

A Review of Quantum Computing

Arebu Dejen

School of Electrical and Computer Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Addis Ababa, Ethiopia
Email: arbdjn@gmail.com

Murad Ridwan

School of Electrical and Computer Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Addis Ababa, Ethiopia

Received: 15 March 2022; Revised: 28 April 2022; Accepted: 26 May 2022; Published: 08 October 2022

Abstract: Quantum computing is a computational framework based on the Quantum Mechanism, which has gotten a lot of attention in the past few decades. In comparison to traditional computers, it has achieved amazing performance on several specialized tasks. Quantum computing is the study of quantum computers that use quantum mechanics phenomena such as entanglement, superposition, annealing, and tunneling to solve problems that humans cannot solve in their lifetime. This article offers a brief outline of what is happening in the field of quantum computing, as well as the current state of the art. It also summarizes the features of quantum computing in terms of major elements such as qubit computation, quantum parallelism, and reverse computing. The study investigates the cause of a quantum computer's great computing capabilities by utilizing quantum entangled states. It also emphasizes that quantum computer research requires a combination of the most sophisticated sciences, such as computer technology, micro-physics, and advanced mathematics.

Index Terms: Quantum computation, Qubit, Quantum Parallelism, Entanglement

1. Introduction

Today in the computing world, innovations are leading to powerful miniaturized integrated circuits. In accordance with Moore's law, chip capacity is doubled after every 18 months. Making chips smaller, as we approach ~ 10 nm size [1], weird things happen with the electrons reveal quantum nature and the principles of classical physics are no more obeyed at such scales. The classical computers though have become compact and fast. Currently the single transistor on a chip is turned on or off by using around hundreds of electrons [2]. In future it is proposed that the transistors will be controlled by a single electron and is said to be the single electron transistor (SET) in which the laws of classical physics is unable to describe the physical systems but the principles of quantum mechanics are used to explain the physical phenomenon [3]. Due to this it is necessary either to develop new semiconductor chips, which could bypass the quantum nature, or embrace the quantum nature itself [4]. Current researches indicate that embracing the quantum nature takes a high degree choice for scientist. This means to employ the principles of quantum mechanics for building novel computers called quantum computers [5].

Feynman [6] proposed in the 1980s that a quantum computer based on quantum logic would be ideal for modeling quantum-mechanical systems, and his ideas have sparked an active area of computing research. It is also amazing that quantum physics may aid in the resolution of fundamental computer difficulties. Peter Shor [7] developed in 1994 a quantum technique for effectively solving the prime-factorization problem on a given composite integer to identify its prime factors. This is a fundamental problem in computing, and it is estimated, though not proven, that finding the prime factors of big integers is computationally challenging for a classical computer. Shor's technique easily solves the integer factorization problem, providing an exponential performance gain over any known classical approach [8,9].

It is worth noting here that there are cryptographic systems that are widely used nowadays RSA [10, 11]. That is predicated on the assumption that there are no effective techniques for addressing the prime factorization issue. As a result, Shor's algorithm would break the RSA cryptosystem if implemented on a large-scale quantum computer [12]. Lov Grover [13] shown that quantum mechanics may be used to the challenge of searching for a marked item in an unstructured database. In this situation, the advantage above conventional computing is quadratic. Another intriguing feature of the quantum computer is that it, in theory, prevents energy dissipation [14]. Classical computers are naturally dissipative since they are built on irreversible logic operations through gates [15]. Quantum evolution, on the other hand, is unitary, and so quantum logic gates must be reversible. As a result, there is no energy dissipation during a quantum computer run, at least in theory [16]. It is commonly known that on a traditional computer, every complicated calculation can be implemented

using a limited collection of simple logic gates. Fortunately, a quantum computer retains the same feature. In the quantum circuit model, it turns out that each unitary transformation operating on a many-qubit system may be divided into gates acting on a single qubit.

The quantum computer's power promises to solve efficiently the most difficult problems in computational science theory, such as factorization of large integers, database search problems, and discrete logarithms, which are difficult to solve using current classical computers in the speculated time period [17, 18]. Everyone is familiar with the voltage levels used in today's microprocessors to denote physical quantities (1's and 0's). However, in the developing theory of quantum computation, physical quantities are represented in terms of two-state quantum systems [19] by the polarization state of a photon; spin directions of electrons or atomic nuclei in a magnetic field, despite the fact that such systems face numerous challenges. This study provides an overview of quantum-based computational sciences and describes the current state of the art in the topic. The concept of powerful computation and secrecy of future communication is introduced based on quantum computing. This study also discusses the many quantum circuits and kinds of quantum computation, such as parallelism and reverse operations.

2. Current state of the art

Quantum computers have the potential to do calculations far beyond the capabilities of any ordinary supercomputer. Researchers may change the development of novel materials by allowing them to imitate matter's behavior down to the atomic level. They have the potential to destabilize cryptography and security by breaking otherwise unbreakable codes. However, researchers are only now on the verge of developing quantum computers powerful enough to perform tasks that conventional computers cannot [20]. This survey has been evaluated some source of quantum computers presently available at the laboratory level. IBM makes use of quantum events that occur in superconducting materials. The IBM Q [21] quantum cloud service was launched in January 2018. Its current core devices comprise two processors with five superconducting qubits (ibmqx2 and ibmqx4), a 16-qubit processor (ibmqx5), and a 20-qubit processor. In a 15-millikelvin chilly atmosphere, IBM Q (shown in fig.1) operates coherently.

