Azerbaijan Journal of High Performance Computing, Vol 4, Issue 1, 2021, pp. 48-52
https://doi.org/10.32010/26166127.2021.4.1.48-52

Decoding a Teleported Boolean Function Based on The Extended Deutsch-Jozsa Algorithm

Heba Kadry[1], Manal G. Eldin[2], M. G. Zidane[3]

[1] *Department of Mathematics, Faculty of Science, Sohag University, Sohag, Egypt, halimaty@gmail.com*
[2] *Department of Mathematics and Computer Science, Faculty of Science, Beni-Suef University, Beni-Suef, Egypt, Hosny.M@gust.edu.kw*
[3] *Department of Computer Science, KSAI university, Egypt, comsi2014@gmail.com*

*Correspondence: Manal G. Eldin, Department of Mathematics and Computer Science, Faculty of Science, Beni-Suef University, Beni-Suef, Egypt, Hosny.M@gust.edu.kw

Abstract

Quantum teleportation opened the realm of quantum information, such that a two communicated sender and a receiver ''Alice and Bob'' can teleport an unknown quantum state in between. Consequently, computation on the qubits has become feasible. In this paper, we propose a teleportation model to teleport a multivariate Boolean function based on the integration between teleportation protocol and the extended Deutsch-Jozsa algorithm. The proposed model uses the teleportation protocol to teleport the multivariate Boolean function through an unknown qubit from Alice to Bob. Then, it uses the extended Deutsch-Jozsa algorithm to decode the class of teleported function among 2^n possible classes.

Keyword: Teleportation, Computing models, Concurrence Measure, Boolean Function, Deutsch-Jozsa algorithm

1. Introduction

Information processing on quantum systems is one of the most promising topics in quantum technology era (Farouk, A., Zakaria, M., et al., 2015; Nagata, K., Nakamura, T., & Farouk, A., 2017; Zidan, M., Abdel-Aty, et al., 2017, November; Batle, J., Ooi, C. R., et al., 2016; Nguyen, D. M., & Kim, S., 2019; Nguyen, D. M., & Kim, S., 2019; Sagheer, A., Zidan, M., & Abdelsamea, M. M., 2019). Recently, correlations in quantum mechanics can be shown via three aspects: entanglement, discord and geometric discord. Entanglement is one of the main resources for quantum communication which performs teleportation (Luo, Y. H., Zhong, H. S., et al., 2019), and solves some of quantum computing problems (Zidan, M., Abdel-Aty, A. H., et al., 2019a; Zidan, M., Abdel-Aty, A., et al., 2018; Zidan, M., Abdel-Aty, A. H., et al., 2019b). Quantum teleportation is a powerful tool to exchange quantum information between two partners separated in a huge distance in the universe (Xu, P., Ma, Y., 2019; Ren, J. G., Xu, P., et al., 2017; Nagata, K., Nakamura, T., & Farouk, A., 2017).

Teleportation protocol of unknown qubit was first proposed theoretically and realized experimentally later (Ren, J. G., Xu, P., et al., 2017) . Then many researchers proposed additional protocols to teleport multiple qubits (Chou, K. S., Blumoff, J. Z., et al., 2018). Recently, teleportation of quantum gate was proposed. However, teleportation of a multivariate Boolean function still open research problem. In this paper, we propose a model for teleportation of a multivariate Boolean function between Alice and Bob. Alice encodes and teleports an Oracle U_f which contains some multivariate function $f: \{0, 1\}^n \rightarrow \{0, 1\}$ through the teleportation protocol to Bob. Then, Bob decodes the teleported function via the Extended Deutsch-Jozsa algorithm to one of 2^n classes.

Section 2, summarizes the quantum teleportation protocol and the Extended Deutsch-Jozsa Algorithm. In Section 3, the proposed protocol for decoding a teleported multivariate

Boolean Function based on the Extended Deutsch-Jozsa Algorithm is explained in details. Section 4 is devoted concludes the main findings of the paper.

