Quantum Computing Basics: A Research Perspective for Beginners

Karan Yadav
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
ykaran12x@gmail.com

Tanmay Kurale
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
tanmaykurale289@gmail.com

Aashu K. Rajbhar
Department of Computer Science and Engineering
Jain Deemed-to-University
Bengaluru, India
aashurajbhar20@gmail.com

Chandra Bhusan K. Yadav
Department of Computer Science and Engineering
Jain Deemed-to-University
Bengaluru, India
juisch20220010845@gmail.com

Subhash P. Sah
Department of Computer Science and Engineering
Jain Deemed-to-University
Bengaluru, India
prasdsah500@gmail.com

Moin Hasan
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
mmoinhhasan@gmail.com

***Abstract*—In this article we present a comprehensive overview of fundamental concepts in quantum computing tailored for novices. Unraveling the intricacies of qubits and gates, we establish a foundational understanding of this transformative field. Our exploration extends to the bewildering phenomena of superposition and entanglement, offering insights into their real-world implications such as quantum teleportation. Beyond theoretical exploration, we examine potential research avenues, encompassing quantum algorithms and machine learning applications. This article serves as a gateway for enthusiasts, bridging the knowledge gap and providing a solid introduction to the multifaceted landscape of quantum computing research.**

Keywords*— *Quantum Computing, Qubits, Gates, Superpostion, Entanglement, Quantum Teleportation, Quantum Algorithms

I. Introduction

Quantum computing is a multidisciplinary field comprising aspects of computer science, physics, and mathematics that utilizes quantum mechanics to solve complex problems faster than classical computers [1], [2], [3]. The field of quantum computing includes hardware research and application development. Quantum computers are able to solve certain types of problems faster than classical computers by taking advantage of quantum mechanical effects, such as superposition and quantum interference [4], [5].

Quantum computers use qubits, which are different from bits in classical computers in that they can exist in several states at once and do operations in parallel [6], [7]. This special quality has the potential to solve challenging issues that are now beyond the capabilities of traditional computers, especially in the fields of modeling, optimization, and cryptography. A qubit in quantum computing is the basic unit of information, capable of existing in multiple states simultaneously through superposition and exhibiting entanglement for enhanced computational capabilities [8], [9], [10]. A qubit can be in a state of 1 or 0 or a superposition of both. Using linear algebra, the state of a qubit is described as a vector and is represented by a single column matrix $\begin{bmatrix} a \\ b \end{bmatrix}$. Qubit 0 and qubit 1 are represented in Eq.1 and Eq.2 respectively.

$$\text{Qubit } 0 = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1}$$

$$\text{Qubit } 1 = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2}$$

Where, $|0\rangle$ and $|1\rangle$ are known as Ket-0 and Ket-1 respectively. Transpose conjugate of Ket is known as Bra ($\langle 0|$ and $\langle 1|$). It is also known as a quantum state vector and must meet the requirement that $[a]^2 + [b]^2 = 1$.The elements of the matrix represent the probability of the qubit collapsing one way or the other, with $[a]^2$ being the probability of collapsing to zero, and $[b]^2$ being the probability of collapsing to one. The following matrices all represent valid quantum state vectors.

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}, and \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{bmatrix}$$

Quantum operations can also be represented by a matrix. When a quantum operation is applied to a qubit, the two matrices that represent them are multiplied and the resulting answer represents the new state of the qubit after the operation. For example, Pauli-X Gate as given in Eq. 3 is used to flip the state of a qubit from 0 to 1 (or vice-versa) as shown in Eq. 4

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{4}$$

Similarly, Hadamard Gate as given in Eq. 5 puts a qubit into superposition state where it has an even probability of collapsing either way, as shown in Eq.6

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{5}$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}. \tag{6}$$

Notice that $[a]^2 = [b]^2 = 0{,}1$ meaning that the probability of collapsing to zero and one state is the same [11]. Both Pauli-X Gate and Hadamard Gate are further discussed in Section II. One important aspect to be considered here is that a matrix which represents a quantum operation has one requirement – it must be a unitary matrix. A matrix is unitary if the inverse of the matrix is equal to the conjugate transpose of the matrix.