The commercially available D-Wave 2000Q quantum computer [22] uses quantum dynamics to speed and allow novel ways for addressing discrete optimization, sampling, and machine learning issues. To solve a problem, D-Wave systems employ a technique known as quantum annealing. D-Wave systems are being employed for advanced research by some of the world's most sophisticated companies, including Lockheed Martin, Google, NASA Ames, the University of Southern California, and Los Alamos National Laboratory. All of the world's top corporations, including Intel and Microsoft, are investing heavily in quantum technology. Quantum computing, Ion-Q, quantum Circuits, algorithms, teleportation, cryptography, and hardware designs are among the well-funded firms.

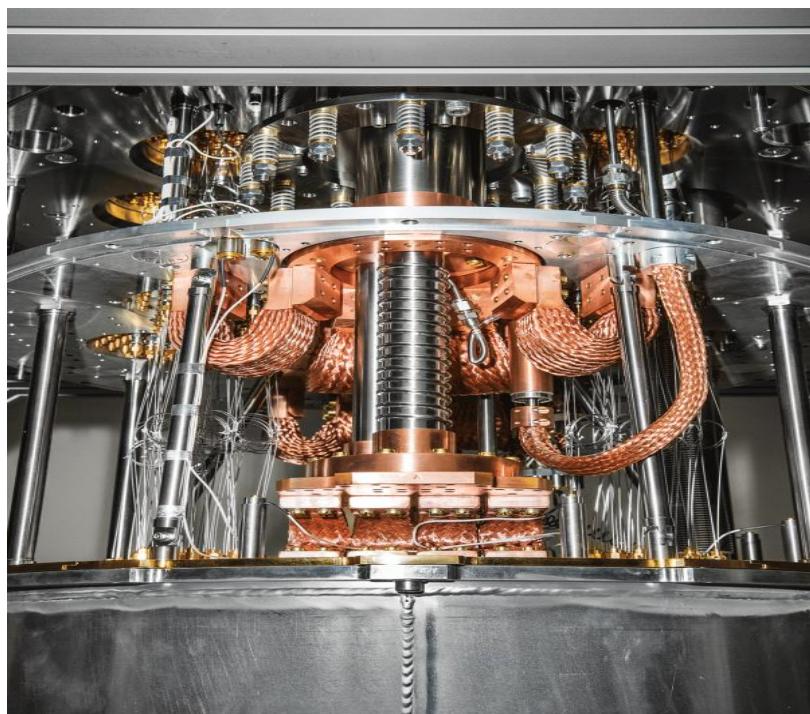


Fig. 1. The chips inside IBM's quantum computer (at bottom) are cooled to 15 millikelvin.[20]

3. Representing Information

Information may be physically manifested in a variety of ways in quantum computing. To have anything similar to a classical bit, we require a quantum computational bit system, also known as a quantum bit or qubit, with just two states when measured. Methods for encoding binary data in a way that allows quantum effects to be noticed (e.g. entanglement and superposition). This bi-stable state quantum system can be physically realized via electron spin, photon polarization, and atom energy level. The most fundamental building unit of a computer, the bit, may only exist in one of two unique states in the classical model, a 0 or a 1.

The rules of a quantum computer are altered. A quantum bit, often known as a 'qubit,' may exist not only in the classical 0 and 1 states, but also in a coherent superposition of both. When a qubit is in this condition, it may be considered of as existing in two worlds, one as a 0 and the other as a 1. An operation on such a qubit affects both values simultaneously. The important point is that by conducting a single operation on the qubit, we have executed the operation on two distinct values. Similarly, a two-qubit system would conduct the operation on four values, while a three-qubit system would perform it on eight. Increasing the number of qubits therefore exponentially increases the quantum parallelism [23]. With the correct type of algorithm it is possible to use this parallelism to solve certain problems in a fraction of the time taken by a classical computer.

A simple quantum system is the two level spin-1/2 particles. Its basis states, spin-down $|\downarrow\rangle$ and spin-up $|\uparrow\rangle$, may be recalled to represent as quantum state zero and one i.e $|0\rangle$ and $|1\rangle$, respectively. The state of single particle is described by the wave function $\Psi = \alpha|0\rangle + \beta|1\rangle$. The squares of the complex coefficients $|\alpha|^2$ and $|\beta|^2$ represent the probabilities for finding the particle in the corresponding states [24].

Generalizing this to a set of k spin-1/2 particles we find that there are new basis states in quantum mechanical vectors that span a Hilbert space corresponding to the 2^k possible bit-strings of length k. The dimensionality of the Hilbert space grows exponentially with k. In some very real sense quantum computations make use of this enormous size even in the smallest systems.