2. Methodology

2.1. The Extended Deutsch-Jozsa Algorithm

Here, we proceed to summarize the Extended Deutsch-Jozsa (EDJ) algorithm which was proposed based on the computing model that is explained. For an oracle U_f which encodes some unknown Boolean function $f\colon \{0,\ 1\}^n \rightarrow \{0, 1\}$. There exists, 2^n possible different classes can be generated from n Boolean variables. Each class label d1 contains $\frac{2^n!}{d_1!(2^n - d_1)!}$ possible Boolean functions. The algorithm that classifies a given Boolean function via an Oracle U_f to one of 2^n classes is the EDJ algorithm compared to original Deutsch-Jozsa algorithm. which classifies only 2 classes (balanced class and constant class). The steps of EDJ algorithm are as follows:

Register preparation: initialize the two quantum registers as a tensor product of a register of size n qubits, $|\chi\rangle = |0\rangle^{\otimes n}$, and two ancillary qubits $|nb\rangle = |00\rangle$. Therefore, the state of the system is as follows:

$$|\zeta_0\rangle = |\chi\rangle \otimes |nb\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes 2}$$
$$|\zeta_1\rangle = H^{\otimes n}|\chi\rangle \otimes I^{\otimes 2}|bn\rangle$$
$$|\zeta_2\rangle = U_f|\chi, b\rangle \otimes I|n\rangle$$

Repeat the steps 1, 2, and 3 to get another decoupled copy of $|bn\rangle$ because M_Z operator needs two copies of $|bn\rangle$ to quantify the degree of entanglement in between.

5. Apply the operator M_Z on the two copies of the qubits $|bn\rangle$ and estimate P0011 and P1100 to quantify the concurrence value C and estimate the P0000 and P1111 , where P0000, P0011, P1100 and P1111 in are the probabilities of the states |0000⟩, |0011⟩, |1100⟩ and |1111⟩, respectively.

(i) If $P_{0000} > P_{1111}$ then $U_f \in class$ label d_1,

$$d_1 = \frac{2^n}{2}(1 - \sqrt{1 - C^2}$$

a) If $d_1 = 0\ then\ U_f\ is\ the\ constant\ function\ f(x_1, x_2, \ldots, x_n) = 0$

$b)\ If\ d_1 = \frac{2^n}{2}\ then\ U_f\ is\ a\ balanced\ function$

$c)\ If\ 0 < d_1\ and\ d_1 \neq \frac{N}{2}\ then\ U_f \in \text{the class label}\ d_1.$

(ii) If $P_{0000} < P_{1111}$ then $U_f \in$ the $class$ label d_1,

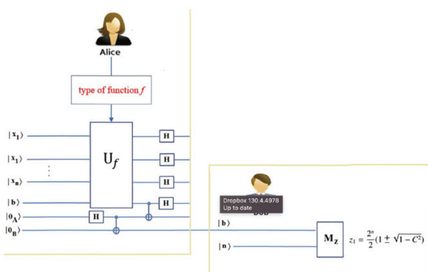

Fig. 2. Diagram shows the main operations of the proposed protocol for teleporting and decoding a Boolean Multivariate function between Alice and Bob.

$$d_1 = \frac{2^n}{2}(1 + \sqrt{1 - C^2})$$

a) If $d_1 = 2^n, then\ U_f\ is\ the\ constant\ function\ f(x_1, x_2, \dots, x_n) = 1$

$b)\ If\ d_1 = \frac{2^n}{2}\ then\ U_f\ is\ a\ balanced\ function$

$c)\ If\ 0 < d_1\ and\ d_1 \neq \frac{2^n}{2}\ then\ U_f \in \text{the class label}\ d_1.$

3. The Proposed Decoding Protocol of a Teleported Multivariate function

Assume that Alice needs to distribute some key with Bob. Alice and Bob agreed in between to use a function which has included in one of 2n class label. This agreement is hidden from Eve. Alice and Bob's goals are to determine which class label of the function chosen by Alice without revealing information about the function to Eve. Hence, Alice needs to teleport U_f via the qubit $|t\rangle$

to Bob. Bob needs to figure out the class label d_1 of the multivariate function which is teleported via the quantum channel by Alice using the Extended Deutsch-Jozsa algorithm which is explained in Section 2.1.

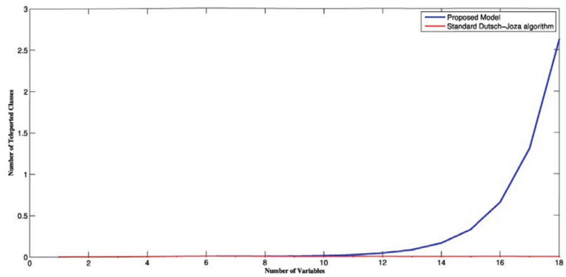

Fig. 3. Comparison between he number of classes by the proposed model and the number of classes using standard Deutsch-Jozsa algorithm.