Quantum computing is crucial due to its potential to solve complex problems faster than classical computers, posing challenges to cryptography while offering secure communication solutions. Its applications span optimization tasks, drug discovery, materials science, machine learning, climate modeling, financial simulations, and artificial intelligence; promising breakthroughs and advancements across various industries. However, the field is still in its infancy, facing significant technical challenges such as error correction and maintaining the delicate quantum coherence required for computation. As researchers strive to overcome these obstacles, the ongoing development of quantum computing stands poised to revolutionize various industries and scientific fields.

Therefore, in this article, we present a basic view of quantum computing with specific attention towards the beginners. This article covers the introductory concepts of quantum computing explaining qubit, quantum gates, and important quantum mechanisms, etc. In addition, it also discusses in-demand research domain towards quantum computing.

Rest of the article is organized as follows: Section II comprises of the quantum gates followed by the basics of quantum mechanics in section III. Research areas in quantum computing are explained in section IV. The paper is finally concluded in section V.

II. Quantum Gates

Quantum gates are fundamental building blocks in quantum computing, analogous to classical logic gates in classical computing. Quantum gates perform operations on qubits, and manipulate their quantum states [12], [13]. Quantum gates can be broadly classified as:

a) Single qubit gates
b) Multiple qubit gates

A. Single Qubit Gates

Single qubit gates are quantum gates that operate on individual qubits in quantum computing. These gates manipulate the quantum state of a single qubit, allowing for the creation of various quantum states and the performance of specific quantum operations. The popular single qubit gates are Pauli Gates (Pauli-X, Pauli-Y, and Pauli-Z) and Hadamard Gate. They are explained as follows:

- Pauli Gates: Pauli Gates are fundamental quantum logic gates used in quantum computing to manipulate qubits, which are the basic units of quantum information. They are named after the physicist Wolfgang Pauli. It is essential for performing various quantum operations, including quantum algorithms and quantum error correction. There are three main Pauli Gates, viz., Pauli-X Gate, Pauli-Y Gate, and Pauli-Z Gate

The Pauli-X Gate plays a role analogous to the NOT in the classical computing. The Pauli-X Gate flips the state of a qubit. If a qubit is initially in the state |0⟩, applying the Pauli-X Gate changes it to |1⟩, and vice versa. In Fig.1, the function of the Pauli-X gate is depicted, while Fig.2 illustrates the transformation in the qubit's state on the Q-Sphere following the application of the Pauli-X gate. The equation (5) shows the bra-ket notation for Pauli-X gate.

Q-sphere provides the visual representation of the states of the single qubit as well as multiple qubits [14]. A qubit can be anywhere on the surface of the sphere, indicating its superposition state. In the Q-sphere representation, the states |0⟩ and |1⟩ of a qubit are typically depicted at opposite poles of the sphere, similar to the North and South poles of the Earth.

- |0⟩ State Representation:

The state |0⟩ of a qubit is represented by a point at the "North Pole" of the Q-sphere. This point signifies that the qubit is in the pure state |0⟩, meaning it's certain to yield the outcome 0 upon measurement.

