A Review On The Fundamental Concepts Of Quantum Elements, Efficient Quantum Algorithms And Quantum Error Correcting Codes

C. H. Ugwuishiwu , U. E. Orji, O.Ukwueze , P. O. Ogbobe

Abstract: Quantum Elements, Efficient Quantum Algorithms and Quantum Error Correcting Codes are some of the fundamental concepts of quantum computing. In this paper, the authors aim to introduce readers and potential researchers to the subject areas to help them appreciate the intrigues and ideas behind quantum computing. The authors introduced the basic concepts of quantum physics which is the foundation for quantum computing. Related literature such as books, journals, conference proceedings, lecture notes and webpages on this field of study were sourced and reviewed from top databases like IEEE Xplore, JSTOR, ScienceDirect etc.

Keywords: Quantum elements; quantum algorithm; error correcting codes; quantum physics.

1.0 Introduction

Quantum information processing is envisaged to perform specific tasks that has proven to be too complex for the conventional computers, for example; simulating quantum systems [1, 2], large number factorization [1], or distributing private shared keys securely [3]. For a quantum system to work properly, it needs to function in a controlled environment where the risks of decoherence (interacting with the environment) is minimized. The main idea behind fault-tolerant quantum computation is to mitigate the impact of noise in a quantum system and keep the error-rate to the barest minimum below the accuracy threshold of the system [4]. This is the basis for quantum error correction codes. Quantum information processors have the ability to exploit the unique quantum features like superposition and entanglement; this is not possible in classical devices. Thus, quantum information systems offer the potential for significant improvements in information communication and processing [5]. With the advancements in quantum computation, certain real world problems can now be solved efficiently; while some problems on a classical computer would take millions of years to solve, a quantum computer could potentially solve some of those same problems in a couple of days [6]. However, there are also some classical computing problems that quantum computation cannot improve on and even some that the improvement is rather insignificant. For example, classical computers are better at some chores than quantum computers like email and other routine activities. The bottom line remains that quantum computation will significantly impact current security architectures although there are many fields that will enjoy the quantum features including, faster and more accurate quantum simulators. From the field of classical computing, we learnt about the concept of error correction during the process of storing or transmitting data from one point in memory to another. Information loss come as a result of bit flips in the strings of bits being transferred. The bit flips ensure pockets of errors on the information at the receiving end of the transmission. In the same vein, minute errors that occur in quantum gates tend to build up in a large circuit and eventually lead to large errors that frustrate computation [7]. Efficient computer algorithms have been developed over the years in the quest for more performance enhancement in classical computing [8]. Similarly, in quantum computing, efficient quantum algorithms were established to improve the computing power of quantum technology; generally, every polynomial time algorithm is considered 'efficient' [9] for example, an algorithm that factors any n digit number in O (n^3) operations is said to be more efficient than an algorithm that sorts n numbers in O (n^2) operations. This paper acquaints readers with some of these efficient quantum algorithms while building up from the concepts of the basic quantum elements found in the field of quantum physics. The work also goes ahead to have a peek into the concept of quantum error-correcting codes. The three concepts understudy are all building blocks of a quantum computing system.

2.0 Literature Review

2.1 Background

In this section, relevant researches on quantum elements, efficient quantum algorithms and quantum error correction codes will be discussed. Presumably, the paper will help motivate potential researchers in the field of the study.

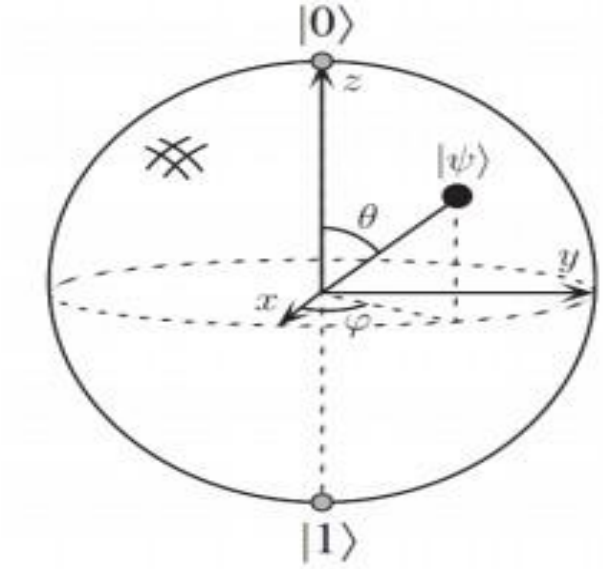
2.2 The Basic Principles of Classical/Quantum Element

The architecture of classical computer is based on Boolean logic structure; thus the basic building unit of a computer is bits consisting of 0s and 1s. In computer hardware, these bits of 0s and 1s are represented via the presence or absence of a voltage, charge, or current [10]. The Logic operations or gates are categorized according to their input and output bit counts [11]. In a quantum computing system, the two-dimensional Hilbert space* serves as a quantum bit (also known as qubit) and exists in two mutually orthogonal states [12]. This is the computational basis states of quantum systems and they also correspond to the classical bit states of “logical 0’ and “logical 1”. However, unlike the classical bit, a qubit can also exist in a phenomenon known as “superposition” which is an arbitrary linear combination of the computational basic states [13].