3.1 Hilbert Spaces

The basic notions required to understand the fundamental principles of quantum computations are introduced in Hilbert Space. In finite-dimensional complex linear vector spaces (C^n) the elements of a vector space V are called vectors, in which a vector is singled out by an n-dimension of complex numbers ($a_0, a_1, a_2, \dots, a_n$), of the vector space. In Hilbert space a vector is noted using the Dirac notation symbol $|a\rangle$ and call it a ket. When we assume two vectors $|a\rangle$ and $|B\rangle \in V$ and let c and d are both constant complex numbers the following properties holds true in Hilbert space [25]

1. Addition will give a new vector $|y\rangle = |a\rangle + |B\rangle$
2. Multiplication of vector $|a\rangle$ by complex number c $\rightarrow c|a\rangle$
3. $c(|a\rangle + |B\rangle) = c|a\rangle + c|B\rangle$
4. $(c+d)|a\rangle = c|a\rangle + d|a\rangle$
5. $(cd)|a\rangle = c(d|a\rangle)$
6. Zero vector 0 do not used Ket notation for it $|a\rangle + 0 = |a\rangle$ and $|a\rangle - |a\rangle = 0$
7. Linear independent:- $c_1|a_1\rangle + c_2|a_2\rangle + \dots + c_m|a_m\rangle = 0$ iff a complex number $c_1 = c_2 = \dots = c_m = 0$ only

Inner Product

The inner product of an order of vectors $|a\rangle, |B\rangle \in V$ is a complex number, denoted as $\langle a|B\rangle$ with the following requirements. $\langle a|$ bra notation for vector $|a\rangle$ [26]

- I. $\langle a|B\rangle = \langle B|a\rangle^*$ skew symmetry
- II. $\langle a|cB+dY\rangle = c\langle a|B\rangle + d\langle a|Y\rangle$ linearity
- III. $\langle a|a\rangle \geq 0$ Positivity
- IV. Let $|a\rangle = (a_1, a_2, \dots, a_n)$ and $|B\rangle = (B_1, B_2, \dots, B_n)$ in Hilbert space
 $\langle a|B\rangle = \langle B|a\rangle^* = \sum_{i=1}^n a_i^* B_i$

The norm of vector $|a\rangle$ is defined as $\|a\| = \sqrt{\langle a|a\rangle} = \sqrt{\sum_{i=1}^n |a_i|^2}$

3.2 Qubit

In the present classical computers the electric current flowing through the conducting wires is in the two basic states i.e. when there is no current flowing then it is said to be logical '0' or else when there is flow of current then it is represented as logical '1'[4]. These two states form a bit of information. But in the quantum computation the information is recorded in terms of the two electronic states of quantum bit or 'qubit' that represents $|0\rangle, |1\rangle$ or any value in between them at the same time, which is represented in a two dimensional complex Hilbert space [27]. Vector form representation for single qubit, ket-0 and ket-1 is looks like.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1)$$

Qubit may have a variety of complex coefficients in Hilbert space. However, all qubit vectors are dimensionally limited to a unit vector.

3.3 Multiple Qubits

The potential amount of information available during the computational phase grows exponentially with the size of the system, i.e. the number of qubits. This is because if we have n qubits the number of basis states is 2^n [19]. E.g. if we have two qubits, forming a quantum register then there are four computational basis states: forming, $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ here $|01\rangle$ means qubit-1 is in state $|0\rangle$ and qubit-2 is $|1\rangle$ etc. [20]. we can use a tensor product to relate it as $|01\rangle = |0\rangle \otimes |1\rangle$

4. Superposition

A system can be in two or more states at the same time, which is known as superposition. A single particle, for example, can be going along two separate routes at the same time. This means that the particle possesses wave-like qualities, which might imply that waves from different routes can interfere with one other [21]. Interference can lead the particle to behave in ways that are hard to explain in the absence of these wave-like features. As shown in the figure below a qubit can be exist in $|0\rangle$ state, $|1\rangle$ state or in between base states with different probability.

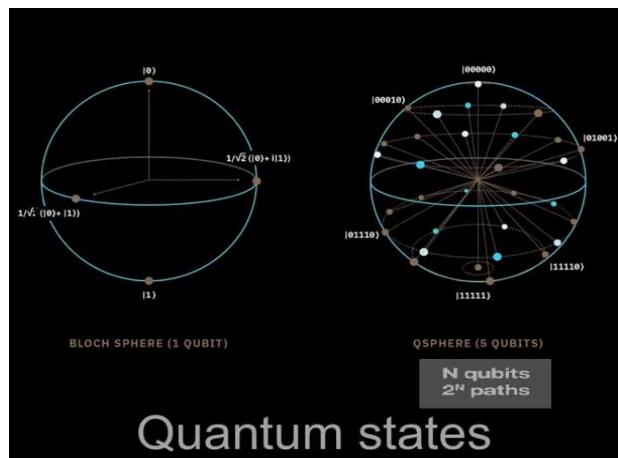


Fig. 2. Superposition of quantum state

Take the electronic states of an atom for the ground and excited levels are defined as $|0\rangle$ and $|1\rangle$ respectively which is in terms of the Dirac notation and is one of the suitable for the quantum computation. But according to the laws of quantum mechanics the electronic state of an atom is the superposition of the two basic states and is represented by the wave function ψ as [22]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2)$$

Where $|\alpha|^2 + |\beta|^2 = 1$, β and α are probability amplitudes and $|0\rangle$ and $|1\rangle$ are base states.