- |1⟩ State Representation:

The state |1⟩ of a qubit is represented by a point at the "South Pole" of the Q-sphere. This point signifies that the qubit is in the pure state |1⟩, meaning it's certain to yield the outcome 1 upon measurement.

$$\sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{5}$$

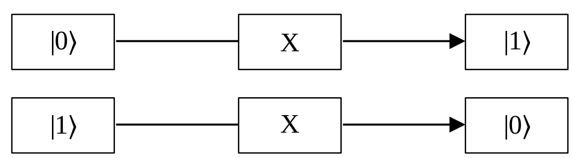

Fig.1: Pauli - X Gate

The Pauli-Y Gate (Fig.3) changes the state of a qubit and introduces a phase shift similar to a bit flip and a phase flip in combination rotation around y-axis by π. Fig.4 shows the operation of Pauli-Y gate on a qubit on Q-sphere.

$$\sigma_y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} = i|1\rangle\langle 0| - |0\rangle\langle 1| \tag{6}$$

The Pauli-Z Gate is a single-qubit gate that leaves the |0⟩ state unchanged and introduce a phase flip (sign change) to the |1⟩ state. This gate is crucial in quantum algorithms for manipulating and transforming qubits states, and it plays a role in creating superposition states and implementing various quantum operation. Pauli-Z Gate action on Q-Sphere are represented in Fig.6

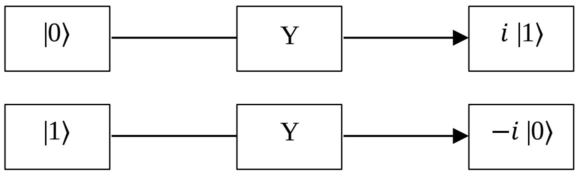

Fig.3: Pauli-Y Gate

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{7}$$

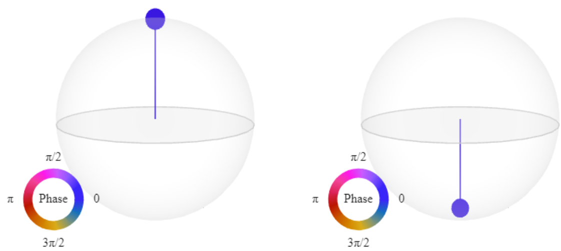

Fig.2. Q-Sphere Representation on Pauli-X Gate

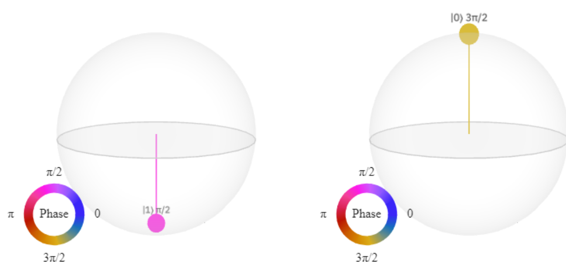

Fig.4 Q-Sphere Representation on Pauli-Y Gate

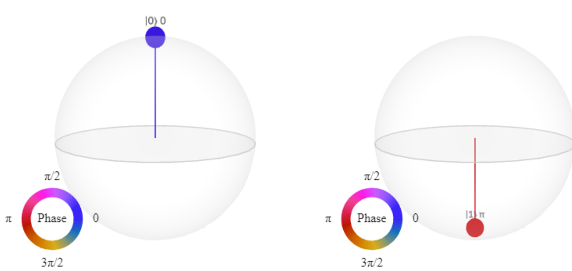

Fig.6. Q-Sphere Representation on Pauli-Z Gate

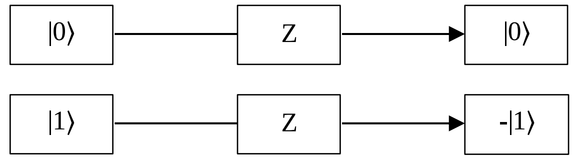

Fig.5: Pauli - Z Gate

- *Hadamard gate*

The Hadamard Gate (Fig.7), often denoted as H, is a fundamental quantum gate that plays a role in quantum computing and quantum algorithms. The Hadamard Gate operates on a single qubit in superposition state. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

