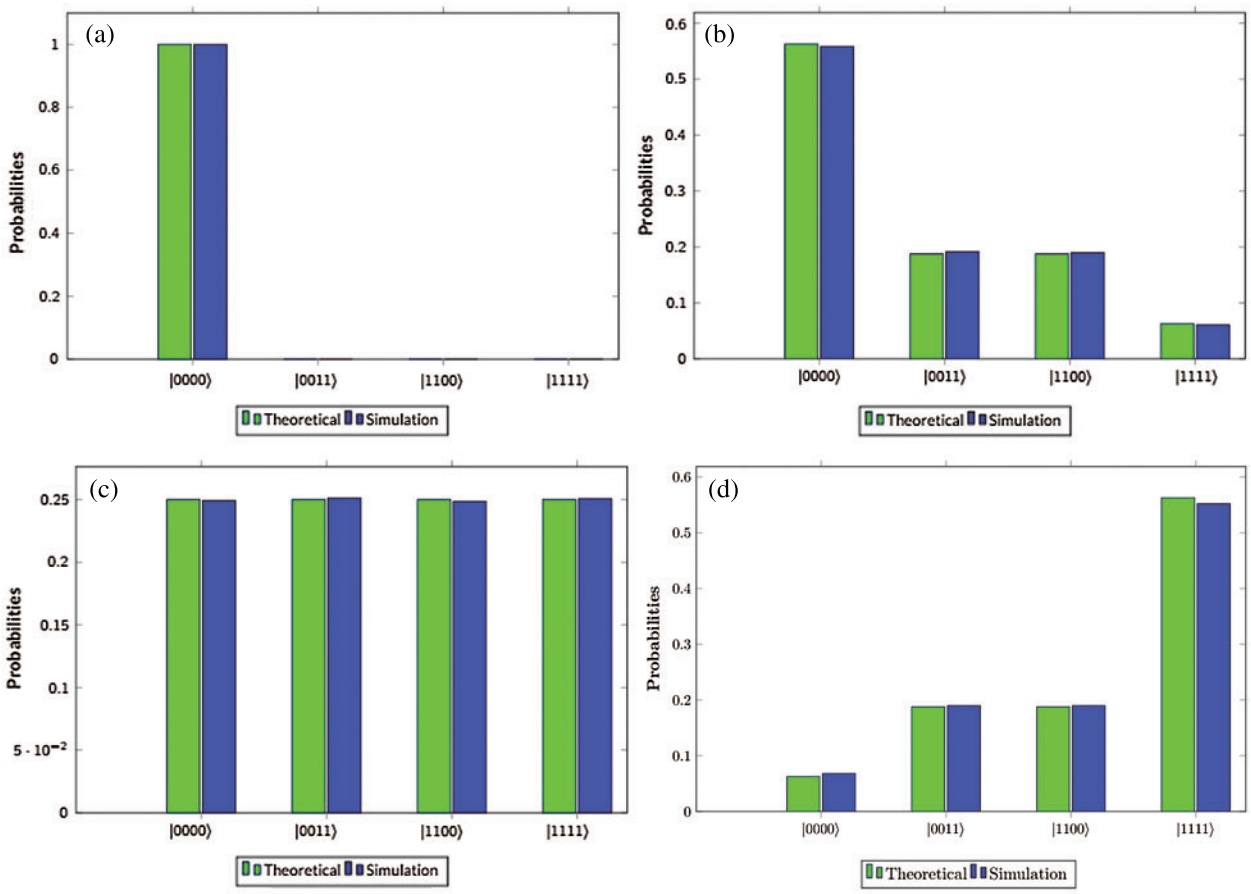


Figure 7: The quantum circuits for two different oracles U_f and U_g, respectively. The hamming distance in between is $Ham(f(x_0, x_1), g(x_0, x_1)) = 4$: (a) The quantum circuit of the oracle U_f that represents the Boolean function $f(x_0, x_1) = 1$. (b) The quantum circuit of the oracle U_g that represents the Boolean function $g(x_0, x_1) = 0$. (a). QHD = 0 (b). QHD = 1 (c). QHD = 2 (d). QHD = 3 (e) QHD = 4