In case of classical computers the two bits can be represented as 00, 01, 10 and 11. But the quantum two-bit in contrast can represent any of those numbers simultaneously. Consequently if the number of qubits increases the number of superposition will exponentially increases which results in calculating the complicated numbers speedily which the current computer technology is not able to compute.

Like a single qubit, the two qubit register can exist in a superposition of the four states as stated below. The notation for the complex coefficients, i.e. probability amplitudes ($\alpha_0, \alpha_1, \alpha_2, \alpha_3$)

$$|\Psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle \quad (3)$$

All of the probabilities must sum to 1, formally for the general case of n qubits this can be written as

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \quad (4)$$

4.1 Tensor Products

A decomposition into single qubits of a multi-qubit system can be represented by a tensor product \otimes ,

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (5)$$

A tensor product can also be used to combine different qubits.

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \alpha_0\beta_0|00\rangle + \alpha_1\beta_0|10\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_1|11\rangle \quad (6)$$

The ability for the particle to be in a superposition is where we get the parallel nature of quantum computing: If each of the states corresponds to a different value then, if we have a superposition of such states and act on the system, we effectively act on all the states simultaneously.

5. Entanglement

Entanglement is the capacity of two particles to interact instantly over any distance. Particles do not communicate directly, but there is a statistical correlation between the results of measurements on each particle that is difficult to comprehend using classical physics. We claim they communicate immediately because they store no local state and only have a well-defined state once measured. Because of this constraint, particles cannot be utilized to send classical signals faster than the speed of light because we only know the states when we measure them. Entanglement is used in a wide range of quantum algorithms and apparatus.

Quantum entanglement for computing is the process by which atoms get entangled in such a manner that they cannot be interfered with by the outside world. The one atom spins in one way, whereas the others spin in different directions that may be mathematically connected [24]. Complex algorithms that answer billions of computations may be constructed by combining superposition and entanglement. With the aid of the entanglement effect, information may be safely transferred from sender to receiver. Any effort to eavesdrop will be discovered, and the communication will be completely disrupted. The key challenge for academics right now is to influence atoms using quantum physics to establish entanglement .

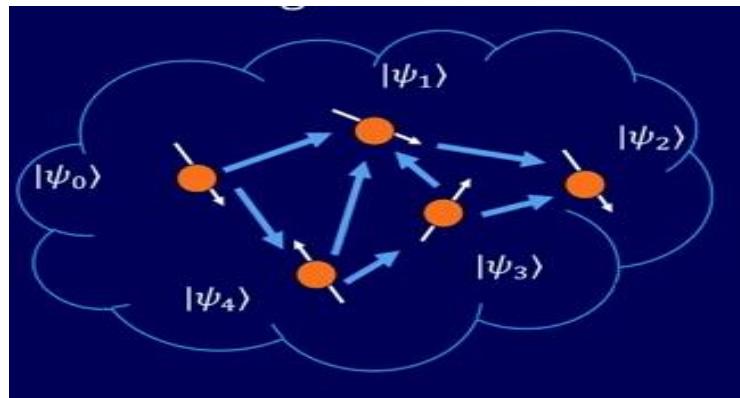


Fig.3. Entangled quantum states

Subatomic particles can be entangled, which implies they are connected no matter how far apart they are. When measured, their influence on each other is immediate. This can be handy in computational situations. Fig.3 shows how qubits are associated in an entangled state. This form of correlation may be applied to the first or second qubit in a variety of ways to produce correlations that are statistically significant. Measuring entangled states accounts for their correlations. This is a significant benefit over traditional calculation.

6. Quantum Parallelism

The property of superposition is exploited to design new quantum microprocessors by developing the concept of parallelism [25]. Atoms in the macroscopic universe travel in a variety of orientations and via various pathways. The main concept is that the computer should employ these atoms to conduct several computations at the same time. In other words, quantum computers can do several calculations concurrently. The quantum computer can factorize big numbers utilizing the idea of parallelism, something the classical computer cannot accomplish. [26] For example, supercomputers can factorize a 500-digit number in billions of years, whereas a quantum computer can accomplish it in a year. Similarly for searching information from the large unsorted database the concept of quantum parallelism can be used.

6.1 Quantum Circuits

A quantum state represents one or more qubits and performs an operation by using a series of unitary operators known as quantum gates. A quantum circuit is the outcome of a succession of unitary operators, as shown in fig.4.