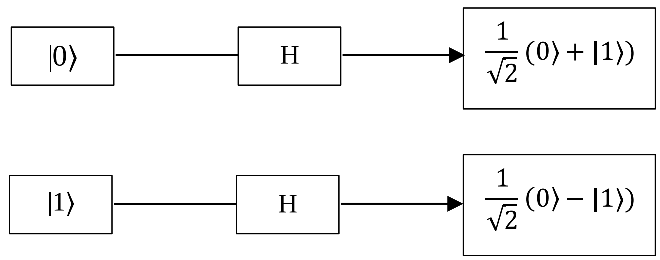

Fig.7: Hadamard Gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \tag{8}$$

- *Phase Gate*

A phase Gate, often represented as S or T, is a type of single-qubit quantum gate used in quantum computing. These gates introduce phase shifts to the quantum states of qubits meaning that add $\Omega/2$ to the phase.

B. Multiple Qubits Gates

Two-qubit quantum gates are quantum gates designed to operate on pairs of qubits in quantum computing. Unlike single-qubits gates that act on individual qubits, two-qubits gates manipulate the quantum state of two qubits simultaneously. These gates play a crucial role in creating entanglement, enabling quantum parallelism, and facilitating the execution of more complex quantum algorithms.

- *CNOT Gate*

The CNOT Gate, or Controlled Not Gate, is a fundamental two-qubit quantum gate in quantum computing [15], [16]. The CNOT Gate performs a specific operation on two qubits: it flips the state of the target qubit (the second qubit) if the control qubit (the first qubit) is in the state $|1\rangle$.CNOT Gate is shown in equation (9).

Table 1: Conversion of CNOT Gate

$\|a\rangle$	$\|b\rangle$	$\|a\oplus b\rangle$
0	0	0
0	1	1
1	0	1
1	1	0

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{9}$$

- *Swap Gate*

The SWAP Gate (equation 10), also known as the exchange gate or the interchange gate, is a fundamental two-qubit quantum gate in quantum computing. It performs the operation of exchanging the quantum states of two qubits. This gate is essential for various quantum algorithms and quantum circuit constructions

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{10}$$

- *CZ Gate*

The CZ Gate(eqn.11), or Controlled-Z Gate, is a two-qubit quantum gate in quantum computing. It is a controlled phase shift gate, meaning it applies a phase shift to the target qubit's state based on the state of the control qubit

$$\text{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{11}$$

- *Toffoli Gate*

The Toffoli Gate(eqn.12), also known as the CNOT Gate, is a three-qubit quantum gate in quantum computing [17]. It performs a NOT operation on a target qubit (the third qubit) only if both control qubits (the first and second qubits) are in the state |0>.

$$\text{Toffoli} = \begin{bmatrix} I4 & 0 \\ 0 & CNOT \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{12}$$

III. BASIC QUANTUM MECHANISMS

Delving into the fundamentals of quantum mechanics, our exploration begins with the cornerstone concept of superposition followed by quantum entanglement and teleportation.

A. *Superposition*

Superposition is a fundamental concept in quantum mechanics that also plays a crucial role in quantum computing [18], [19], [20]. In classical computing, bits exist in one of two states: 0 or 1. Quantum bits, or qubits, on the other hand, can exist in a superposition of both 0 and 1 states simultaneously. Mathematically, this is represented as a linear combination of the 0 and 1 states, denoted as $|0\rangle$ and $|1\rangle$. The qubit state is often expressed as $\alpha|0\rangle + \beta|1\rangle$, where$\alpha$ and β are complex numbers representing probability amplitudes. This unique property of qubits is a key feature exploited in quantum computing algorithms. In the initial state, the qubits are prepared in the $|0\rangle$ state. Upon the application of the Hadamard gate, the qubits enter into equal superposition, evolving into a state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Following this superposition state, a measurement operation resolves the qubits to a definite state, resulting in either $|0\rangle$ or $|1\rangle$ with probabilities determined by the coefficients in the superposition. Superposition state can be achieved by using Hadamard gate as shown in Fig.8. When a measurement is made on a qubit, its superposition collapse to one the basis states ($|0\rangle$ or $|1\rangle$) as shown in Fig.9 with a probability determined by the square of the magnitude of the probability amplitudes. Quantum superposition is a key resource that sets quantum computing apart from classical computing. It allows quantum computers to process information in ways that classical computers cannot, opening the door to solving certain types of problems more efficiently.