* The two-dimensional Hilbert space ‘H’ in quantum mechanics denotes the angular momentum or “spin” of a spin-half particle (such as electron, proton, etc.), and it provides the physical representation of a qubit.

2.2.1 Classical Element

In classical computers, algorithms and logical operations like NOT, OR, and AND defines how computations are done, they also act on and transform strings of bits [14]. The



operation of the classical computer processor is best understood as shown in figure 1:

- **Datapath -** This component provides a small temporary data storage space within the processor and handles data manipulation in the processor.
- **Control -** This component is tasked with generating control signals. These signals determine the memory and datapath operations.
- **Memory -** This component stores instructions and the data used by executing programs.
- **Input -** This component consists of all external devices like the keyboard, mouse, disks, etc., through which command is given to the processor.
- **Output -** This component consists of all external devices like the display unit (monitor), printers, disks, etc., that receive data from the processor.

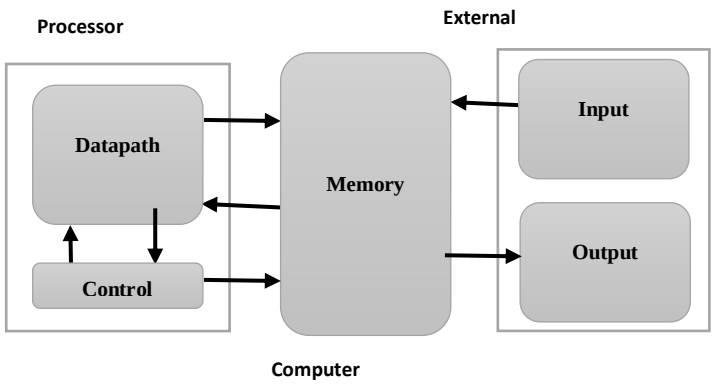


Figure 1: Architecture of a Classical Computer

2.2.2 Review on Related Literature on Classical Element

The authors in [15] described in detail the evolution of classical computers and their pioneers. They also showed the different models of classical computers and their architecture. They examined how Boolean algebra was used as the building block for constructing classical computer. While differentiating between classical and quantum computing in [16], the author also explained how computers work, the capabilities of classical computers, and their limitations. The author gave a clear but concise description of how the binary system is the bedrock of classical computers and how it is used to transfer and process information inside a classical computer. In [17], the author demonstrated the basic concepts of classical computation depicting the basic structure of classical information bit as a two-state system ∈ {0, 1}. The author also showed how a digital computer operation is schematically represented by circuits made up of wires and logic gates.

2.3 Quantum Elements

It is universally accepted that bit is the most fundamental element in computer science. However, unlike the classical computers which primarily has two states 0 and 1, the quantum bit (qubit) has unlimited states |0> and |1> signifying the superposition of the two basic states [18] as shown in figure 2: a Quantum bit (qubit) represented by a sphere called Bloch.

The Bloch sphere represents an infinite space where probability of the qubit presence is estimated by its wave function square given as: $|\psi> = \alpha|0> + \beta|1>$ and normalized as $|\alpha|^2 + |\beta|^2 = 1$. Where $|\alpha|^2$ is the probability of the qubit in state |1> and $|\beta|^2$ for the state |0> respectively. As earlier mentioned, this qubit might be in a superposition of these two known states and this is the most significant difference between bits and qubits [20].

Quantum computer is divided into five major layers with difference types of processing as shown in figure 3.

