Getting Started With Quantum Computation: Experiencing The Quantum Experience

Ranveer Kumar Singh[1], Prathamesh Ratnaparkhi[2], Bikash K. Behera[3] and Prasanta K. Panigrahi[3]**
[1]BS-MS Student, Department of Mathematics, Indian Institute of Science Education and Research Bhopal, Bhauri 462066, Madhya Pradesh, India
[2]Mechanical Engineering, Vishwakarma Institute of Technology, 666, Upper Indira Nagar, Bibwewadi, Pune, Maharashtra 411037
[3]Indian Institute of Science Education and Research, Kolkata, Mohanpur 741246, West Bengal, India

Abstract. Quantum computation is an emerging field of research at the intersection of computer science, information theory and quantum physics. With applications in cryptography, simulation of complex quantum mechanical systems, artificial intelligence, weather forecast and market prediction, quantum computers will be indispensable in the future. Recent years have seen immense progress on the experimental front, with the IBM Quantum Experience (IBM QE), real quantum computers are within reach for anyone. We introduce here the basic concepts of quantum computation for using IBM QE, needing only the knowledge of matrix multiplication.

Keywords. IBM Quantum Experience, Quantum Computation, Superposition, Entanglement

INTRODUCTION

Using principles of quantum physics developed in the early 20^{th} century, a completely new field, "quantum computation" has emerged, unifying computer science, information theory and physics. It started with Richard Feynman's observation [1] that a computer can be designed that can use the laws of quantum mechanics to simulate the nature. The idea was to use a quantum state as the fundamental building blocks of the computer, the simplest one is a two-level system, called a *qubit*, which evolves according to the laws of quantum mechanics. An example of a quantum two-level system can be the two-spin states of an electron or the two polarizations of light. The classical bits are represented by 0 or 1, or physically they can be voltage on and off in a chip. These numbers are manipulated using normal addition operation. Unlike the classical bit that represents only one state at a time, a quantum bit (qubit) can be in both the states at the same time i.e., in a superposition of both the states. As is well-known, "quantum mechanics" also called 'matrix mechanics', a single qubit state is represented by a 2×1 matrix, being a linear superposition of $|0\rangle = [1, 0]^T$ and $|1\rangle = [0, 1]^T$, i.e., $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$ and α, β are complex numbers. This superposition of states observed in quantum physics gives an infinitude of states in which a qubit can be, which in turn

** pprasanta@iiserkol.ac.in

increases the computing power of quantum computers. This feature of quantum computers, known as "quantum parallelism" enables us to perform large number of operations in small time interval that reduces the complexity of the problems. Thus classically intractable problems like the travelling salesman problem can be solved on a quantum computer efficiently [2].

More generally, there is a certain class of problems called non-polynomial (NP) problems [3], which cannot be solved efficiently on the current "classical" computers. The phrase "cannot be solved efficiently" means that as the size of the input parameter increases, the time required to solve the problem increases exponentially. Consider the aforementioned travelling salesman problem [4, 5]; a salesman has to visit n different cities, which path should he follow so that he can visit all the cities with the minimum distance travelled? It has been calculated that for number of cities as small as 10 there are 10!/2 =1814400 possible paths in which he can visit them. For solving this problem, a classical computer works in the following way; it will systematically calculate the total distance for each possible configuration and then compare among them to find the optimal solution, i.e., the minimum path among all the possible paths. The time required to solve this problem increases exponentially with the number of cities, thus for a sufficiently large number of cities the computer will take forever to find the solution. Like this, there are other hard problems [6] which require a computer that can perform a large number of operations with minimum time-complexity. This is exactly what a quantum computer can do.

Apart from "quantum parallelism", another peculiar feature which quantum mechanics exhibits is *Entanglement* [7]. Entanglement refers to two or more quantum particles having correlated quantum states. For example, in a singlet state, two electrons are physically separated and in anti-parallel directions. The quantum state of the two electrons can be written as, $\frac{|01\rangle-|10\rangle}{\sqrt{2}}$, where $|0\rangle$ and $|1\rangle$ stand for spin-up and spin-down states of electrons. Entanglement allows to perform an operation on two qubits simultaneously which cannot be done with classical bits. Thus qubits can exist in superposition of more than one state and also can be entangled with each other, which classical bits cannot exhibit. Using these features of quantum mechanics, several non trivial algorithms have been designed in quantum computation. Quantum teleportation [8], where an unknown quantum state is transferred between two distant parties, has been achieved using entangled channels (Sec. 3) between the sender and the receiver.