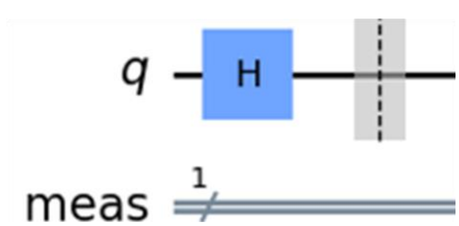

Fig.8 Superposition before measuring

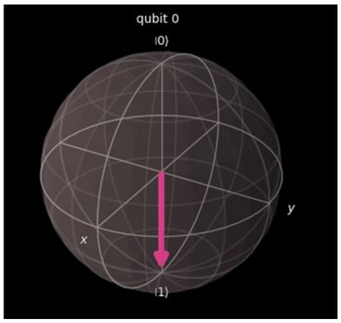

Fig.9: Collapse in state 1 after measuring

B. Entanglement

Quantum entanglement is a phenomenon in quantum mechanics where two or more particles become correlated in such a way that the state of one particles is directly related to the state of the other, regardless of the distance between them [21], [22]. This correlation is maintained even if the entangled particles are separated by large distances. The concept of entanglement is a fundamental aspect of quantum mechanics and has significant implications for quantum computing.

In classical physics, the properties of separated objects are independent of each other. In quantum entanglement, the states of entangled particles are correlated in a way that goes beyond classical explanations. Entangled states are often described using Bell states, which are specific superpositions of two qubits. The most well-known Bell state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$, where $|00\rangle$ and $|11\rangle$ represent the possible states of two entangled qubits.

C. Quantum Teleportation

Quantum teleportation is a remarkable phenomenon in the field of quantum information theory that allows the transmission of quantum states from one location to another, without physically moving the particles themselves [23], [24], [25], [26]. Unlike the teleportation depicted in science fiction, quantum teleportation relies on the principles of quantum mechanics, particularly quantum entanglement and classical communication, to achieve its objectives. One of the first scientific articles to investigate quantum teleportation is "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels"[1] published by C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters in 1993, in which they proposed using dual communication methods to send/receive quantum information [27], [28]. Entangled states are often described using Bell states, which are specific superpositions of two qubits. The most well-known Bell state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$, where $|00\rangle$ and $|11\rangle$ represent the possible states of two entangled qubits.

- Principles of Quantum Teleportation:

The fundamental principles underlying quantum teleportation involve exploiting the phenomenon of quantum entanglement and leveraging classical communication channels. The process typically requires three main components: the sender, the receiver, and a shared entangled pair of particles.

- Entangled Pair Generation: The process begins with the creation of an entangled pair of particles, usually qubits, which exhibit a special type of correlation known as entanglement [29], [30]. These particles are often referred to as the "Bell pair" or "EPR pair." The entangled pair is typically generated through techniques such as spontaneous parametric down-conversion or quantum circuits.
- State Preparation: The sender (P1) possesses a quantum particle whose state (usually represented as a qubit) she wishes to teleport to the receiver (P2) [31]. P1 and P2 also share one of the entangled particles from the Bell pair as shown in Fig.13.
- Measurement and Classical Communication: Alice performs a joint measurement on the quantum state she wishes to teleport and her portion of the entangled pair. This measurement collapses the combined state of the two particles, resulting in a classical outcome. She then communicates the outcome of her measurement to Bob using classical communication channels, such as a conventional data transmission.
- State Reconstruction: Upon receiving Alice's measurement results, Bob applies a specific quantum operation, dependent on the classical information received, to his portion of the entangled pair. This operation transforms the state of Bob's particle into an approximation of the original state of the particle initially possessed by Alice.
- Bell State:

Bell states, also known as EPR pairs, are foundational quantum states that play a pivotal role in various quantum information tasks and experiments. First introduced by John Bell in the context of quantum entanglement, Bell states have since become a cornerstone of quantum information theory. Bell states are a set of four (shown in eqn.(13,14,15,16)) maximally entangled quantum states shared between two particles, typically qubits. Each Bell state represents a distinct correlation between the states of the two qubits, transcending classical correlations.