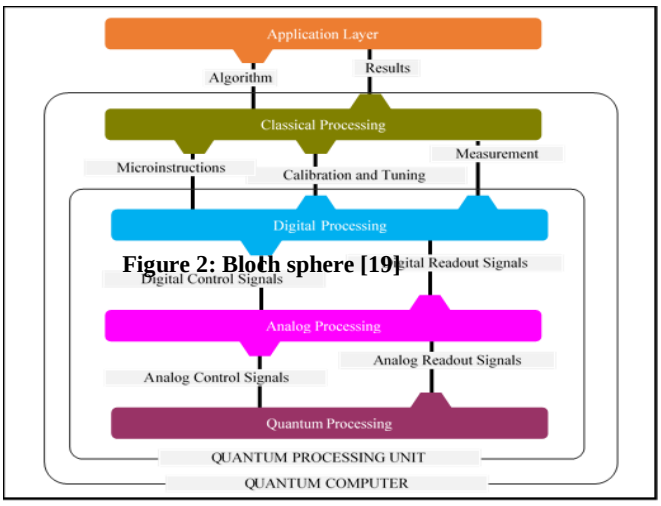


Figure 2: Bloch sphere [19]

Figure 3: A Blueprint for a Practical Quantum Computer [21]

- **Application Layer-** This layer represents the user interface in the system but it is not part of the quantum computer.
- **Classical Layer-** This layer is tasked with: i) Optimizing quantum algorithms and compiling it into microinstructions. ii) Processing quantum-state measurements and feeds it to a classical algorithm

to produce results. Finally, iii) Handles calibration and tuning needs of the lower layers.

- **Digital Layer-** This layer is tasked with converting the microinstructions got from the Classical Layer into pulses thus enabling them to act as quantum logic gates. The feedback from this layer comes in the form of a quantum measurement.
- Analog Layer- The analog-processing layer produces phase and amplitude modulated voltage signals that are transmitted to the next layer to execute qubit operations.
- Quantum Layer- This layer is for storing qubits and is strictly kept at absolute room temperature. It is where error correction is handled and determines how well the computer performs. This layer also handles the integration of the digital and analog layer onto the same chip.
- Quantum Processing Unit (QPU) - this layer comprises three key layers namely; the digital, analog, and quantum processing layers. A quantum computer is made-up of the combination of the QPU and classical layer [21, 22].

2.3.1 Basic principles of quantum physics that influenced quantum computing

Quantum Physics is the underlying principle behind quantum computers. It is therefore pertinent to look at the elements of quantum Physics to enable one understand what the elements of quantum computers are.

The following are essential elements of quantum physics that informs the theories behind quantum computers and their elements:

- Particles are waves and vice versa: The study of quantum physics identifies with the intertwining nature of objects as having both particle-like and wave-like properties. Quantum particles are discrete and (in principle) countable thus, exhibits the characteristics of particles, however; they also show effects like diffraction and interference which are characteristics of waves [23].
- Quantum states are discrete: In quantum physics, everything comes in discrete amounts. You can only detect a quantum system in a specified state [24].
- Probability is all we ever know: The outcome of an experiment with quantum mechanics is only ever in probabilities and not the actual outcomes [25]. The fact here is that, in quantum computation, the outcome of an experiment is not guaranteed because with each new electron, comes an entirely new experiment where the outcome is always random.
- Measurement determines reality: A quantum particle's state is indeterminate until the exact state is measured. This means that until a quantum particle is measured, it actually exists in all the states simultaneously [26]. And after it is measured, it will remain only in that one state [27].
- Quantum correlations are non-local: The entanglement is arguably the strangest yet most important aspect of quantum mechanics. When two quantum particles interact correctly, their states will become co-dependent, regardless of their proximity [28]. For example, one particle can be in the U.S while the other is in Paris; however, if measured simultaneously, the measurement result in the U.S will definitely reveal that of Paris and vice versa. This explains why quantum mechanics is said to be non-local.
- Everything not forbidden is mandatory: The movement of a quantum particle from one point to another will take absolutely every possible path in its way and simultaneously including highly improbable paths. This is explained by the theory of quantum electro-dynamics (QED) and it takes contributions from every possible process, even the ridiculously unlikely ones [29].
- Quantum physics is not magic: Even though quantum physics seem strange, it does not suspend all the rules of common sense. The fundamental principles of physics still holds: energy is still conserved and nothing can move faster than the speed of light.

2.3.2 Review on Related Literature on Quantum Elements

Hamidreza et al. in [30] showed the history and fundamental ideas behind quantum computing with a focus on quantum computing architecture. The authors described the primary elements of quantum computers, which are the qubits, and presented quantum gates and their functions and qubit fabrication methods. In [31], the authors introduced qubits as the basic unit of information in quantum computing. The authors went further by comparing bit vs. qubit with emphasis on the superposition feature of the qubit. The authors also explained in detail the basics of quantum gates and their fabrication. The author in [32] succinctly explained the history, theories, and applications of quantum elements with more emphasis on the fundamentals on how quantum systems were made, especially on buzzing topics like the quantum Turing Machine, quantum gates, and Shor's algorithm.

