Journal of Quantum Computing
DOI:10.32604/jqc.2020.015688
Article

Tech Science Press

A Critical Overview on Quantum Computing

Saptarshi Sahoo[1,*], Amit Kumar Mandal[1], Pijus Kanti Samanta[2], Indranil Basu[1] and Pratik Roy[1]

[1]Institute of Engineering and Management Salt Lake Electronics Complex, Kolkata, 700091, West Bengal, India
[2]Department of Physics (PG & UG), Prabhat Kumar College, Contai, 721404, West Bengal, India
[*]Corresponding Author: Saptarshi Sahoo. Email: uzumaki.sahoo@gmail.com
Received: 10 November 2020; Accepted: 26 December 2020

Abstract: Quantum Computing and Quantum Information Science seem very promising and developing rapidly since its inception in early 1980s by Paul Benioff with the proposal of quantum mechanical model of the Turing machine and later By Richard Feynman and Yuri Manin for the proposal of a quantum computers for simulating various problems that classical computer could not. Quantum computers have a computational advantage for some problems, over classical computers and most applications are trying to use an efficient combination of classical and quantum computers like Shor's factoring algorithm. Other areas that are expected to be benefitted from quantum computing are Machine Learning and deep learning, molecular biology, genomics and cancer research, space exploration, atomic and nuclear research and macro-economic forecasting. This paper represents a brief overview of the state of art of quantum computing and quantum information science with discussions of various theoretical and experimental aspects adopted by the researchers.

Keywords: Quantum computing; quantum information science

1 Introduction

Researchers are making new discoveries in this novel area of quantum technology at all levels of the computing system stack, from the design of quantum algorithms to the development of practically realizable devices for qubits, at various laboratories in North America, Europe, China, Japan, etc., by their respective governments and also in the corporate research and development labs of the giant technology companies like Google, IBM, Microsoft, Honeywell and D-Wave [1–7]. Since the development pace is quite fast and the degree of availability of quantum computing services is also improving. Although we do not expect quantum computers to become as commonplace as our modern day personal computers, but they are expected to be available for applications for governments, large research universities and corporates within a decade. Quantum entropy or quantum relative entropy in quantum information theory is an important concept which measures the distinguishability of two quantum states and was introduced by Shanon in 1948 [8]. This entropy is also known as Shannon entropy. It was first shown that Information was equivalent to power/energy through the mathematical formula as:

$$H\left(x\right)=-\sum_{i}P_{X}\left(x_{i}\right)\cdot\log_{b}P_{X}\left(x_{i}\right) \tag{1}$$

Here, Eq. (1) H is the entropy of a random variable X and P_X (x_i) is the probability of possible outcomes of x_i from X. Now for a binary system H can be expressed as [9].

$$H\left(n\right)=\log_{2}\left(n\right) \tag{2}$$

In Eq. (2), unit of H is 'bits'. The conditional form of Shannon entropy can be given as:

$$H\left(X \mid Y\right) = -\sum_{i,j} p\left(x_i, y_i\right) \log \frac{p\left(x_i, y_i\right)}{p\left(y_i\right)} \tag{3}$$

In (3) X and Y are the random variable describing the event taking place and can have values x_i and y_j respectively. $p(x_i, y_i)$ is the probability such that $X = x_i$ and $Y = y_i$. This quantity should be understood as the amount of randomness in the random variable X given the random variable Y. However, near the beginning of 1990, it was shown that information can also be processed using the principles of quantum mechanics mainly, Superposition and Entanglement (Non-local correlation). The information which is processed using the principle of quantum mechanics, known as Quantum Information and the fundamental unit of Quantum Information is called Qubit [10–11]. Quantum Computing is the study of the processes and methods to store and manipulate information governed by the ideals of Quantum Mechanics such as, Superposition and Entanglement. The term Superposition comes from the wave-mechanics phenomena of superposition of more than one wave with each other. The "addition" of waves happens maintaining the relative phases of waves. The term Entanglement is solely from Quantum Mechanics. In mere loose terms it means, more than one entity is somehow connected, altering(measurement) one of them also leads to altering the other. There are set of criterions [12] put forward by David DiVincenzo which tries to summarise the basic structure and needs of a quantum computer, they are:

- A quantum physical system must have two orthogonal basis quantum states.
- It should be possible to prepare the system in one of the orthogonal states.
- There should be a (macroscopic) procedure for measuring the Qubit distinguishably.
- One can create a universal set of Quantum Logic Elements to act upon it.
- Coherence time (Time to remain in superposition upon action of external disturbances) should be longer than decoherence time.
- Scalability: –Should be able to create a huge number of Qubit and is enabled to control each Qubit separately such that all are safe from decoherence.