There are ways to improve the efficiency of classical computers. For instance, one way would be to make bigger computers i.e., to have more transistors on a chip. A bigger computer solves a problem of given size in less time. In order to tackle problems of bigger and bigger size in less and less time, the transistors will have to get smaller and smaller, so small that eventually there are only a few silicon atoms. According to Moore's law [9], "The number of transistors in a dense integrated circuit doubles every two years". At this stage, we again fall prey to the laws of quantum physics due to the small size. Heat generation in the computing process is another disadvantage working in the microscopic level. In Landauer's principle [10], it is argued that "a minimum heat generation, of the order of κT, is required for each irreversible function". Thus the emergence of quantum computers under a well defined framework of quantum mechanics has been one of the most

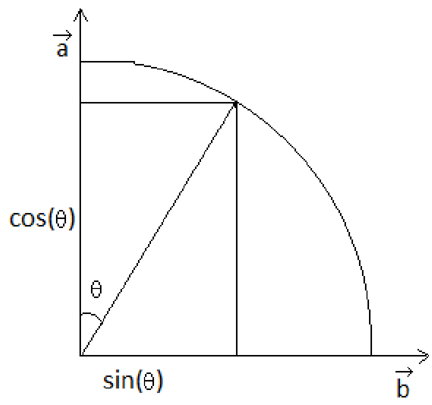

Figure 1. The state of a polarized light

important developments of the 20^{th} century.

1. ORIGIN OF RANDOMNESS

Superposition is at the heart of quantum computation since it gives rise to randomness. To understand how randomness comes up at microscopic scale, consider an example of plane polarized light incident on a polarizer. If we represent the state of polarization parallel to optical axis by $\vec{a}$ and the state perpendicular to it by $\vec{b}$ then a photon polarized at an angle θ with respect to the vertical axis can be represented as $\vec{x}(\theta) = (\vec{x}(\theta) \cdot \vec{a})\vec{a} + (\vec{x}(\theta) \cdot \vec{b})\vec{b} = (\cos\theta)\vec{a} + (\sin\theta)\vec{b}$. Fig. 1 illustrates this fact. When light with this state of polarization $\vec{x}(\theta)$ travelling along z axis, is incident on a polarizer it is observed that transmitted intensity is $\cos^2(\theta) I_0$, where I_0 is incident intensity and θ is angle between plane of polarization and optical axis.

Now suppose we have some kind of an apparatus which emits only one photon at a time. Then if using the apparatus we let a photon strike the polarizer then the photon will either pass through or it will be absorbed. What decides whether the photon will pass through polarizer or not? Passing photon through polarizer constitutes a measurement and according to Copenhagen interpretation of quantum mechanics the state of the system collapses to one of the basis states upon measurement. This collapse is totally random and all we can talk about a priory is the probability with which the photon will collapse to given basis state. An analogy of coin toss will be helpful to understand the idea of superposition-measurement-collapse. When the coin is in air it is neither heads nor tails, it is in superposition. As it hits the ground it lands on heads or tails at random. The probability that an incident photon in state $(\cos\theta)\vec{a} + (\sin\theta)\vec{b}$ will collapse to state $\vec{a}$ is given by $\cos^2(\theta)$ and that of state $\vec{b}$ is $\sin^2(\theta)$. Note that the sum of probabilities i.e., $\sin^2(\theta)+\cos^2(\theta)$ is 1. Thus out of n incident photons $\cos^2(\theta).n$ are randomly found in state $\vec{a}$ and thus the transmitted intensity is $\cos^2(\theta) I_0$. This analysis at microscopic scale is totally consistent with macroscopic intensity law (Malus' Law). If we rotate the analyzer such that the optical axis is parallel to the plane of polarization (rotation of measurement basis) then the photon is in state $\vec{a}$. Now $\cos^2(\theta) = 1$, thus every photon that arrives at polarizer passes through. There is no random behaviour. We see that randomness arises when the system is in superposition of measurement basis states.