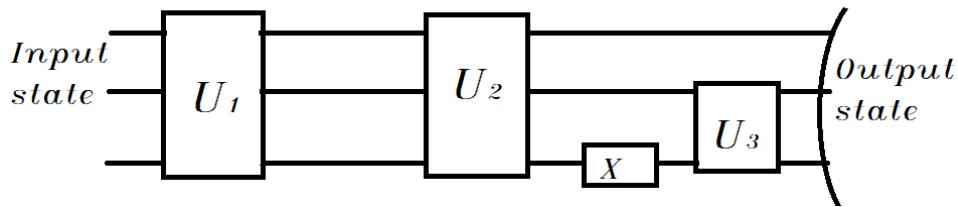


Fig.4. Simple form of quantum circuit

A quantum circuit is a series of operations and measurements are taken at the output on n -qubits state looks like. Each operation is unitary and can be described by $2^n \times 2^n$ matrix. Each line represents an abstract wire, and the boxes that contain U_n represent quantum logic gates or a collection of gates [27]. A quantum circuit may be built and quantum algorithms can be implemented using a mix of quantum gates, wires, input states, and output measurements. Although it is always possible to reorganize quantum circuits, all measurements are performed at the conclusion of the circuit.

6.2. Quantum gates

In addition to conventional logic gates that accept and generate 1's and 0's, there are quantum logic gates that aid in the production and reception of quantum bits. The sole restriction that these gates must meet (as required by quantum computation) is that they must be unitary, where a unitary matrix is one that meets the requirement underneath. This opens up a plethora of potential gates.

$$U^\dagger U = I$$

The matrix performs the function of a quantum operator on a qubit. Because the resulting values must meet the normalizing criterion, the operator's matrix must be unitary. The probability amplitudes must still total to one if they are unitary. Before the procedure, for a particular qubit state

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (7)$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad (8)$$

After the gate is applied

$$|\Psi'\rangle = U|\Psi\rangle = \alpha'|0\rangle + \beta'|1\rangle \quad (9)$$

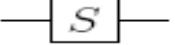
$$|\alpha'|^2 + |\beta'|^2 = 1 \quad (10)$$

6.2.1 Single Qubit Gates

Just as a single qubit can be represented by a column vector, gate acting on the qubit can be represented by a 2×2 matrix. The following table summarizes single qubit gates as name of the gate circuit symbol, matrix equivalency and qubit conversion operation.

Table 1. Single qubit gates

No.	Name of gate	Circuit symbol	Matrix equivalency	Qubit conversion When Applied
1	Pauli I gate		$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$ 0\rangle \rightarrow I \rightarrow 0\rangle$ $ 1\rangle \rightarrow I \rightarrow 1\rangle$ $\alpha 0\rangle + \beta 1\rangle \rightarrow I \rightarrow \alpha 0\rangle + \beta 1\rangle$
2	Pauli X gate		$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$ 0\rangle \rightarrow X \rightarrow 1\rangle$ $ 1\rangle \rightarrow X \rightarrow 0\rangle$ $\alpha 0\rangle + \beta 1\rangle \rightarrow X \rightarrow \alpha 1\rangle + \beta 0\rangle$
3	Pauli Y gate		$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$ 0\rangle \rightarrow Y \rightarrow i 1\rangle$ $ 1\rangle \rightarrow Y \rightarrow -i 0\rangle$ $\alpha 0\rangle + \beta 1\rangle \rightarrow Y \rightarrow \alpha i 1\rangle - \beta i 0\rangle$
4	Pauli Z Gate		$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$ 0\rangle \rightarrow Z \rightarrow 0\rangle$ $ 1\rangle \rightarrow Z \rightarrow 1\rangle$ $\alpha 0\rangle + \beta 1\rangle \rightarrow Z \rightarrow \alpha 0\rangle - \beta 1\rangle$

5	Phase Gate		$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$ 0\rangle \rightarrow S \rightarrow 0\rangle$ $ 1\rangle \rightarrow S \rightarrow i 1\rangle$ $\alpha 0\rangle + \beta 1\rangle \rightarrow S \rightarrow \alpha 0\rangle + \beta i 1\rangle$
---	-------------------	---	--	--

6.2.2 Hadamard Gate

Sometimes called the *square root of NOT gate*, it turns a $|0\rangle$ or a $|1\rangle$ into a superposition (note the different sign). This gate is one of the most important in quantum computing.

$$\text{---} \boxed{H} \text{---}$$

where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (11)

Which outputs for every qubit state as follows

$$\begin{aligned} |0\rangle &\rightarrow H \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow H \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ \alpha|0\rangle + \beta|1\rangle &\rightarrow H \rightarrow \alpha \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) + \beta \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

6.2.3 Multi Qubit Gates

A real quantum gate must be reversible, which necessitates the employment of a control line that is unaffected by the unitary transformation [28]. Take, for example, any two-qubit gate with a 4×4 unitary matrix, as illustrated below in fig. 5.