The above criteria are more like an ideal Quantum Computing. We everyday are trying to check all the above points. But in real machines it is not that much easy. Mostly the last two points are very hard to attain. Ongoing research is going on to bring closer and closer to the above mentioned criteria.

2 Qubit

Qubit can also be defined as a two-state quantum-mechanical system. In the language of mathematics, it can be called a two dimensional vector in Hilbert Space, ($\mathfrak{H}$) [10].

$$\left|\psi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \tag{4}$$

In Eq. (4) a, b $\in \mathbb{C}$, $|\psi\rangle \in \mathfrak{H}$. According to the Born's rule [10], $|a|^2$ gives the probability of getting $|0\rangle$ state and similarly $|b|^2$ gives the probability of getting $|1\rangle$ upon measuring the qubit $|\psi\rangle$. We can further assume two constraints as:

- Unit length ($|a|^2 + |b|^2 = 1$) of the state vector.
- Measurement is not affected by global phase.

Using the above reasoning we can write the expression of qubit in a reduced form Eq. (5):

$$\left|\psi\right\rangle = \cos\frac{\theta}{2}\left|0\right\rangle + e^{i\phi}\sin\frac{\theta}{2}\left|1\right\rangle \tag{5}$$

where, $\varphi \in \mathbb{R}$. One thing is to note that previously in Eq. (4) we needed four Real numbers to denote the qubit state, but in Eq. (5) we only require two real numbers. Hence, it can be mapped to 3-dimensional Euclidean space.

Such representation of a single qubit can be visualized through the Bloch sphere. Fig. 1 is a Bloch Sphere representing the state of a qubit. In a Bloch sphere, a qubit is an arrow residing on the surface of the sphere correspond to the pure states of the system, whereas the interior points correspond to the mixed states tip on a unit radius sphere in $\mathbb{R}^3$ space (see for more details [11]).

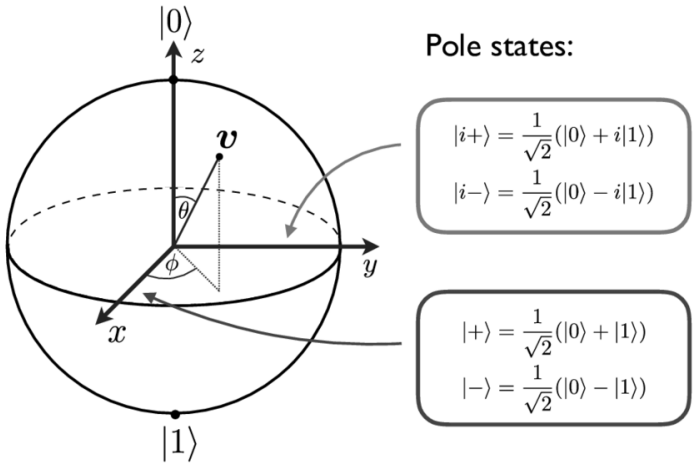

Figure 1: Bloch sphere

2.1 Multiqubit Systems

For more than one qubit system, we define the state vector residing in a composite system, defined by a tensor product. Here we are demonstrating for a two qubits system only. it can be generalized for N-qubit systems. Let System A and System B be associated with Hilbert Spaces, $\mathfrak{H}^{(A)}$ and $\mathfrak{H}^{(B)}$ respectively. Hence Hilbert space $\mathfrak{H}^{(AB)}$ be associated with composite system AB. Mathematically is defined in Eq. (6):

$$\mathfrak{H}^{(A)} \otimes \mathfrak{H}^{(A)} = \mathfrak{H}^{(AB')} \tag{6}$$

In Eq. (6), "$\otimes$" refers to tensor product [44] and a state in the Hilbert space $H^{(AB)}$ can be defined as bellow:

$$\left|\psi_{AB}\right\rangle = \left|\psi_{A}\right\rangle \otimes \left|\psi_{B}\right\rangle = \sum_{j} c_j \left|\alpha_j\right\rangle \tag{7}$$

In Eq. (7), $|\psi_{AB}\rangle \in \mathfrak{H}^{(AB)}$,$|\psi_A\rangle \in \mathfrak{H}^{(A)}$ and $|\psi_A\rangle \in \mathfrak{H}^{(B)}$. Also, $c_j \in C$ and $\{|\alpha_j\rangle\}$ are the orthogonal basis states of $\mathfrak{H}^{(AB)}$.