To achieve this purpose, Alice and Bob can teleport and decode arbitrary multivariate Boolean function adopting the following proposed protocol:

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

$$|\zeta_0^{c1}\rangle = |\chi\rangle \otimes |b\rangle \otimes |0_A 0_B\rangle = |0\rangle^{\otimes n} \otimes |0\rangle \otimes |0_A 0_B\rangle$$

where the subscript A refers to Alice's qubit and the subscript B refers to Bob's qubit. These two qubits are used to create the quantum teleportation channel between Alice and Bob in the next two steps as explained in Section 2.1.

$$|\zeta_1^{c1}\rangle = (I^{\otimes n+1} \otimes \mathrm{H} \otimes \mathrm{I}|\zeta_1\rangle$$

ii. $|\zeta_2^{c1}\rangle = (I^{\otimes n+1} \otimes \mathrm{CNOT}|\zeta_2\rangle$

2. Alice processing:

(a) $|\zeta_3^{c1}\rangle = (H^{\otimes n} \otimes I^{\otimes 3})|\chi\rangle|\mathrm{b}\rangle \otimes \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$

(b) $|\zeta_4^{c1}\rangle = (U_f \otimes I^{\otimes 2})|\chi\rangle|\mathrm{b}\rangle \otimes \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$, where the action of an Oracle U_f on the first n + 1 qubits is $U_f|x_1, x_2, \dots, x_n x_{n+1}\rangle = |x_1, x_2, \dots, x_n, (x_1, x_2 \dots x_n + x_{n+1}) mod 2\rangle$. It should be noted that the qubit which has index n+1 is the qubit which is labeled $|\mathrm{b}\rangle$.

(c) Teleportation operation: Alice teleports the qubit $|\mathrm{b}\rangle$ to Bob using teleportation protocol (see Section 2.1), in the next three steps as follows:

i. $|\zeta_5^{c1}\rangle = (H^{\otimes n+1} \otimes I^{\otimes 2} |\zeta_4\rangle$ Remark: in the above step, the Hadmard gate is applied to the first n+1 of the system $|\zeta_4\rangle$ not to the qubit $|b\rangle$ only, because the qubit $|b\rangle$ is entangled with the first n + 1 qubits due to the effect of an Oracle U_f.

ii. $|\zeta_6^{c1}\rangle = (\mathrm{I}^{\otimes n} \otimes \mathrm{CNOT} \otimes \mathrm{I}|\zeta_5\rangle$.

Alice perform measurement process on the two qubits which have the indices 1 and n + 2 in the quantum system have the state defined by $|\zeta_6\rangle$. Then, she sends the classical message msg which contains the measurement result to Bob.

iv. Alice repeats steps 1-2 to teleport another copy of the state $|\zeta_6^{c2}\rangle$ to Bob.

Bob processing: After Bob receives the classical message, msg, from Alice, he applies I gate, X gate, Z gate or XZ gate upon the content of the message msg is 00, 01, 10 or 11, respectively, on his qubit, then system is transformed to the state $|\zeta_7^{c1}\rangle$. Then,

Bob adds another qubit $|n\rangle = |0\rangle$ to the system, $|\zeta_8^{c1}\rangle = |\zeta_7^{c1}\rangle \otimes |0\rangle$.

ii. After that. Bob receives the second copy of the state $|\zeta_6^{c1}\rangle$ and transforms it to the state $|\zeta_8^{c2}\rangle$. Bob applies the operator Mz to the last four qubits of the state $|\zeta_8^{c1}\rangle \otimes |\zeta_8^{c2}\rangle$. Then, he estimates the probabilities of the states |0000⟩, |0011⟩, |1100⟩ and |1111⟩, and calculates the concurrence value $C = \sqrt{2(P_{0011} + P_{1100}}$

(I) If $P_{0000} > P_{1111}$ then $U_f \in class$ label d_1,

$$d_1 = \frac{2^n}{2}(1 + \sqrt{1 - C^2})$$

a) If $d_1 = 0$ $then\ U_f\ is\ the\ constant\ function\ f(x_1, x_2, \dots, x_n) = 0$

$b)\ If\ d_1 = \frac{2^n}{2}\ then\ U_f\ is\ a\ balanced\ function$

$c)\ If\ 0 < d_1\ and\ d_1 \neq \frac{N}{2}\ then\ U_f \in \text{the class label } d_1.$

(II) If $P_{0000} < P_{1111}$ then $U_f \in$ the $class$ label d_1,

$$d_1 = \frac{2^n}{2}(1 + \sqrt{1 - C^2})$$

a) If $d_1 = 2^n, then\ U_f\ is\ the\ constant\ function\ f(x_1, x_2, \dots, x_n) = 1$

$b)\ If\ d_1 = \frac{2^n}{2}\ then\ U_f\ is\ a\ balanced\ function$

$c)\ If\ 0 < d_1\ and\ d_1 \neq \frac{2^n}{2}\ then\ U_f \in \text{the class label } d_1.$

The quantum circuit of the whole protocol is shown in Fig. 1. The proposed protocol can be used to teleport a multivariate Boolean function from Alice and Bob and is decoded by Bob. Fig. 2 compares the number of class that can be decoded by Bob using the original Deutsch-Jozsa algorithm and the proposed protocol upon EDJ algorithm. This figure shows that the number of classes in increased exponentially as a function in the number of variables in case EDJ algorithm compared to original Deutsch-Jozsa which classifies only two classes (constant and balanced classes).