2.4 Efficient Quantum Algorithms

Before now, we have come to know an algorithm as the systematic process of solving problems. Algorithms from the classical computing perspective is a finite step-by-step sequence of instructions, where each instruction can be carried out on a classical computer. On the other hand, quantum algorithms run on a realistic model of quantum computation. The efficiency of an algorithm is measured by the asymptotic value of how the Algorithm's resources grows with input. Time and space is the most considered resources when measuring in terms of the number of operations and bits or qubits [33]. The Shor's algorithm proposed in 1994 by Peter Shor is a quantum algorithm for prime factorization [34]. His algorithm made a very great advancement in quantum computing, and today, we can boldly say Shor's algorithm opened the door for us to appreciate the concept and significance of quantum computing. One of the limitations of classical computing is that an algorithm that can solve prime factorization at high speed is non-existent. This property was ensured by the safety guarantee of the Rivest, Shamir, and Adelman's RSA code which they propounded in 1978 [35]; however, Shor's algorithm broke the jinx and can be employed to unlock the RSA code. A high-speed algorithm by Shor's specification entails that the algorithm can be processed in polynomial time thus it is said to be "efficient."

Shor's algorithm came with it a chance for decoding the hitherto highly secure RSA code. This implies that the RSA code which has been considered safe, is now at risk if the implementation of quantum computers in practice becomes feasible [36]. As shocking as the news was, it served to motivate a lot of interest in the research into quantum computing, and as of now, a lot of money is being pumped into enquiries on how to bring about quantum computers. What Peter Shor actually did was that he swapped the problem of factorization with that of finding the period [37]. With period finding and the subsequent solving using quantum Fourier transforms, Shor was able to annihilate the problem of factorization.

2.4.1 Shor's Algorithm for Factorization

1. First, pick a pseudo-random positive integer c < d, then calculate the gcd(c, d) in polynomial time, you can achieve this via the Euclidean algorithm. If gcd(c, d) ≠ 1, then there is a nontrivial factor of n, and the problem is done. However, if gcd(c, d) = 1, proceed to step 2 below.
2. Using a quantum computer, get the unknown period P of the sequence and is given as follow; t mod d, t2 mod d, t3 mod d, t4 mod d,... 4.
3. To proceed, If P is an odd integer number, step 1 is repeated. However, if P is an even integer number, proceed to the next step. Where the period P is even, then $(c^{P/2}-1)(c^{P/2}-1)=c^{P}-1=0 \bmod d$.
4. Next, check if $c^{P/2}+1=0 \bmod d$, and if so, repeat step. However, if $c^{P/2}+1 \neq 0$, proceed to step 5.
5. Finally, compute $x = \gcd(c^{P/2}-1, d)$ using the Euclidean algorithm, and since $c^{P/2}+1 \neq 0 \bmod d$ has been proven in step 4 above, we can also show that x is a significant prime factor of d [36].

2.4.2 Grover's algorithm

Grover's algorithm can be deployed when you have a function that returns 'True' for one of its possible inputs and 'False' for the rest. Here, the algorithm is used to find the function that returns True. The easiest way to go about this will be to express the inputs as bit strings and encode these using the $|0\rangle$ and $|1\rangle$ states of a string of qubits. So the bit string 0011 would be encoded in the four qubit state $|0011\rangle$.It is also vital to implement the function using quantum gates. The next step is to find a sequence of gates that will implement a unitary U such that:

$U|a\rangle = -|a\rangle$, $U|b\rangle = |b\rangle$

Where a represents the bit string for which the function would return True, while b is any for which it would return False.

Suppose we start with a superposition of all possible bit strings, which is pretty easy to do by just Hadamarding everything. Then, all inputs start off with the same amplitude of $1/\sqrt{2n}$ (where n represents the length of the bit strings we are searching). However, when we apply the oracle U, the amplitude of the state we are looking for will change to $-1/\sqrt{2n}$. Furthermore, we use the Grover Diffusion Operator, D to amplify it because it is not an easily observable difference. The operator checks how each amplitude is different from the mean amplitude and then invert this difference.

So, if you have a superposition of bit strings bj, the diffusion operator has the effect

$D : \sum_j \alpha_j |b_j\rangle \mapsto \sum_j (2\mu-\alpha_j)|b_j\rangle$

Where $\mu = \sum_j \alpha_j$ is the mean amplitude, so any amplitude $\mu+\delta$ gets turned into $\mu-\delta$ [38].

2.4.3 Applications of Grover's algorithm

Grover's algorithm as an effective subroutine can enhance quantum speedups for many problems.

The following lists just a few of these speedups associated with Grover's algorithm.