2.2 Density Operator Formalism and Von-Neuman Entropy

To represent a mixed quantum state (a statistical ensemble of quantum states) [13–14], we approach to density matrix formalism.

$$\rho = \sum_{i} p_i \left|\psi_i\right\rangle\left\langle\psi_i\right| \tag{8}$$

In Eq. (8) $\{|\psi\rangle\}$ are the pure states mixed in an ensemble with probability of p_i. Some properties of Density operator [15]:

- Eq. (9) always holds.

$$Tr\left(\rho\right) = 1 \tag{9}$$

- Eq. (10) holds only for Pure sates.

$$Tr\left(\rho^2\right) = 1 \tag{10}$$

- Eq. (11) holds only for Mixed sates.

$$Tr\left(\rho^2\right) < 1 \tag{11}$$

Time evolution of density operator can be given by von Neumann Eq. [15] (12).

$$i\hbar\frac{\partial\rho}{\partial t} = \left[H, \rho\right] \tag{12}$$

Additionally, through this form, we can also define entropy of quantum information known as Von Neumann Entropy [15]. It is defined as follows:

$$S = -tr\left(\rho \ln \rho\right) = -\sum_i p_i \ln\left(p_i\right) \tag{13}$$

where S is the Von Neumann entropy and other notations are defined above Eq. (8). This formalism is rigorously mathematics oriented. This is generally used to quantify error correction and degree of entanglement of multipartite systems.

3 Quantum State Evolution and Quantum Gate

$$i\hbar\frac{\partial}{\partial t}\left|\psi\left(t,r\right)\right\rangle = H\left|\psi\left(t,r\right)\right\rangle \tag{14}$$

We know that a closed quantum system evolves with time in accordance with the Schrodinger equation (26) [16]. Following this way, we can also deduce quantum states evolve unitarily [10, Chap. 2] through time as:

$$\left|\psi\left(t\right)\right\rangle = U\left(t,t_0\right)\left|\psi\left(t_0\right)\right\rangle \tag{15}$$

Here in Eq. (15), $U\left(t,t_0\right) = T\exp\left[-i\int_{t_0}^{t} H\left(\tau\right)d\tau\right]$; T is the time ordering operator. Classical computers require gates to perform computations. Similarly in quantum computers require gates. Here, the gates are expressed in terms of unitary operators acting on the qubit states. Another important fact is that quantum computers have capability of reversible computation. The reasons being:

- Quantum systems evolve unitarily in time satisfying Schrodinger equation and hence it has an inherent reversible nature.
- If the system is not reversible, some amount of data is deleted in the system (Like adding two numbers and returning their result. The add function is irreversible cause two entities of information goes in and one entity of information comes out). Now by Landauer's principle [17].

$$W = k_b T \ln 2 \tag{16}$$

where k_b is Boltzmann's constant, T is the temperature of the heat sink in Kelvin (Usually the room temperature) and W signifies minimum possible amount of energy required to erase one bit of information. This energy, even very miniscule, can disrupt the states in an unprecedented manner.

There is a great advantage of reversible computing, it costs low energy than irreversible one. Theoretically, a quantum computer should not cost any energy until unless we measure the Qubits to its working basis. Hence, keeping the notion of reversible computing in mind, people must design systems for tasks, that may appear irreversible, should somehow be wrapped by extra bits known as ancillary bits, to accomplish the task. These ancillary bits may not be useful for the output purposes, but is very crucial in the intermediate stages.