Creating Bell state using qiskit:

For creating bell state we use Hadamard Gate and CN0T on qubits $|00\rangle$. Entangle state is a state $|\Psi\rangle$ that cannot be expressed as a tensor product $|q1\rangle \oplus |q2\rangle$.Fig.10 and Fig.11 show the gates required and it's calculation using Hadamard equation, CNOT equation to create Bell states.

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle \tag{13}$$

$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle \tag{14}$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle \tag{15}$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle \tag{16}$$

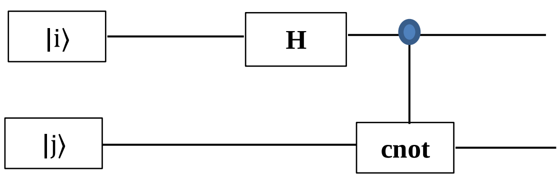

Fig.10 Quantum Circuit for Bell State Generation

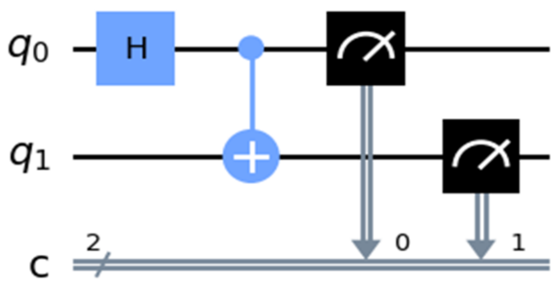

Fig 11: Bell State

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

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$$

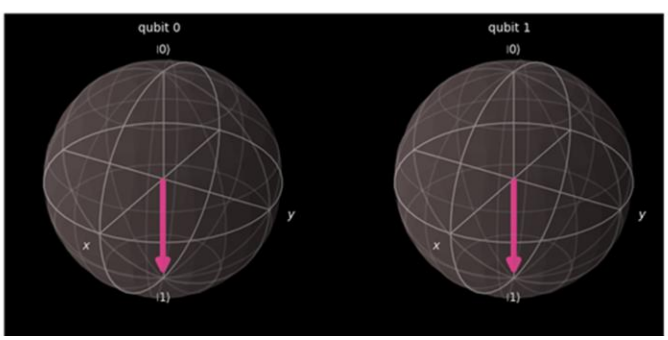

Fig.12: Bloch sphere of Bell state

Quantum teleportation is a process by which the quantum state of one particle can be transmitted to another particle, effectively "teleporting" the information. This process relies on the principles of quantum entanglement and is a key concept in quantum information theory.