- Searching through an unsorted list for example; to get the minimum of an unsorted list of N integers or an arbitrary and unknown function like, $f:\{0,1\}^n-\mathbb{Z}$).
- Solving graph-theoretic problems to determine graph connectivity: in classical systems, it takes $O(N^2)$ time of order to determine whether a graph on N vertices is connected; however, Grover's algorithm solves this problem in time $O(N^{3/2})$.
- In text processing and bioinformatics, pattern matching is a fundamental problem that Grover's algorithm can help tackle [39].

2.5 Review on Related Literature on Efficient Quantum Algorithm

Since Shor's algorithm, researchers have been in a rat race to design the next big quantum algorithm. The authors in [40] proved an efficient quantum reduction from computing S-units to the continuous hidden subgroup problem using a polynomial-time quantum algorithm for computation of the ideal class group (CGP) via the Generalized Riemann Hypothesis. They also deployed the algorithm to solve the principal ideal problem (PIP) in number fields of arbitrary degree. The authors showed how the CGP and PIP reduce naturally to the computation of S-unit groups. In [37], the author carried out a detailed survey of some well-known quantum algorithms emphasizing more on the applications' of the algorithms with little focus on their technical details. The report discussed some recent developments in the field and possible applications of quantum algorithms in broad areas like cryptography, search and optimization, solving large systems of linear equations etc. This author [39] discussed the early quantum algorithms and demonstrated how they were able to solve complex computational problems. The author went further to compare how classical algorithms would fare in solving the same problems and the advantages of the quantum algorithms, especially the exponential speedups they exhibited.

3.0 Error Correcting Codes

The origins of error corrections are linked to Claude Shannon's 1948 landmark paper titled "A mathematical theory of communication." Shannon identified a number termed "channel capacity," where he proposed that in a communication channel that may be prone to interference and noise, arbitrary reliable communication is possible but only below the "capacity channel" [41]. The importance of Error correction as one of the most fundamental aspects of digital communication cannot be overemphasized. It is responsible for the validity of real-time interactions. In reality, every communication channel experiences some form of transmission errors. These errors needs to be continuously taken care of as they occur, hence the importance of error correction. Shannon's result proved that data can be encoded before transmission and verified when received by the receiver.

3.1 Classical Error Correcting Codes

Classical computers use dynamic random-access memory, or RAM, to speed up their program runtime; the RAM works by storing data in tiny capacitors. Furthermore, electrical or magnetic interference could be a major source of spontaneous bit-flips experienced in these capacitors, resulting in error. Although this interference is rare; however when it does occur, it can cause undesirable consequences. In correcting these errors, the computer is designed to use specialized hardware controllers, which traditionally are principled on the Hamming code [42]. The most classic example of error correction algorithm is the repetition code. Here each bit in an input message is duplicated severally. For example, if you had the message, '01101', encoded using this repetition method, it would become '000 111 111 000 111'. Thus, if a random bit flip or error occurred, it could be corrected by simply taking the most common bit of each three-bit segment as demonstrated here: '100 111 101 000 110'. Obviously, this message includes multiple errors. However, we can correct the error and decode the message to the original message 01101. But here is the problem, this method is not very efficient, it consumes more space as you can see adding two parity bits for each bit of the original code takes more space in memory. Additionally, it is essential to note that we could no longer correct the error if more than one bit in these three-bit segments was affected by an error [43]. Other classical error-correcting codes include the binary hamming code, Linear Error-Correcting Codes, The Binary Golay Code, etc.

3.2 Review on Related Literature on Classical Error Correcting Codes

In [44], the authors proposed a geometric functional analysis solution for reconstruction of signals in linear measurements along with its error-correcting codes. Their work is based on the combination of principles of coding theory, signal processing, combinatorial geometry, and geometric functional analysis. Authors in [42] extensively discussed the fundamentals of the classical error-correcting codes, that is, the theorems associated with error-correcting codes, including the origins of linear codes and coding theory.
Detecting and correcting errors in arithmetic computations is vital to developing reliable systems, in [45], the authors gave a summary of the most important results that are obtainable in the theory of coding.

3.3 Quantum Error Corrections

Quantum error correction (QEC) combines the study of quantum mechanics and the concept of the classical theory of error correcting codes. Both are concerned with the fundamental problem of ensuring fault-tolerant quantum computation. It does not only deal with noise on stored quantum information system, but also with faulty quantum gates, faulty quantum preparation, and faulty measurements. For Quantum error correction, noise could arise from decoherence which is a reoccurring threat because qubits inevitably have unwanted interactions with their surroundings thus leading to the decoherence state. These environmental interactions are harmless in a classical computer (and can even be helpful by introducing friction which impedes accidental bit flips); however, decoherence in a quantum computer leads to irreparable damages to the delicate superposition states that the machine is meant to process. Superposition feature of quantum computers is the power of quantum machines. A research in [46] suggested a simple example of quantum error correction with a three-qubit codeas shown in figure 4. This quantum error-correcting algorithm uses three "physical" qubits to protect a single "logical" qubit of information against bit-flips. Although it is worthy of note that this code is not very effective since it can't protect against phase-flips. The |0⟩ state of the logical qubit corresponds to all three physical qubits being in their |0⟩ states, likewise the |1⟩ state corresponds to all three being |1⟩ state. This state of the system is known as the "superposition" and is designated as |000⟩ + |111⟩.