3.1 Single Qubit Gates

Hence the Quantum Gates applied must be Unitary, thereby preserving of norm of the state vector. Every single qubit gates are rotations on the Bloch vector on Bloch sphere. Generalized Single Qubit gate can be given in [10, Chap. 4] (17) as:

$$U = \begin{bmatrix} e^{i\left(\alpha-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} & -e^{i\left(\alpha-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} \\ e^{i\left(\alpha+\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} & e^{i\left(\alpha+\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} \end{bmatrix} \tag{17}$$

where $\alpha, \beta, \gamma, \delta \in R$.

Some common single qubit gates are summarized below:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{18}$$

Above (18) is a Hadamard Gate. It is very useful in creation of equivalent superposition of state. Such as:

$$\begin{aligned} H|0\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle \\ H|1\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle \end{aligned} \tag{19}$$

There are also Pauli Gates defined as:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{20}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{21}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{22}$$

Gate (20) is similar to classical not gate. The effects on a single qubit of (20), (21) and (22) are given below:

$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle$

$Y|0\rangle = i|1\rangle \quad Y|1\rangle = -i|0\rangle$

$Z|0\rangle = |0\rangle \quad Z|1\rangle = -|1\rangle$

There are also rotation gates, which rotates a Bloch vector around specified axes.

$$R_x(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} = e^{-i\frac{\theta}{2}X}; \qquad R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} = e^{-i\frac{\theta}{2}Y}$$

$$R_z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix} = e^{-i\frac{\theta}{2}Z}$$

$R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$ defines rotation by angle θ around *X*-axis, *Y*-axis and *Z*-axis respectively in the Bloch Sphere [11].

3.2 Two Qubit Gates

Some of the commonly used two qubit gates are given below [11, Chap. 5]: Most important and widely used to endorse entanglement in a circuit is the CNOT gate. The definition as follows:

$\text{CNOT}|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$

($\oplus$ defines exclusive OR or addition modulo-2) In matrix form it can be represented as:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Another important 2-qubit gate is Swap gate:

$\text{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

3.3 Three Qubit Gates

Some of the commonly used three qubit gates are ccNOT and cSWAP gate.The ccNOT and cSWAP are also called Toffoli gate [18]and Fredkin's gate [19] respectively. Below are the representations.

$$\text{cCNOT}|x\rangle|y\rangle|z\rangle = |x \wedge y \oplus z\rangle; \quad \text{cCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\text{cSWAP}|x\rangle|y\rangle|z\rangle = |x\rangle|x \oplus y\rangle|x \oplus z\rangle; \quad \text{cSWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A descriptive list of Quantum gates and much more detailed information can be found [10–11,20]

4 Quantum Algorithms

Before diving into different types of quantum algorithms let us state that how does Quantum Computation differ from its Classical counterpart. To be precise, the two phenomena, Superposition and Quantum entanglement, enable huge information processing power. In this context, let us explain briefly about Quantum Superposition and Entanglement.

- **Superposition:** Unlike classical bits which can be either in a state 0 or in a state 1 at some instant, a qubit can be in a superposition of state 0 as well as state 1. This is quantum superposition (4). Two qubit case can be stated as Eqs. (23)–(24):

Let two states be:

$$\begin{aligned} |\psi\rangle &= a|0\rangle + b|1\rangle \\ |\phi\rangle &= c|0\rangle + d|1\rangle \end{aligned} \tag{23}$$

where, $|\varphi\rangle, |\psi\rangle \in \mathfrak{H}$. Therefore, superposition state of two qubits can be written as:

$$|\psi\rangle \otimes |\phi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} \tag{24}$$

This enables us to provide quantum parallelism and randomization in the algorithms. Which fastens process by a phenomenal degree? But there is a catch. Measurement destroys the huge parallelism. Hence we need to construct smart and robust algorithms to make use of this excellent power savvily.

- **Entanglement:** It can be defined as a non-local correlation between particles. According to Einstein, it is the "Spooky effect at the distance", and which he never approved off [21]. Although we specify two particles, that is 2 entities but according to quantum mechanics there is only one entity, the wave function of the entangled pair(s). This seems a little counter-intuitive but the mathematics checks out. Afterwards John Bell verified Entanglement with his famous Bell Inequality [22].

For pure states, if the product states cannot be fractured then the states are entangled.