Unitary Matrix

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Quantum Gate **2nd State**

Fig. 5. Multi-qubit gate operation

The most frequent two-qubit quantum gates are CNOT, CCNOT, Toffoli gate, Not2 gate, and CSWAP gate. However, only the CNOT gate is discussed in detail in this paper work, which is presented at fig.6. The quantum CNOT gate may accept two states lines, one of which is the control line and the other is connected to the NOT gate. Because it is a two-qubit gate, it may be represented as a 4×4 matrix, which yields the following results;

$$\text{where CNOT gate} == \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (12)$$

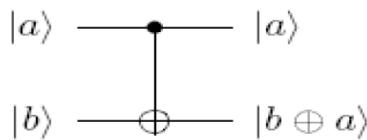


Fig. 6. CNOT gate circuit

The output of the CNOT on each input qubit is calculated as

$$|00\rangle \rightarrow \text{CNOT} \rightarrow |00\rangle$$

$|01\rangle \rightarrow \text{CNOT} \rightarrow |01\rangle$
 $|10\rangle \rightarrow \text{CNOT} \rightarrow |11\rangle$
 $|11\rangle \rightarrow \text{CNOT} \rightarrow |10\rangle$
 $(\alpha|0\rangle + \beta|1\rangle)|1\rangle \rightarrow \text{CNOT} \rightarrow \alpha|00\rangle + \beta|10\rangle$,
 $|0\rangle(\alpha|0\rangle + \beta|1\rangle) \rightarrow \text{CNOT} \rightarrow \alpha|00\rangle + \beta|01\rangle$
 $|1\rangle(\alpha|0\rangle + \beta|1\rangle) \rightarrow \text{CNOT} \rightarrow \alpha|11\rangle + \beta|10\rangle$

Qubit NOT2 Gate

$\text{NOT}_2 = I \otimes X$ is the tensor product of identity gate and not gate. NOT2 gate has the following matrix representation

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The following output on the corresponding input are expected from NOT_2 gate

$|00\rangle \rightarrow \text{NOT}_2 \rightarrow |01\rangle$
 $|01\rangle \rightarrow \text{NOT}_2 \rightarrow |00\rangle$
 $|10\rangle \rightarrow \text{NOT}_2 \rightarrow |11\rangle$
 $|11\rangle \rightarrow \text{NOT}_2 \rightarrow |10\rangle$

7. Reversible Computation

Programs on a quantum computer are performed via unitary evolution of an input provided by the system's state. We can always reverse the computation on a quantum computer since all unitary operators U are invertible with. One of the most challenging aspects of the program for miniaturizing ordinary computers is the difficulties in dissipating heat [29]. Landauer investigated the physical constraints imposed on computing due to dissipation. He demonstrated that practically all calculation processes may be conducted in a reversible way, dissipating no heat. The basic need for any deterministic device to be reversible is that its input and output be uniquely retrievable from one another.

Let a quantum state, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is given as an input and apply on two Hadamard gates, the circuit reverses the input with two level of operation as shown in fig.7. $H^\dagger H = I$, so $|\psi\rangle I = |\psi\rangle$



Fig. 7. Reversibility of quantum operation by two Hadamard gate

As a result of reversibility operation, quantum computer can break the minimum energy for bit operation set by Landauer's principle shown in the fig.8.

Reversibility vs. Landauer's principle

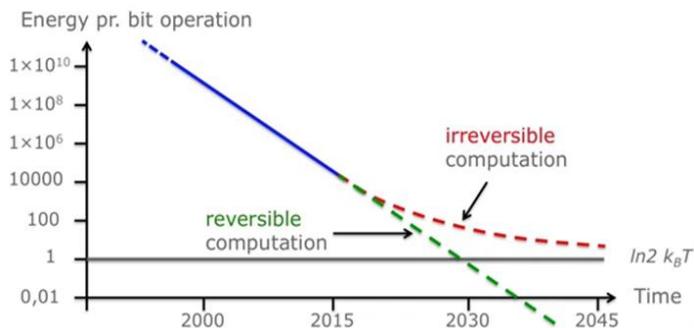


Fig. 8. Reversibility Vs. Landau's principle

8. Challenges in Quantum computation

A quantum computer provides a significant improvement in the utilization of computational resources such as time, energy, and memory. In one piece of quantum gear, a huge parallel computation may be accomplished. This means that it performs the same mathematical operation on $2L$ distinct input numbers recorded in coherent superposition of L

qubits in a single computing step. Because it has $2L$ processors operating in parallel to handle unexpectedly complicated tasks. However, it faces the following major challenges; these can be still a hot research area.

8.1 Building quantum computer

The lack of a well-defined architecture and system model, the absence of standards for qubit implementation, and the computer itself being overly sensitive to the environment all pose significant challenges for researchers attempting to construct a quantum computer. It is commonly known that quantum computation takes place with atomic scale systems in the huge Hilbert space. The computation entails constructing a trajectory from a simple beginning state to a complicated state. The fundamental difficulty in achieving environmental error-free coupling is maintaining this trajectory. The disturbance is caused by coupling to external noise. The ion trap technique, cavity quantum electrodynamics, quantum dots, and nuclear magnetic resonance spectroscopy are the most prevalent promising methods found for isolating quantum systems.

8.2 Qubit implementation

The main issue throughout the calculation process is the implementation of qubits. Qubits can be implemented in a variety of methods, including particle spinning, photon polarization, and the ground and excited states of atoms. While choosing a physical representation of a qubit and measuring qubits are tough tasks. De coherence occurs as a result of quantum material imperfections, affecting computer performance. Various implementation modeling methodologies are continuously being researched by various organizations.