2. THE POWER OF SUPERPOSITION

Interestingly, the same superposition which leads to randomness also allows for performing operations on all possible states at once. This leads to quantum parallelization i.e. unlike classical computer which has to process one input at a time a computer based on quantum principles, a "Quantum Computer" can process all possible inputs at once. Quantum parallelization relies on the fact that a qubit can exist in a superposition of base states. Each component of this superposition can be thought of as a single argument of a function. A function operated on the qubit, which is in a superposition of states, is thus operated on each of the components of the superposition, but this function is only applied one time. Since for n qubits, there are a total of 2^n possible states, thus what would take a classical computer an exponential number of operations, can be performed on a quantum computer in one operation. Although quantum parallelization offers a large speedup over classical computers, the result may still be random, so the whole idea is to design the operations in such a way that the probability of getting the correct answer is enhanced. But this has its own shortcomings. With larger number of superposed states, the probability of measuring a particular superposed state becomes low and hence the answer is probabilistic. Moreover, according to the laws of quantum mechanics, superposition is lost upon measurement on the quantum state. Thus if we only use superposition states then the probability of retrieving the answer is low. But for problems which are beyond reach of classical computers a probabilistic answer is better than no answer at all. Fortunately in some cases, although the solution is difficult to find, it is easy to check a given solution. For example, finding out prime factors of a number is a NP hard problem [3], but given a prime factor of a number it is just matter of easy multiplication to check whether they are really the prime factors or not. Thus a parallel computing algorithm can be devised to multiply all the factors in just one operation. Thus a probabilistic answer can be checked and if found incorrect, the process can be rerun to find another answer.

3. QUANTUM ENTANGLEMENT

Quantum entanglement as introduced earlier is the distinguishing feature of quantum mechanics. In mathematical language, a two qubit state can be represented as,

$$|\psi\rangle = \Big(a|0\rangle + b|1\rangle\Big) \otimes \Big(\alpha|0\rangle + \beta|1\rangle\Big) = a\alpha|00\rangle + a\beta|01\rangle + b\alpha|10\rangle + b\beta|11\rangle \qquad (1)$$

where $\otimes$ is the tensor product between the two quantum states, and $|00\rangle = |0\rangle \otimes |0\rangle$, similarly it applies for other states, $|01\rangle$, $|10\rangle$, and $|11\rangle$. The above state (Eq. (1)) reveals that the first qubit is in the state $a|0\rangle + b|1\rangle$ and the second qubit is in the state $\alpha|0\rangle + \beta|1\rangle$. Now consider another such state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2}$$

It is an easy exercise to check that this state cannot be factored in the form $(a|0\rangle + b|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$. Hence it shows that the state of individual qubits are not completely specified. States of the form Eq. (2) are called entangled states. The state in Eq. (2) is called EPR pair after Einstein, Podolsky and Rosen [11] who used this state to propose a paradox in quantum mechanics (famously known as EPR paradox). This state has the property that measurement on one of the qubit reveals the state of the other instantaneously. Such states are of utmost importance in quantum computation. As discussed above we observe that measurement on one qubit of an entangled state determines the state of the other irrespective of their location in space. Thus entangled states have been used as communication channel in cryptographic protocols. All of quantum key distribution (QKD) protocols which provide a way to share a private key between two parties (Alice and Bob) separated in space, rely on entanglement. These protocols use entanglement to check if a key sent by one party has been hijacked in between by eavesdropper. In most of the QKD protocols, if Alice wants to send a secret key to Bob then firstly they prepare some entangled state with each of them having half of the entangled particles. Then Alice performs a measurement on some of her particles and then communicates the result to Bob via classical channel. Since immediately after the measurement the state of the other half of the particles is known to Bob as communicated by Alice, he measures his particles to check if someone has tried to access the key by measuring on his particles. If Bob finds the same result as informed by Alice then he can be sure that the key shared is secret. Some modifications of this protocol is used in most of these protocols. It is also known that Grover's search algorithm and Shor's factorization algorithm, which are some of the most important quantum algorithms use entangled states [12, 13].