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle\right) \neq |\psi_A\rangle \otimes |\psi_B\rangle \tag{25}$$

$$\begin{aligned} |\psi_{AB}\rangle &= \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_B\rangle + |1_A\rangle|0_B\rangle\right) \\ &= \left(\frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}}\right) \otimes |0_B\rangle \\ &= |+_A\rangle \otimes |0_B\rangle \end{aligned} \tag{26}$$

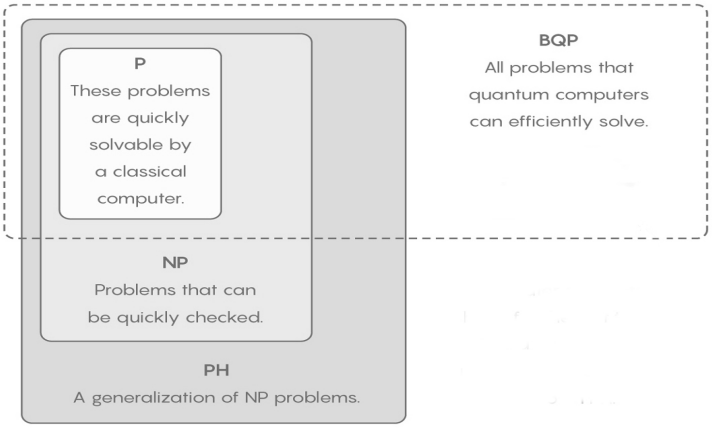

Figure 2: PSPACE

From above we can see that Eq. (25) is an entangled state, whereas Eq. (26) is in product state. In a generalized manner the Bell states, which are maximally entangled can be given as Eq. (27):

$$|\psi(x,y)\rangle = \frac{|0\rangle|y\rangle + (-1)^x|1\rangle|-y\rangle}{\sqrt{2}} \tag{27}$$

where $(x, y) \in \{0,1\}^2$. This plays a great role in solving problems which are having inherent non-locality associated with it. Generally speaking in the area of communication over large distances.

Coming up with good quantum algorithms seems to be a tiresome task. There are at least two reasons supporting the previous statement.

1. Firstly, algorithm design is not an easy task. Finding good quantum algorithms is made doubly difficult because of the additional constraint that we want our quantum algorithms to be better than the best known classical algorithms.
2. A second reason for the difficulty of finding good quantum algorithms is that our intuitions are much better accustomed to the classical world than they are to the quantum world. If we think about problems using our native intuition, then the algorithms which we come up with are going to be classical algorithms. It takes special insights and special tricks to come up with good quantum algorithms.

Before getting into quantum algorithms we would like to point to the complexity class that Quantum computers aim to solve. That class is called BQP (Bounded error quantum polynomial time) [10, Chap. 4]. A decision problem is a member of BQP if there exists a quantum algorithm (an algorithm that runs on a quantum computer) that solves the decision problem with high probability and is guaranteed to run in polynomial time. Making a run of the algorithm will correctly solve the decision problem with a probability of at least 2/3. Loosely we can tell that BQP is the quantum version of BPP. And the suspected shape [23] and space may look like Fig. 2.

Some renowned algorithms as follows:

- **Shor's factoring algorithms:** Historically this algorithm brought many researcher's attention to quantum computing. Basically it is a prescription to find prime factors of a given large number. Classically there are solutions to these factorization problems but are too slow and become intractable for larger numbers $\left[O\left(e^{\mathrm{cn}^{\frac{1}{3}}\log^{\frac{2}{3}}n}\right)\right]$. Using Peter Shor's famous algorithm, the complexity reduces to polynomial time $[O(n^2 \log n \log\log n)]$ [24]. As it is seen that an exponential speedup is acquired. Now, what is the importance of this algorithm? Well, modern Encryption algorithm (RSA) [25] is believed to be secure because we believe that there are no algorithms which enable us to quickly factor large numbers into prime factors. That is, security is based upon our ignorance. But since the discovery of Shor's algorithms, it is only a matter of time, anyone comes with a Quantum Computer and breaches our valuable privacy. Hence we should aspire to make better algorithms to protect our privacy.
- **Quantum cryptography:** It is the process of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is Quantum Key Distribution [26] which offers an theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (No-cloning theorem [27]). This could be used to detect eavesdropping in quantum key distribution. This primarily saves us from Shor's algorithm from breaking RSA encryption. There are other types of algorithms called post-quantum cryptography which are classical algorithms aiming to create cryptographic algorithms which are safe against quantum computers.
- **Quantum teleportation:** This falls rather in communication protocol [28]. According to the No-cloning theorem, one cannot create copies of unknown quantum states. Hence this algorithm allows us to send an unknown quantum state from one part (commonly known as Alice) to another party (commonly known as Bob). In the process Alice loses her quantum state. This is done over a

maximally entangled shared Bell State. In recent times this has been done physically over great distance. This type of communication is physically secured by the laws of quantum mechanics.