- ★ **Gate model** implementation, which is developed and used by IBM, uses superconducting circuit to implement qubits as computational system.
- ★ **Topological Model** implementation, which is developed and used by Microsoft, and uses quasi-particle for implementation
- ★ **Adiabatic Model** implementation, which is developed and used by D-wave, quantum annealing their method to use qubit as computational service.

8.3 De coherence

To compute, the qubits should couple up, measure their states, and then be kept largely free of interactions that cause noise and de coherence. The quantum information is disseminated outside of the quantum device and lost in the environment, causing the computation to fail [30]. This is referred to as de coherence. Despite this, researchers have succeeded in developing physically realizable systems such as ultra-small Josephson junctions, cold ion traps, nuclear spin quantum computation, harmonic oscillator quantum computation, and NMR quantum computation [31]. However, the major issue that all realization systems face is that of de coherence.

8.4 Measurements

At the conclusion of the logic circuit, each quantum circuit's associated quantum state is measured. However, because the quantum world is irreducibly tiny, measuring a quantum system without having an influence on that system is impossible because our measurement apparatus is likewise quantum mechanical [32]. As a result, it is impossible to correctly anticipate all of a particle's characteristics. When it comes to qualities that occur in complementary pairs, such as spin up or spin down of electrons, if we know one with a high degree of confidence, we must know practically little about the other [33, 34]. Measuring the output state of each logic gate will cope with quantum mechanics' uncertainty rules.

9. Conclusion

This review examined numerous quantum computing computational approaches as well as changes in quantum bit characteristics during the computational phases. A quantum computer has the theoretical capability of replicating any finite physical system and may hold the secret to building an artificially intelligent computer. The capacity of quantum computers to execute operations across a myriad of parallel worlds enables them to perform jobs swiftly that conventional computers would never be able to effectively complete. The research gives an introduction to quantum entanglement computation. The book is packed with information regarding quantum reverse computing and quantum gates. The study also stressed the critical role of qubits on quantum circuits, which is extremely important in the field of research.

References

- [1] Quantum Architectures and Computation Team (Microsoft and Google), "Defining and detecting quantum speedup", *Center for Quantum Information Science & Technology, University of Southern California*, January 2014
- [2] Vitányi P., "Time, space, and energy in reversible computing", In Proceedings of the 2nd conference on Computing Frontiers , PP 435-444, Ischia, Italy May 04 - 06, 2005
- [3] Scott Aaronson, "The Learnability of Quantum States", *University of Waterloo Institute for Quantum Computing*, June 2005