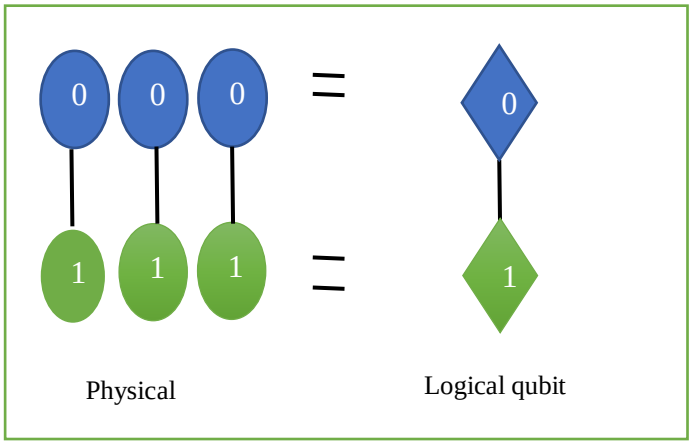


Figure 4: Quantum error correction with a three-qubit code

If a bit-flip occurs with one of the qubits, how do we detect and correct the error without directly measuring any of the qubits? Here is how to go about this problem; the qubits can be fed through two gates in a quantum circuit; where one gate checks the "parity" of the first and second physical qubit to ascertain if they're the same or different while the other gate checks the parity of the first and third qubit respectively. But if there is no error i.e., the qubits are in the state |000⟩ + |111⟩, the parity-measuring gates confirms that the first and second, and the first and third qubits are always the same. However, if the first qubit accidentally bit-flips, producing the state |100⟩ + |011⟩, the gates detect a difference in both of the pairs and so on for the second and third qubit.

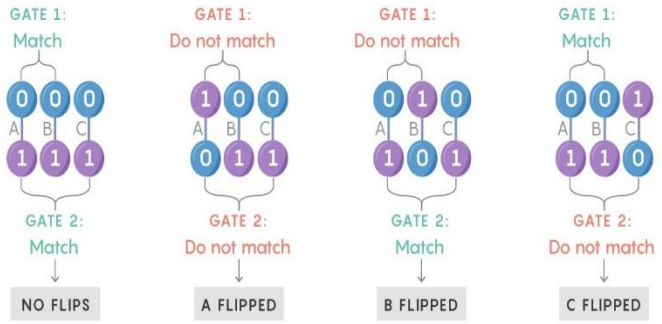


Figure 5: Finding and fixing quantum errors [46]

These unique outcomes indicate the corrective surgery needed to flip back the first, second, or third physical qubit without collapsing the logical qubit as shown in figure 5.

3.3.1 Review on Related Literature on Quantum Error Correcting Codes

Author in [47] showed the derivation of quantum error-correcting codes via the encoding and decoding of quantum algorithms from their underlying mathematical structure. The authors used examples to illustrate the construction of these quantum error-correcting codes. In [48], the authors proposed a method to construct Entanglement-assisted quantum error correcting codes (EAQECCs) with good error performance by constructing the quantum code from classical codes through the relaxation of the duality condition. The author in [49] explained the fundamentals of quantum error correction and its usefulness in building reliable quantum computers. The author covered important subjects like the background of quantum error correction, general properties of quantum error correcting codes, fault-tolerant quantum computation, and many more.

4.0 Result Discussion/ Findings

This paper aims to simplify and introduce readers to the basic principles of quantum elements, efficient quantum algorithms, and quantum error correcting codes. To help potential researchers in the field appreciate the subjects, the classical aspects of each part of the subject area was discussed to match the relationship between the traditional classical computer and the anticipated powerful quantum machine. Some relevant researches done in the various fields of the study were reviewed. The paper is intended to be a motivating factor and a good foundation for beginners in the field of quantum computing to explore further into quantum science.