- **Grover's search algorithm:** Classically to search an item from a list of unsorted items a classical computer takes $O(N)$. In 1996 Lov Grover came up with a quantum version for this search algorithm from a list of basis states. The time complexity is calculated as $O\left(\sqrt{N}\right)$. A quadratic speed up is achieved [29].

Hence it can be inferred that some problems have better solutions through quantum approach.

5 Errors in Quantum Computing and the Need to Correct Them

As spotted by John Preskill we are in Noisy Intermediate-Scale Quantum (NISQ) systems [30] era of quantum computing, therefore the biggest challenge of today is to create quantum computers which are error prone and can work even if there are errors. In the previous sections we witnessed few advantages of Quantum computing. It is really hard to isolate a quantum system and evolve it unitarily. In practice we tend to observe and work with systems which are a part of huge composite systems. And in most cases, time evolution is not unitary. There are other problems too, even if we somehow completely isolate the system from the surrounding, but when we apply gates they are not ideal Eq. (28), There are going to be some errors (due to decoherence [31,32] and other quantum noise) in the physical realized quantum gates. Hence errors creep in.

$$U = U_0\left(1 + O\left(\varepsilon\right)\right) \tag{28}$$

Here, U will differ from the intended U_0 by some amount of order ε. One might think that computational power is proportionally linked with number of qubits, but he/she should take into account that accommodating larger number of qubits degrades the coherence time (How long can a quantum superposition state survive is called the coherence time. It depends on where a qubit physically lives).

In recent times smart people have come up with quite some smart theoretical techniques that can in effect reduce the errors. Although here we are not going to take a deep look in error-correction theories, we are going to classify different types of error that might occur and affect the information processing. Broadly we can divide errors in 2 types they are:

- **Bit flip Error:** Like classically it flips bits in a bit-steam, thereby corrupting the whole system. Redundancy is a possible solution.

$|0\rangle \rightarrow |1\rangle$
$|1\rangle \rightarrow |0\rangle$

- **Sign-flip Error:** As the name suggested it flips the relative phases and there by creating errors in computation.

$|0\rangle \rightarrow |0\rangle$
$|1\rangle \rightarrow -|1\rangle$

A phase error is serious, because it makes the state orthogonal state $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ flip to the orthogonal state $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

There are channels which create both types of errors simultaneously. And there are known algorithms which try to solve this issue (The Shor's code [33]). Like the theoretical approach, there are many physical approaches done for a particular type of implementation of quantum computing. Since we are in NISQ era, applying Shor's scheme is quite costly, hence it is always tried to come up with algorithms which will require less qubits and errors are automatically managed on its own.

6 Physical Realization

This paper is a theoretical survey on the up-to-date establishing fact on quantum computation. It is really beautiful how collaborative work from all these experts from their respective fields enable us to make machinery as complex as quantum computers. In practice, it can be seen that the description of qubit exactly matches the property of spin in spin- 1⁄2 particles [34]. Hence electrons serve as a good candidate for serving as a qubit. We get two orthogonal states as spin up and spin down. There are also photons which can be used as a qubit [10,35–36]. Since photons are spin-1 particles, it is spin is not used rather its polarization characteristic is used. We get two distinctive states namely, horizontal and vertical polarization. There are other models such as NMR [34], quantum dot [37], superconducting qubits [38], Ion trap [34], etc, are currently used as well as are under research and development to better the implementations. Trapped ions are among the most promising systems for practical quantum computing (QC). The basic requirements for universal QC have all been demonstrated with ions, and quantum algorithms using few-ion-qubit systems have been implemented. A descriptive review can be found in [39]. The dynamics and working of trapped ion type quantum computer can be found here [40]. They [41] present model capturing the essential physics and use tight-binding simulations for a more quantitative analysis thereby discussing the relevance of our findings to the development of compact and scalable electron–spin qubits in silicon. Superconducting qubits [42] are solid state electrical circuits fabricated using techniques borrowed from conventional integrated circuits. They are based on the Josephson tunnel junction [43], the only non-dissipative, strongly non-linear circuit element available at low temperature. Liquid state nuclear magnetic resonance (NMR) techniques have produced some spectacular successes in the construction of small quantum computers [44]. Recently there is another approach in physical realization of quantum computing, nitrogen–vacancy (NV) [45] centers in diamond. NV type quantum computer are the most closest we get for operating a quantum computer at room temperature. In this review [45], they briefly discuss the understanding and prolonging center spin coherence, steering and probing spin states with dedicated quantum control techniques, and exploiting the quantum nature of these multi-spin systems, such as superposition and entanglement, to demonstrate the superiority of quantum information processing.