4. QUANTUM COMPUTER

Quantum computers are built from *quantum circuits* which consist of wires and elementary *quantum gates*, in the same fashion as classical computers are made using electrical wires and logic gates. Quantum gates are used to carry around and manipulate quantum information encoded in qubits. In the language of quantum mechanics a qubit is represented by the superposition state $\alpha|0\rangle + \beta|1\rangle$ where $|0\rangle$ and $|1\rangle$ are the two states of a quantum bit analogous to the 0 and 1 state of a classical bit (cbit). A qubit can be physically represented by trapped ions, superconducting junctions, NMR etc. Quantum gates are the implementation of operations performed on a quantum state by Linear operators. In the language of mathematics we say that quantum states are vectors in a mathematical object called Hilbert space. Thus the mathematical language of quantum mechanics is Linear algebra. The operators acting on quantum states are represented by matrices. So any manipulation of a quantum state is carried out by operators. In quantum computation, these operations are realized via quantum gates. There are several quantum gates classified as single qubit gate and multiple qubit gate which as the names suggest act on single qubit and multiple qubits respectively. Thus a quantum computer essentially consists of a series of qubits, each of which is a quantum system described using two dimensional vector space. The qubits are prepared in known state say, $|0\rangle$ then a transformation is applied on them which puts them in superposition. Once in superposition a series of transformations via quantum gates are applied which act on every possible input. After quantum gates act on the qubits, a measurement is done to retrieve the answer. Using this procedure different quantum algorithms are designed to solve various problems using quantum circuits constructed using a specified sequence of quantum gates.

5. A BRIEF HISTORY OF QUANTUM COMPUTATION

In the 1920s, with the evolution of quantum mechanics which had already resolved several absurdities such as "ultraviolet catastrophe" and the instability of atom due to electron's accelerated motion etc predicted by classical physics, people started to think if quantum mechanics could be used to achieve things which classically cannot be achieved. For example in the early 1980s, researchers started thinking if quantum effects could be used to signal faster than light which was forbidden classically according to the special theory of relativity. It turned out that this problem was equivalent to cloning a quantum state which is very well possible classically. However, it was proved that it was impossible to clone a quantum state [14]. This *no-cloning theorem* was one of the earliest results in quantum computation and quantum information. Making use of this no-cloning theorem, the first idea in the field of quantum information called "Quantum Money" was proposed by Stephen Wiesner in 1970 (which remained unpublished until 1983) [15].
In 1981 Richard Feynman had realized that the inability of computers to simulate quantum mechanical systems is because their working principles are classical. He proposed that a computer used for simulation of quantum mechanical systems should be based on quantum principles. To use quantum principles for computing, it was necessary to gain complete control over quantum state which is so fragile towards environmental effects. Thus since 1970s many such techniques were developed. For example, methods were developed to trap a single atom in an "atom trap" and study its properties with stunning accuracy. In the mean time computer science was also developing rapidly with the remarkable paper by Alan Turing in 1936 [16]. Turing presented a notion of what we call a programmable, a model for computation called *Turing machine*. Subsequently, John Von Neumann developed a theoretical model to build a practical computer which would be capable as a *Universal Turing machine*. In the late 1960s, the *Church Turing* thesis was presented, which states that "Any algorithmic process can be simulated efficiently using a Turing machine". However, the challenge came when it was observed that many problems which were believed to have no solution on Turing machine could be solved using *analog computers*. But the problem was that if the realistic assumptions of noise in analog computers were taken into account, then it was difficult to operate

on such problems. This challenge was successfully resolved when the theory of *error correcting codes* and *fault tolerant quantum computation* was proposed. Following this several quantum algorithms were proposed to solve various problems. From late 60s to late 90s the research in the field led to formation of theoretical framework for quantum information. The most important of them, the *factorization algorithm* by Shor (1994) [17] and *list search algorithm* by Grover (1996) [18] demonstrated the power of quantum computation. The first experimental demonstration of quantum algorithm was done in 1998 by Jones and Mosca at Oxford University [19].
Since late 1990s, experimental side has progressed tremendously. Linear optics, superconducting junction, nuclear magnetic resonance and trapped ions have been used as qubits. However, efforts to build quantum computers have not met great successes till date. Small quantum computers capable of performing dozens of calculations on a few qbits have been developed but the problem of building a universal quantum computer still remains a challenge for future researchers. A huge step in the development of a universal quantum computer has been accomplished by IBM [20], which has developed 5-, 16-, 20- and 50-qubit quantum computers. Two of them, the 5- and 16-qubit quantum computers are available to public, providing an opportunity to everyone to perform experiments on the quantum computers.

6. IBM Q EXPERIENCE

With continuous efforts, IBM developed a quantum computer which used superconducting qubits. Since its inception in May 2016, IBM Quantum Experience (IBM QE) has proven to be a valuable asset for researchers working in the field of quantum computation. More than 80 academic papers have been published based on the research carried out with help of IBM QE. Through this platform, researchers, students and enthusiasts get access to a real quantum processor and a simulator. The qubits used are superconducting Josephson junctions. They are stored at very low temperature, only a few miliKelvin above absolute zero, in order to protect them from the thermal noise. A $^3He/^4He$ dilution refrigerator is used to achieve the required low temperature. The state of a qubit is changed by shooting it with microwave radiation of predetermined frequency and phase. On the other hand, measurement of the state of a qubit is done by measuring its response to certain microwave radiation.