Hence, the simulation result of measuring the hamming distance by the proposed algorithm is $Ham(f(x), g(x)) = \frac{4}{2}\left(1 - \sqrt{1-0}\right) = 0$; the same value that is expected theoretically. The results of the second experiment that measures $Ham(f(x), g(x))$ between the Boolean functions $f(x_0, x_1) = x_1$, and $g(x_0, x_1) = x_0 x_1$ are shown in Fig. 8b. It reveals that both the simulation results of estimating the probabilities P_{0000}, P_{0011}, P_{1100}, and P_{1111} match the theoretical values expressively with fidelity $F = 0.999975604$. Theoretically, the Hamming distance between the Boolean functions $f(x_0, x_1) = x_1$, and $g(x_0, x_1) = x_0 x_1$ from their truth tables is $Ham(f(x), g(x)) = 1$. Practically, Fig. 8b shows that the probabilities P_{0011}, P_{1100} are 0.1912 and 0.1899, respectively. Hence, the concurrence value is $C = 0.87304469$ using Eq. (4). According to Fig. 8b, it is obvious that $P0000 > P1111$. Therefore, the simulation result of measuring the hamming distance by the proposed algorithm is $Ham(f(x), g(x)) = \frac{4}{2}\left(1 - \sqrt{1-(0.87304469)^2}\right) = 1.024719592 \approx 1$. That matches theoretical result significantly. The results of the third experiment that measures $Ham(f(x), g(x))$ between the Boolean functions $f(x_0, x_1) = x_0 x_1$, and $g(x_0, x_1) = x_0 x_1 \oplus x_1$ are shown in Fig. 8c. It indicates that both the simulation results of estimating the probabilities P_{0000}, P_{0011}, P_{1100},

and P_{1111} match the theoretical values expressively with fidelity $F = 0.99999766$. Theoretically, the Hamming distance between the Boolean functions $f(x_0, x_1) = x_0x_1$, and $g(x_0, x_1) = x_0x_1 \oplus x_1$ from their truth tables is $Ham(f(x), g(x)) = 2$. Practically, Fig. 8c shows that the probabilities P_{0011}, P_{1100} are 0.2513 and 0.2487, respectively. Hence, the concurrence value is $C = 1$ by Eq. (4). Fig. 8c manifests that $P_{0000} \geq P_{1111}$. Accordingly, the simulation result of measuring the hamming distance by the proposed algorithm is $Ham(f(x), g(x)) = \frac{4}{2}\left(1 - \sqrt{1-(1)^2}\right) = 2$. Hence, in this experiment the theoretical results match the simulation results ideally. The results of the fourth experiment that measures $Ham(f(x), g(x))$ between the Boolean functions $f(x_0, x_1) = x_0 \oplus x_1$, and $g(x_0, x_1) = x_0x_1$ are shown in Fig. 8d. It shows that both the simulation results of estimating the probabilities P_{0000}, P_{0011}, P_{1100}, and P_{1111} match the theoretical values expressively with fidelity $F = 0.999907003$. Theoretically, the Hamming distance between the Boolean functions $f(x_0, x_1) = x_0 \oplus x_1$, and $g(x_0, x_1) = x_0x_1$ from their truth tables is $Ham(f(x), g(x)) = 3$.



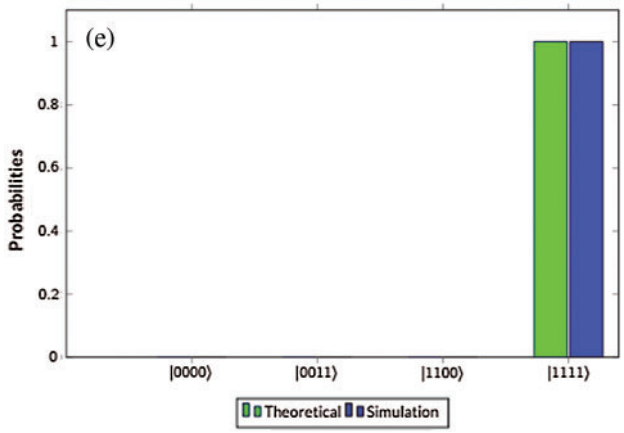


Figure 8: Comparison between the theoretical results and simulation results for the proposed algorithm to measure different hamming distance *Ham(f(x),g(x))* between two unknown oracles (a) $Ham(f(x), g(x)) = 0$; (b) $Ham(f(x), g(x)) = 1$; (c) $Ham(f(x), g(x)) = 2$; (d) $Ham(f(x), g(x)) = 3$; (e) $Ham(f(x), g(x)) = 4$

Practically, it is clear from Fig. 8d that $P_{0011} = P_{1100} = 0.1899$, respectively. So, the concurrence value is $C = 0.8716$ by Eq. (4). Fig. 8d shows that $P_{1111} > P_{0000}$. Thus, the simulation result of measuring the hamming distance by the proposed algorithm is $Ham(f(x), g(x)) = \frac{4}{2}\left(1 - \sqrt{1 + (0.8716)^2}\right) = 2.980274196 \approx 3$. Thus, both of the experimental results and the theoretical results are consistent. The results of the last experiment that measures $Ham(f(x), g(x))$ between the Boolean functions $f(x_0, x_1) = 1$ and $g(x_0, x_1) = 0$ are shown in Fig. 8e. It shows that both the simulation results of estimating the probabilities P_{0000}, P_{0011}, P_{1100}, and P_{1111} match the theoretical values exactly with fidelity $F = 1$. Theoretically, the Hamming distance between the Boolean functions $f(x_0, x_1) = 1$, and $g(x_0, x_1) = 0$ from their truth tables is $Ham(f(x), g(x)) = 4$. Practically, it is clear from Fig. 8e that the probabilities P_{0011}, P_{1100} are zero; this implies that $C = 0$ from Eq. (4).