7 Conclusion

This concludes our overview of Quantum Computer. We have seen three converging parts which support this subject's existence and further growth.

1. **Quantum computers can solve hard problems.** It seems that a new classification of complexity has been erected, a classification better founded on the fundamental laws of physics than traditional complexity theory, which is called BQP. It primarily consists of classes of NP, P and also outside PH class.
2. **Quantum errors can be corrected.** With suitable coding methods, we can protect a complicated quantum system from the destructive effects of decoherence. More error correction algorithms are emerging to surface which shall aid us to create more error prone Quantum computers.
3. **Quantum hardware can be constructed.** We are privileged to be witnessing the dawn of the age of coherent manipulation of quantum information in the laboratory.

Acknowledgement: We are grateful to the peoples for the support and encouragement.

Funding Statement: The author(s) received no specific funding for this study.

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

References

[1] A. Cho, "Google claims quantum computing milestone," *Science*, vol. 365, no. 6460, pp. 1364–1390, 2019.

[2] P. Jurcevic, A. Javadi-Abhari, L. S. Bishop, I. Lauer, D. F. Bogorin *et al.,* "Demonstration of quantum volume 64 on a superconducting quantum computing system," arXiv preprint arXiv:2008.08571, 2020.

[3] S. Moses, J. Pino, J. Dreiling, C. Figgatt, J. Gaebler *et al.,* "Demonstration of the QCCD trapped-ion quantum computer architecture," arXiv preprint arXiv:2003.01293, 2020.

[4] J. Gukelberger, M. Roetteler and M. Troyer, "A case study for quantum software development: Linear systems solver," *American Physical Society*, vol. 2019, no. 1, 2019.

[5] R. LaRose, "Overview and comparison of gate level quantum software platforms," *Quantum,* vol. 3, no. 1, pp. 130–140, 2019.

[6] F. Hu, B. N. Wang, N. Wang and C. Wang, "Quantum machine learning with d-wave quantum computer," *Quantum Engineering*, vol. 1, no. 2, pp. e12–e20, 2019.

[7] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala *et al.,* "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, 2019.

[8] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[9] T. F. E. Wikipedia, "Entropy (information theory)," [Online]. Available: https://en.wikipedia.org/wiki/Entropy_(information_theory).

[10] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," *Physics Today*, vol. 54, no. 2, pp. 60–68, 2001.

[11] N. S. Yanofsky and M. A. Mannucci, "Quantum computing for computer scientists," Cambridge University Press, 2008.

[12] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte der Physik: Progress of Physics*, vol. 48, no. 9, pp. 771–783, 2000.

[13] J. Von Neumann, "Mathematical foundations of quantum mechanics: New edition," Princeton University Press, 2018.

[14] D. McMahon, "Quantum computing explained," John Wiley & Sons, 2007.

[15] E. Schrödinger, "An undulatory theory of the mechanics of atoms and molecules," *Physical Review*, vol. 28, no. 6, pp. 1049–1056, 1926.

[16] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development*, vol. 5, no. 3, pp. 183–191, 1961.

[17] T. Toffoli, "Reversible computing," in *International Colloquium on Automata, Languages, and Programming,* pp. 632–644, Springer, 1980.