As of November 2018, IBM has made available two 5-qubit and one 16-qubit quantum computers. These devices can be remotely accessed using Quantum Information and Science Kit (QISKit) provided by IBM QE. The quantum composer (Fig. 2) is a user friendly graphic user interface developed by IBM, used to write quantum algorithms or run experiments in the field of quantum computation and quantum information. Along with composer, the online platform includes a beginner's guide, a full user's guide and a forum to share ideas and reach out for help. The typical process of writing and running an algorithm is as follows: initially, all the qubits in composer are in the state $|0\rangle$, appropriate gates are taken from side panel and dropped on a qubit to change the state of the qubit. The information processing occurs when the state of one qubit is conditionally evolved based on the state of some other qubits using conditional gates (e.g. $CNOT$ gate). Finally measurements

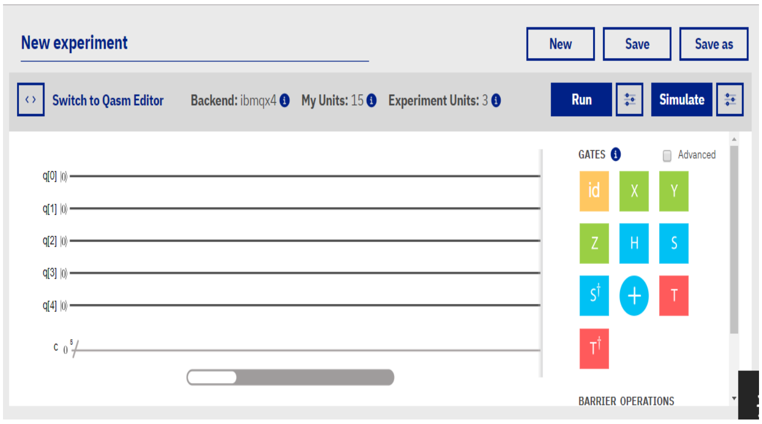

Figure 2. The composer of IBM Q Experience. Image Credit:IBM Q Experience.

are done to know the states of all or some qubits and the results are stored in classical registers and displayed as a bar chart. For example, a two-qubit algorithm can have four possible outcomes $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. So the result of a two-qubit algorithm gives probability of getting each one of these as output. As we know for a particular run, the result is random but when we run the algorithm many times we may find that a certain result occurs more often than other. The whole idea is to apply transformations (quantum gates) in such a way that the probability of getting desired output is enhanced.

To start building quantum circuits one first needs to visit IBM QE website and register with email addresses. Then go to the composer and start a new circuit. There is an option to choose to run the circuit on real quantum computer or simulate the results using custom topology. A circuit sent to run on the real device, is queued and the process takes time. Thus it is advisable to use custom topology for trial and error and for testing the circuit prior to sending it to real device. Quantum algorithms involving 5 qubits can be constructed using the quantum composer but implementing a 16 qubit algorithm requires writing the algorithm in QASM language. Then it can be run on the real quantum computer or simulated using QISKit. It is to be noted that QISKit is an open-source framework for working with noisy quantum computers at the level of pulses, circuits, and algorithms.

Thus running a real time quantum computer is now at hand. Observing bizarre quantum phenomena such as quantum teleportation, cryptography protocols can be easily realized on IBM Q. IBM Q is improving the quantum computing power day by day. IBM Q has recently announced a 50-qubit quantum computer for commercial purposes. A number of experiments in the field of quantum computational and information processing have been performed on the 5-qubit, and 16-qubit real quantum chips. Experimental realization of quantum cheque [21–23], observation of Topological Uhlmann phase [24], algorithmic simulation [25], developing quantum error correction codes [26–29], experimental test of Mermin's inequalities [30], testing quantum algorithms [31], optimization of quantum circuits [32] etc. have been tested and verified on the real quantum chips.