- [4] D-Wave Computing Company, Computational Power Consumption and Speedup Summary, D-wave white paper, 2017
- [5] I.D James, (August 2017), “A History of Microprocessor Transistor Count 1971 to 2017” ,Available: https://en.wikipedia.org/wiki/Transistor_count
- [6] Yuanhao Wang, Ying Li, Zhang-qi Yin, and Bei Zeng, “16-qubit IBM universal quantum computer can be fully entangled”, March 2018, Unpublished.
- [7] Gabriel Târziu, “Quantum Vs. Classical Logic: The Revisionist Approach”, *Logos & Episteme*, Vol. 3, Iss. 4, pp 579-590 , 2012.
- [8] Janet Anders, Saroosh Shabbir, Stefanie Hilt, Eric Lutz, “Landauer’s principle in the quantum domain, Developing in computational model”, *Cornell University Library quant-Phy*, Vol-1 pp. 13-18, 2010
- [9] Vishal Kumar, Asif Ali Laghari, Shahid Karim, Muhammad Shakir, Ali Anwar Brohi , “Comparison of Fog Computing & Cloud Computing” *I.J. Mathematical Sciences and Computing*, 2019, 1, 31-41, DOI: 10.5815/ijmsc.2019.01.03
- [10] Zuhui Subedar, Ashwini Araballi, “ Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication” *I. J. Mathematical Sciences and Computing*, 2020, 4, 35-41, DOI: 10.5815/ijmsc.2020.04.04
- [11] Peter W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, *IEEE Computer Society Press*, January 1996
- [12] Rodney Van Meter, “Quantum Computing’s Classical Problem, Classical Computing’s Quantum Problem”, *Keio University, Japan Foundations of Physic*, Volume 44, Issue 8, pp 819–828, August 2014
- [13] Andrew Lutomirski, Scott Aaronson, Edward Farhi, Peter Shor, “Breaking and making quantum money: toward a new quantum cryptographic protocol”, *Massachusetts Institute of Technology, Cambridge*, December 2009
- [14] Scott Aaronson, Adam Bouland, Joseph Fitzsimons, and Mitchell Lee, “The Space Just Above BQP”, *Massachusetts Institute of Technology, Cambridge*, December 2014
- [15] Paul Isaac Hagouel and Ioannis G. Karayannidis, “Quantum Computers: Registers, Gates and Algorithms”, *Proc. 28th International Conference on Microelectronics*, Serbia, 2012,
- [16] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashe,”On the implausibility of classical client blind quantum computing” , *University of Texas at Austin*, April 2017
- [17] Yazhen Wang, “Quantum Computation and Quantum Information”, *Journal of Statistical Science, Institute of Mathematical Statistics*, Volume 27, PP 373-394,Number 2012
- [18] G. Benenti, G. Casati, G. Strini, “Principles of Quantum Computation and Information”, Volume I, World Scientific Pub Co Inc. New edition edition , 2005
- [19] Scott Aaronson, Andris Ambainis, “Quantum Search of Spatial Regions”, *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Scienc.*, Volume 1, pp. 47–79, June, 2013
- [20] Mingsheng Ying, “Quantum computation and quantum theory”, *Science Direct Artificial Intelligence Journal*, Volume 174, Issue 2, Pages 162-176, February 2010
- [21] Adrien Feix, Mateus Araújo, and Caslav Brukner, “Quantum superposition of the order of parties as a communication resource”, *Institute for Quantum Optics and Quantum Information (IQOQI), Vienna, Austria* March , 2018
- [22] Yang Chen, Shaoshu Li, “A Brief Introduction to Hilbert Space”, *Cornell University Lecture*, December, 2016
- [23] Shuo Sun, Hyochul Kim, Glenn S. Solomon, and Edo Waks, “ A Quantum Phase Switch Between A Single Solid-State Spin And A Photon”, University of Maryland, *Nature Nanotechnology* volume 11, pages 539–544, 2016
- [24] B. C. Sanctuary, “Quantum correlations between separated particles”, *McGill University, Canada*, 2004
- [25] Shailesh Saxena, Mohammad Zubair Khan, Ravendra Singh,” Green Computing: An Era of Energy Saving Computing of Cloud Resources” *I. J. Mathematical Sciences and Computing*, 2021, 2, 42-48, DOI: 10.5815/ijmsc.2021.02.05
- [26] Louis De Broglie, “The wave nature of the electron”, *Ohio State University Nobel Lecture*, December 12, 1929
- [27] Zi-Wen Liu, Christopher Perry, Yechao Zhu, Dax Enshan Koh, and Scott Aaronson, “ Doubly infinite separation of quantum information and communication”, *Massachusetts Institute of Technology Phys. Rev. A. Vol- 93, Iss-1*, January 2016
- [28] A. Imamoglu, D. D. Awschalom, G. Burkard , “Quantum information processing using quantum dot spins and cavity-QED”, *University of California Physical Review Letters*, Vol. 83, Iss. 20, November 1999
- [29] Shaifali Singhal Anjali Jain Anil Kr Gankotriya, “An Investigation of Quantum Teleportation”, *Second International Conference on Advanced Computing & Communication Technologies*, India, 2012
- [30] Y. H. Lee, M. Khalil-Hani, M. N. Marsono, “Improved Quantum Circuit Modeling Based on Heisenberg Representation”, *Springer Science+Business Media Quantum Inf Process*, February 2017
- [31] Aram W. Harrow, Cedric Yen-Yu Lin and Ashley Montanaro, “Sequential measurements, disturbance and property testing”, *Joint Center for Quantum Information and Computer Science, University of Maryland*, October, 2016
- [32] Richard J. Hughes, D. M. Alde, P. Dyer, “Quantum Cryptography”, University of California, Jornal of Contemporary physics, Los Alamos National Laboratory , Volume 36, Issue 3, 1995
- [33] Rui Zhang, Run-hua Shi, Jia-qi Qin, Zhen-wan Peng, “An economic and feasible Quantum Sealed-bid Auction protocol”, , *Springer Science+Business Media on Quantum Inf Process*, January 2018
- [34] Charles H. Bennett, Ethan Bernstein, Gilles Brassard Umesh Vazirani, “Strengths and Weaknesses of Quantum Computing”, *SIAM Journal on Computing*, December 1996

Authors' Profiles



Arebu Dejen has accomplished his BSc degree in electrical and computer engineering from Mekelle University, Tigray, Ethiopia. He has awarded a minister of education top students scholarship for master study in Addis Ababa University. He graduated M.Sc. in Electrical and computer engineering from Addis Ababa institute of Technology, Addis Ababa University Addis Ababa, Ethiopia. Currently, he is a PhD candidate in AAU. His main research topics are computing, algorithm and optimization, electromagnetic wave and their application, antenna and propagation, multi-band antenna, mm-wave communication.



Dr. Murad Ridwan is from Ethiopia. Ha has obtained BSc in Electrical Engineering from Addis Ababa University (AAU), MSc and PhD degrees in Communication Engineering from the same university. He has worked as a satellite base-station and systems engineer and later on as multimedia engineer in satellite communication, Ethiopian telecom. Currently, he is an academic staff at the School of Electrical & Computer Engineering, Addis Ababa Institute of Technology, AAU. His research interests lie primarily in the area of antennas, antenna arrays, beamforming, precoding techniques especially for 5G, electromagnetism, numerical electromagnetics, quantum mechanics and particle physics. He has published several papers. He loves strength exercises, likes playing with mathematics, reading on science, philosophy and religion.

How to cite this paper: Arebu Dejen, Murad Ridwan, "A Review of Quantum Computing", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.8, No.4, pp. 49-59, 2022. DOI: 10.5815/ijmsc.2022.04.05