According to Fig. 8e, $P_{1111} > P_{0000}$, so the simulation result of measuring the hamming distance by the proposed algorithm is $Ham(f(x), g(x)) = \frac{4}{2}\left(1 + \sqrt{1 - 0}\right) = 4$; the same value that is expected theoretically. Overall, the results of the simulations show that the proposed algorithm is verified with reliable fidelity. The Quantum Hamming Distance (QHD) is the $Ham(f(x), g(x))$ investigated in Fig. 8 such that 0, 1, 2, 3 and 4 in Figs. 8a–8e, respectively.

5 Conclusions

In this work, a novel quantum algorithm that measures the Hamming distance between two given oracles is explained. The proposed algorithm retrieves the hamming distances based on the degree of the entanglement between two auxiliary qubits. Therefore, the analysis of the performance of the proposed algorithm is investigated via a case study. Then, the complexity of the proposed algorithm compared to classical algorithm is explained in detail. Finally, the algorithm is verified by IBM's quantum computer simulator. The simulations results shows that the performance of the proposed algorithm is verified with fidelity close to 1.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Abdel-Aty, "Delayed sudden birth and sudden death of entanglement in josephson-charge qubits," *Laser Physics*, vol. 19, no. 3, pp. 511–515, 2009.

[2] M. Abdel-Aty, J. Larson, H. Eleuch and A. S. Obada, "Multi-particle entanglement of charge qubits coupled to a nanoresonator," *Physica E: Low-Dimensional Systems and Nanostructures*, vol. 43, no. 9, pp. 1625–1630, 2011.

[3] A. Drucker and R. De Wolf, "Uniform approximation by (quantum) polynomials," Arxiv Preprint Arxiv:1008.1599, pp. 1–9, 2010.

[4] A. Nayak and F. Wu, "The quantum query complexity of approximating the median and related statistics," in *Proc. of the Thirty-First Annual ACM Symposium on Theory of Computing*, Atlanta, Georgia, USA, pp. 384–393, 1999.

[5] E. Bernstein and U. Vazirani, "Quantum complexity theory," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1411–1473, 1997.

[6] A. De, I. Diakonikolas, V. Feldman and R. A. Servedio, "Nearly optimal solutions for the chow parameters problem and low-weight approximation of halfspaces," *Journal of the ACM (JACM)*, vol. 61, no. 2, pp. 1–36, 2014.

[7] M. Zidan, "A novel quantum computing model based on entanglement degree," *Modern Physics Letters B*, vol. 34, no. 35, pp. 2050401, 2020.

[8] Z. Xie, D. Qiu and G. Cai, "Quantum algorithms on walsh transform and hamming distance for boolean functions," *Quantum Information Processing*, vol. 17, no. 6, pp. 1–17, 2018.

[9] K. Kathuria, A. Ratan, M. McConnell and S. Bekiranov, "Implementation of a hamming distance–like genomic quantum classifier using inner products on ibmqx2 and ibmq_16_melbourne," *Quantum Machine Intelligence*, vol. 2, no. 1, pp. 1–26, 2020.

[10] J. F. Doriguello and A. Montanaro, "Quantum sketching protocols for hamming distance and beyond," *Physical Review A*, vol. 99, no. 6, pp. 062331, 2019.

[11] M. Zidan, A. H. Abdel-Aty, D. M. Nguyen, A. S. Mohamed, Y. Al-Sbou *et al.*, "A quantum algorithm based on entanglement measure for classifying boolean multivariate function into novel hidden classes," *Results in Physics*, vol. 15, pp. 102549, 2019.

[12] A. H. Abdel-Aty, H. Kadry, M. Zidan, Y. Al-Sbou, E. A. Zanaty *et al.*, "A quantum classification algorithm for classification incomplete patterns based on entanglement measure," *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 3, pp. 2809–2816, 2020.

[13] M. Zidan, H. Eleuch and M. Abdel-Aty, "Non-classical computing problems: Toward novel type of quantum computing problems," *Results in Physics*, vol. 21, pp. 103536, 2021.

[14] D. M. Nguyen and S. Kim, "New construction of binary and nonbinary quantum stabilizer codes based on symmetric matrices," *International Journal of Modern Physics B*, vol. 33, no. 24, pp. 1950274, 2019.

[15] D. M. Nguyen and S. Kim, "A novel construction for quantum stabilizer codes based on binary formalism," *International Journal of Modern Physics B*, vol. 34, no. 8, pp. 2050059, 2020.

[16] IBM Quantum Experience, 2020. [Online]. Available: https://www.ibm.com/quantum-computing/.