Hence, upon the proposed protocol, Alice and Bob can share 2^n keys in between instead of only two keys using Detsch-Jozsa algorithm (Zidan, M., 2020). Moreover, has been indicated that the complexity of EDJ algorithm is polynomial time On IBM's quantum computer compared with classical algorithms which solve the same problem in exponential time indicating that the proposed algorithm is faster in contrast with traditional computers.

Finally, the proposed protocol open the door for cloud quantum computing and for proposing set of robust encryption protocols that can use 2^n keys.

Conclusion

In this work, we proposed a novel protocol to decode the class of a teleported multivariate

Boolean function, among 2^n classes based on the Extended Deutsch-Jozsa algorithm that was proposed upon a novel model of quantum computing. The proposed protocol finds the class of the teleported function based on the degree of entanglement according between two extra qubits.

This problem can not be implemented on traditional computers, where teleportation of the qubits can not be achieved on classical systems. Our findings may have potential applications in encryption protocols that can use 2^n keys. In addition, it can be used to perform cloud quantum computing.

References

Batle, J., Ooi, C. R., et al. (2016). Nonlocality in pure and mixed n-qubit X states. *Quantum Information Processing, 15*(4), 1553-1567.

Chou, K. S., Blumoff, J. Z., et al. (2018). Deterministic teleportation of a quantum gate between two logical qubits. *Nature, 561*(7723), 368-373.

Farouk, A., Zakaria, M., et al. (2015). A generalized architecture of quantum secure direct communication for N disjointed users with authentication. *Scientific Reports, 5*(1), 1-17.

Luo, Y. H., Zhong, H. S., et al. (2019). Quantum teleportation in high dimensions. *Physical Review Letters, 123*(7), 070505.

Nagata, K., Nakamura, T., & Farouk, A. (2017). Quantum cryptography based on the Deutsch-Jozsa algorithm. *International Journal of Theoretical Physics, 56*(9), 2887-2897.

Nguyen, D. M., & Kim, S. (2019). Multi-bits transfer based on the quantum three-stage protocol with quantum error correction codes. *International Journal of Theoretical Physics, 58*(6), 2043-2053.

Nguyen, D. M., & Kim, S. (2019). Quantum key distribution protocol based on modified generalization of Deutsch-Jozsa algorithm in d-level quantum system. *International Journal of Theoretical Physics, 58*(1), 71-82.

Nguyen, D. M., & Kim, S. (2019). The fog on: Generalized teleportation by means of discrete-time quantum walks on N-lines and N-cycles. *Modern Physics Letters B, 33*(23), 1950270.

Ren, J. G., Xu, P., et al. (2017). Ground-to-satellite quantum teleportation. *Nature, 549*(7670), 70-73.

Sagheer, A., Zidan, M., & Abdelsamea, M. M. (2019). A novel autonomous perceptron model for pattern classification applications. *Entropy, 21*(8), 763.

Xu, P., Ma, Y., et al. (2019). Satellite testing of a gravitationally induced quantum decoherence model. *Science, 366*(6461), 132-135.

Zidan, M. (2020). A novel quantum computing model based on entanglement degree. *Modern Physics Letters B, 34*(35), 2050401.

Zidan, M., Abdel-Aty, A. H., et al. (2019a). A quantum algorithm based on entanglement measure for classifying Boolean multivariate function into novel hidden classes. *Results in Physics, 15,* 102549.

Zidan, M., Abdel-Aty, A. H., et al. (2019b). Quantum classification algorithm based on competitive learning neural network and entanglement measure. *Applied Sciences, 9*(7), 1277.

Zidan, M., Abdel-Aty, A., et al. (2018). A novel algorithm based on entanglement measurement for improving speed of quantum algorithms. *Appl. Math. Inf. Sci, 12*(1), 265-269.

Zidan, M., Abdel-Aty, et al. (2017, November). Low-cost autonomous perceptron neural network inspired by quantum computation. In *AIP Conference Proceedings* (Vol. 1905, No. 1, p. 020005). AIP Publishing LLC.

Submitted: 16.08.2020
Accepted: 17.05.2021