5.0 CONCLUSION

We have come to see from the foregoing that measurement has a lot to do in determining the state of any quantum particle. The state of any quantum particle cannot be determined unless it has been measured. Prior to that measurement, it is assumed that the particle is in every possible state simultaneously. This is possible due to the concept of superposition. The elements of quantum computers has its origin from the concepts of quantum physics. They tell us the things we are expected to see in the quantum computer which has come with a promise of very fast and more efficient improvement over the conventional classical computers. With more efficient quantum algorithms coming up, we expect to see more improvements in quantum computing as more and more algorithms are caused to run in a polynomial time of execution.

REFERENCES

[1] J.A. Smolin, G. Smith, and A. Vargo, “Pretending to factor large numbers on a quantum computer.” 2013. arXiv preprint arXiv:1301.7007.

[2] M. Xu, D.A. Tieri, and M.J. Holland, “Simulating open quantum systems by applying SU (4) to quantum master equations.” Physical Review A, 2013. 87(6), p.062101.

[3] A. Broadbent, and C. Schaffner, “Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography” 2016. Vol. 78(1), pp.351-382.

[4] J.W. Harrington, “Analysis of quantum error-correcting codes: symplectic lattice codes and toric codes” Doctoral dissertation, California Institute of Technology. 2004.

[5] Monroe, C. Quantum information processing with atoms and photons. Nature 416, 238–246 (2002). https://doi.org/10.1038/416238a

[6] https://www.ibm.com/quantum-computing/what-is-quantum-computing/

[7] C. Sparrow, "Quantum interference in universal linear optical devices for quantum computation and simulation." (2017). https://doi.org/10.25560/67638

[8] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning.” Nature, 2017. Vol. 549(7671), pp.195-202.

[9] P. W. Shor, "Why haven't more quantum algorithms been found?." Journal of the ACM (JACM) Vol. 50, no. 1 (2003): pp. 87-90.

[10] D.P. DiVincenzo, “The physical implementation of quantum computation. Fortschritte der Physik: Progress of Physics.” 2000. Vol. 48(9-11), pp.771-783.

[11] J. Stolze, and D. Suter, “Quantum computing.” Wiley-VCH, Weinheim, 2004. Vol. 29, pp.30-31.

[12] L. Dellantonio, A.S. Sørensen, and D. Bacco, “High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces.” Physical Review A, 2018. 98(6), p.062301.

[13] X. Qiang, X. Zhou, J. Wang, C.M. Wilkes, T. Loke, S. O’Gara, L. Kling, G.D. Marshall, R. Santagati, T.C. Ralph, and J.B. Wang, “Large-scale silicon quantum photonics implementing arbitrary two-qubit processing.” Nature photonics, 2018. Vol. 12(9), pp.534-539.

[14] Jaeger, Gregg. "Classical and quantum computing. Quantum Information: An Overview.” (2007): 203-217.

[15] Yu I. Bogdanov, N. A. Bogdanova, D. V. Fastovets, and V. F. Lukichev. "On the Relationship between Boolean Algebra and Quantum Informatics." Russian Microelectronics 49, no. 1 (2020): 1-15.

[16] N. Raoof, “Difference between Classical Computing and Quantum Computing” Available online at: https://medium.com/faun/classical-computing-c1a126a7bd73, Accessed on: Mar. 23, 2021.

[17] A. Galindo, and M. A. Martin-Delgado. "Information and computation: Classical and quantum aspects." Reviews of Modern Physics 74, no. 2 (2002): 347.

[18] K Valiev, "Quantum computers and quantum computations." Physics-Uspekhi 48, no. 1 (2005): 1

[19] Wie, Chu-Ryang. "Bloch sphere model for two-qubit pure states." arXiv preprint arXiv:1403.8069 (2014).

[20] H.R. Bolhasani, A.M. Rahmani, and F. Kheiri, “An Introduction to Quantum Computers Architecture.” Available online at: https://www.researchgate.net/publication/337144719_An_Introduction_to_Quantum_Computers_Architecture, Accessed on: Mar. 23, 2021.

[21] Richard Versluis "Here’s a Blueprint for a Practical Quantum Computer" Available online at: https://spectrum.ieee.org/computing/hardware/heres-a-blueprint-for-a-practical-quantum-computer Accessed on: May. 23, 2021.

[22] Surya Teja Marella and Hemanth Sai Kumar Parisa, "Introduction to Quantum Computing." Available online at: https://www.intechopen.com/online-first/introduction-to-quantum-computing Accessed on: May. 23, 2021.

[23] R. Omnes, “The interpretation of quantum mechanics.” Princeton University Press, 2018.