[18] E. Fredkin and T. Toffoli, "Conservative logic," *International Journal of Theoretical Physics*, vol. 21, no. 3, pp. 219–253, 1982.

[19] T. F. E. Wikipedia, "Quantum logic gate," 2019. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_logic_gate.

[20] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, pp. 777–787, 1935.

[21] G. Blaylock, "The EPR paradox, bell's inequality, and the question of locality," *American Journal of Physics*, vol. 78, no. 1, pp. 111–120, 2010.

[22] R. Raz and A. Tal, "Oracle separation of BQP and PH," in *Proc. of the 51st Annual ACM SIGACT Sym. on Theory of Computing*, pp. 13–23, 2019.

[23] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[24] W. P. Wardlaw, "The RSA public key cryptosystem," in *Proc. of the Conf. on Coding Theory and Cryptography*, pp. 101–123, Springer, 2000.

[25] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," arXiv preprint arXiv:2003.06557, 2020.

[26] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[27] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1902, 1993.

[28] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pp. 212–219, 1996.

[29] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, no. 1, pp. 79–85, 2018.

[30] H. D. Zeh, "On the interpretation of measurement in quantum theory," *Foundations of Physics*, vol. 1, no. 1, pp. 69–76, 1970.

[31] M. Schlosshauer, "Decoherence, the measurement problem, and interpretations of quantum mechanics," *Reviews of Modern Physics*, vol. 76, no. 4, pp. 1267–1278, 2005.

[32] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, pp. R2493–R2499, 1995.

[33] J. Preskill, "Lecture notes for physics 229: Quantum information and computation," *California Institute of Technology*, vol. 16, no. 1, pp. 1–8, 1998.

[34] F. Flamini, N. Spagnolo and F. Sciarrino, "Photonic quantum information processing: A review," *Reports on Progress in Physics*, vol. 82, no. 1, pp. 016001-016010, 2018.

[35] N. Savage, "Building quantum computers with photons." [Online]. Available: https://spectrum.ieee.org/tech-talk/computing/hardware/building-quantum-computers-with-photons.

[36] M. A. Eriksson, M. Friesen, S. N. Coppersmith, R. Joynt, L. J. Klein *et al.,* "Spin-based quantum dot quantum computing in silicon," *Quantum Information Processing*, vol. 3, no. 1, pp. 133–146, 2004.

[37] Z. Zhou, S. I. Chu and S. Han, "Quantum computing with superconducting devices: A three-level squid qubit," *Physical Review B*, vol. 66, no. 5, pp. 054527–054537, 2002.

[38] C. D. Bruzewicz, J. Chiaverini, R. McConnell and J. M. Sage, "Trappedion quantum computing: Progress and challenges," *Applied Physics Reviews*, vol. 6, no. 2, pp. 021314–021321, 2019.

[39] D. Leibfried, R. Blatt, C. Monroe and D. Wineland, "Quantum dynamics of single trapped ions," *Reviews of Modern Physics*, vol. 75, no. 1, pp. 281–292, 2003.

[40] A. Corna, L. Bourdet, R. Maurand, A. Crippa, D. Kotekar-Patil *et al.,* "Electrically driven electron spin resonance mediated by spin–valley–orbit coupling in a silicon quantum dot," *NPJ Quantum Information*, vol. 4, no. 6, pp. 1–9, 2018.

[41] M. H. Devoret, A. Wallraff and J. M. Martinis, "Superconducting qubits: A short review," arXiv preprint cond-mat/0411174, 2004.

[42] Y. A. Pashkin, O. Astafiev, T. Yamamoto, Y. Nakamura and J. S. Tsai, "Josephson charge qubits: A brief review," *Quantum Information Processing*, vol. 8, no. 2, pp. 55–80, 2009.

[43] J. A. Jones, "Nmr quantum computation: A critical evaluation," *Fortschritte der Physik: Progress of Physics*, vol. 48, no. 9, pp. 909–924, 2000.

[44] I. Oliveira, R. Sarthour Jr, T. Bonagamba, E. Azevedo and J. C. Freitas, "NMR quantum information processing," Elsevier, 2011.

[45] G. Q. Liu and X. Y. Pan, "Quantum information processing with nitrogen vacancy centers in diamond," *Chinese Physics B*, vol. 27, no. 2, pp. 020304–020312, 2018.