7. CONCLUSION

We have seen that a paradigm shift from classical to quantum computation allows us to solve classically intractable problems which could not be solved efficiently before. In brief, we have tried to motivate young students to experiment in the field of quantum computation, using the publicly available quantum computers. Furthermore, quantum computers of different architecture and a brief history of quantum computation have been discussed. The IBM QE platform has been discussed, which anyone can use and implement protocols on a real quantum computer. There are a number of problems for which quantum algorithms are yet to be designed. With the help of IBM QE, any interested researchers can participate in the effort to take the research in quantum computation forward.

References

[1] R. P. Feynman, *Int. J. Theor. Phys.*, Vol. 21, pp. 6-7, 1982.

[2] S. Aaronson, *Quantum Computing Since Democritus*, Cambridge University Press, 2013.

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation And Quantum Information*, Cambridge University Press, 2010.

[4] D. C. M. Jose,*Transportation Research Part*, Vol. 33, pp. 123-152, 1999.

[5] K. Srinivasan, S. Satyajit, B. K. Behera, and P. K. Panigrahi, *arXiv:1805.10928*, 2018.

[6] D. P. Bovet, *Introduction to the Theory of Complexity*, Prentice Hall, 2006.

[7] E. Schrodinger, *Naturwiss.*, Vol. 23, p. 807, 1935.

[8] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, *Phys. Rev. Lett.*, Vol. 70, p. 1895, 1993.

[9] G. E.Moore, *Electronics*, Vol. 38, p. 8, 1965.

[10] R. Landauer, *IBM J. Res. Develop.*, Vol. 5, pp. 183-191, 1961.

[11] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.*, Vol. 47, p. 777, 1935.

[12] V. M Kendon, *Quantum Inf. & Comput.*, Vol. 6, pp. 630-640, 2006.

[13] S. Chakraborty, *arXiv:1305.4454v2*, 2013.

[14] W. K. Wootters and W. H. Zurek, *Nature*, Vol. 299, pp. 802-803, 1982.

[15] S. J. Wiesner, *SIGACT News*, Vol. 15, pp. 78-88, 1983.

[16] A. M. Turing, *Proceedings of the London Mathematical Society*, Vol. s2-42, pp. 230-265, 1937.

[17] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood and I. L. Chuang, *Nature*, Vol. 414, pp. 883-887, 2001.

[18] L. K. Grover, *Proceeding STOC '96 Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212-219, 1996.

[19] J. A. Jones and M. Mosca, *J. Chem. Phys.*, Vol. 109, p. 1648, 1998.

[20] IBM Quantum Experience, URL: https://quantumexperience.ng.bluemix.net/qx/editor.

[21] S. R. Moulick and P. K. Panigrahi, *Quantum Inf. Process.*, Vol. 15, pp. 2475-2486, 2016.

[22] B. K. Behera, and A. Banerjee, and P. K. Panigrahi, *Quantum Inf. Process.*, Vol. 16, p. 312, 2017.

[23] News in New Scientist, *URL: https://www.newscientist.com/article/2140242-quantum-cheques-could-be-a-forgery-free-way-to-move-money/.*

[24] O. Viyuela, A. Rivas, S. Gasparinetti, A. Wallraff, S. Filipp, and M. A. Martin-Delgado, *npj Quantum Inf.*, Vol. 4, p. 10, 2018.

[25] A. A. Zhukov, S. V. Remizov, W. V. Pogosov, and Y. E. Lozovik, *Quantum Inf. Process.*, Vol. 17, p. 223, 2018.

[26] C. Vuillot, *Quantum Inf. Comput.*, Vol. 18, p. 0949, 2018.

[27] D. Ghosh, P. Agarwal, P. Pandey, B. K. Behera, and P. K. Panigrahi, *Quantum Inf. Process.*, Vol. 17, p. 153, 2018.

[28] J. R. Wootton and D. Loss, *Phys. Rev. A*, Vol. 97, p. 052313, 2018.

[29] S. Satyajit, K. Srinivasan, B. K. Behera, and P. K. Panigrahi, *Quantum Inf. Process.*, Vol. 17, p. 212, 2018.

[30] D. Alsina and J. I. Latorre, *Phys. Rev. A*, 94, p. 012314, 2016.

[31] S. Gangopadhyay, Manabputra, B. K. Behera, and P. K. Panigrahi, *Quantum Inf. Process.*, Vol. 17, p. 160, 2018.

[32] M. Sisodia, A. Shukla, A. A. A. de Almeida, G. W. Dueck, and A Pathak, *arXiv:1812.11602*, 2019.