[24] D. Tong, "The Unquantum Quantum." Scientific American 307, no. 6 (2012): 46-49.
[25] I. Pitowsky, "Quantum mechanics as a theory of probability." In Physical theory and its interpretation, pp. 213-240. 2006. Springer, Dordrecht.
[26] M. Schlosshauer, "Decoherence, the measurement problem, and interpretations of quantum mechanics." Reviews of Modern physics 76, no. 4 (2005): 1267.
[27] D. Aerts, and S. Massimiliano "The extended Bloch representation of quantum mechanics and the hidden-measurement solution to the measurement problem." Annals of Physics 351 (2014): 975-1025.
[28] W. Bertrand, "Quantum Entanglement." International Journal of Automatic Control System. 2019; 5(2): 1–7p.
[29] X.S. Geng, L.L. Ji, B.F. Shen, et al. "Quantum reflection above the classical radiation-reaction barrier in the quantum electro-dynamics regime." Commun Phys 2, 66 (2019). https://doi.org/10.1038/s42005-019-0164-2
[30] Bolhasani, Hamidreza, and Amir Masoud Rahmani. "AN INTRODUCTION TO QUANTUM COMPUTERS." Available online at: https://www.researchgate.net/profile/Hamidreza-Bolhasani/publication/337144719_An_Introduction_to_Quantum_Computers_Architecture/links/5f4c8a97299bf13c5062f83f/An-Introduction-to-Quantum-Computers-Architecture.pdf , Accessed on: Mar. 23, 2021.
[31] Č. Brukner, and Z. Anton, "Information and fundamental elements of the structure of quantum theory." In Time, quantum and information, pp. 323-354. Springer, Berlin, Heidelberg, 2003.
[32] S. Akama, "Elements of Quantum Computing: History, Theories and Engineering Applications" Springer International Publishing Switzerland (2015). Available at http://mmrc.amss.cas.cn/tlb/201702/W020170224608149203392.pdf
[33] E. G. Rieffel, "An Overview of Quantum Computing for Technology Managers." arXiv preprint arXiv:0804.2264 (2008).
[34] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring." In:Proc. of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134(1994)
[35] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21, 120–126 (1978)
[36] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, and C. N. Asogwa. "An overview of Quantum Cryptography and Shor's Algorithm." International Journal 9, no. 5 (2020). https://doi.org/10.30534/ijatcse/2020/214952020
[37] D. Simon, "On the power of quantum computation." In: Proc. of the 35th Annual Symposium on Foundations of Computer Science, pp. 116–123 (1994)
[38] "Grover's Algorithm + Quantum Zeno Effect + Vaidman Bomb," Available online at: https://people.eecs.berkeley.edu/~vazirani/f04quantum/notes/lec10/lec11.pdf Accessed on: Mar. 23, 2021.
[39] A. Montanaro, "Quantum algorithms: an overview. npj Quantum Inf 2, 15023 (2016). https://doi.org/10.1038/npjqi.2015.23
[40] B. Jean-François, and S. Fang, "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields." In Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms, pp. 893-902. Society for Industrial and Applied Mathematics, 2016.
[41] W. C. Huffman, and P. Vera "Fundamentals of error-correcting codes." Cambridge university press, 2010.
[42] R. Alrifai, "Error detection and correction using hamming code." Journal of Computing Sciences in Colleges 35, no. 6 (2020): 121-121.
[43] "An Introduction to Error-Correcting Codes - Part 1" available at: https://www.section.io/engineering-education/understanding-error-correcting-codes-part-1/ Accessed on: Mar. 23, 2021.
[44] M. Rudelson and R. Vershynin, "Geometric approach to error-correcting codes and reconstruction of signals," in International Mathematics Research Notices, vol. 2005, no. 64, pp. 4019-4041, 2005, doi: 10.1155/IMRN.2005.4019.
[45] J.L. Massey, O.N. García, "Error-Correcting Codes in Computer Arithmetic." In: Tou J.T. (eds) Advances in Information Systems Science. Springer, Boston, MA. https://doi.org/10.1007/978-1-4615-9053-8_5 (1972)
[46] N. Wolchover, "How Space and Time Could Be a Quantum Error-Correcting Code" Available online at: https://www.quantamagazine.org/how-space-and-time-could-be-a-quantum-error-correcting-code-20190103/ Accessed on: Mar. 23, 2021.
[47] M. Grassl, "Algorithmic aspects of quantum error-correcting codes." Mathematics of Quantum Computation (2002): 223-252.
[48] K. Guenda, S. Jitman, & T.A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes." Des. Codes Cryptogr. 86, 121–136 (2018). https://doi.org/10.1007/s10623-017-0330-z
[49] D. Gottesman, "An introduction to quantum error correction." In Proceedings of Symposia in Applied Mathematics, vol. 58, pp. 221-236. 2002.