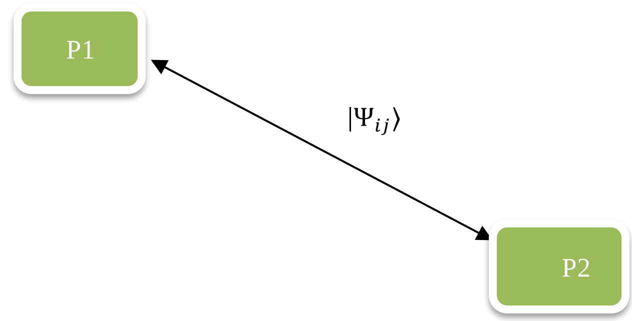

Fig.13. Quantum Communication Scenario between P1 and P2

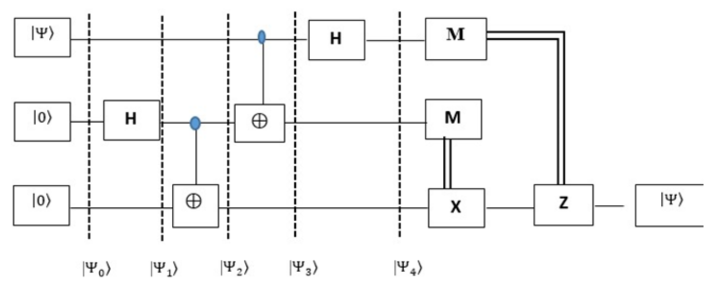

Fig.14: Creation of quantum states using tensor product operations and superpositions

The following calculation involves the creation of quantum states through superposition and tensor product operations, with the application of Hadamard gates to generate superpositions. The final state is represented as a combination of tensor products of individual qubits in superposition states.

$|\Psi_0\rangle = |\Psi\rangle \oplus |\Psi_{00}\rangle$s
$= \alpha|0\rangle + \beta|1\rangle|\Psi_{00}\rangle$

$= \alpha|0\rangle + \beta|1\rangle(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) * |0\rangle$

$|\Psi_1\rangle = \alpha|0\rangle + \beta|1\rangle\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$|\Psi_2\rangle = \alpha|0\rangle(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) + \beta|1\rangle(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))$

$|\Psi_3\rangle = \alpha|0\rangle(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) + \beta|1\rangle(\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle))$

$|\Psi_3\rangle = \alpha|\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) + \beta|\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)(\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle))$

$|\Psi_4\rangle = \frac{1}{2}(\ \alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |101\rangle - |101\rangle)$

$= \frac{1}{2}(\ |00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)$

Table 2: Entangle state change

Classical message	Gates to apply
$\mathbf{x^0z^0}$	Do nothing
$\boldsymbol{x^0z^1}$	Bit flip
$\boldsymbol{x^1z^0}$	Phase flip
$\boldsymbol{x^1z^1}$	Bit and phase flip

IV. Research Areas in Quantum Computing

A. *Cryptography*

- Breaking Classical Cryptography: Quantum computers threaten the security of widely-used classical cryptographic algorithms like RSA and ECC by efficiently factoring large numbers using Shor's algorithm [32], [33], [34].
- Quantum Key Distribution (QKD): QKD utilizes quantum properties for secure communication. It leverages the principles of superposition and entanglement to detect any potential eavesdropping attempts, providing a theoretically secure method for key exchange.

B. *Optimization problem*

- Route Optimization: Quantum computing excels in solving complex optimization problems in logistics and transportation. It can efficiently explore multiple routes simultaneously, leading to more optimal solutions for route planning.
- Supply Chain Management: Quantum algorithms can optimize supply chain operations, minimizing costs and enhancing overall efficiency in areas like inventory management and distribution.

C. *Drug Discovery and material science*

- Molecular Simulations: Quantum computers can simulate molecular interactions with unprecedented detail, accelerating drug discovery by analyzing the behavior of molecules and predicting their properties.
- Material Design: Quantum simulations aid in designing new materials with desired properties, impacting fields like nanotechnology and materials science.

D. *Machine learning and AI*

- Quantum Machine Learning: Quantum algorithms, such as quantum support vector machines and quantum neural networks, can enhance machine learning tasks, offering potential speedups in pattern recognition, classification, and optimization problems [35], [36], [37].

E. *Finance and portfolio Optimization*

- Financial Modeling: Quantum computing can contribute to more accurate financial modeling, enabling faster risk assessments and improving algorithmic trading strategies.
- Portfolio Optimization: Quantum algorithms can efficiently handle the complexity of portfolio optimization, assisting in better investment decision-making.

V. Conclusions

This report aimed to offer a comprehensive overview for beginners, unraveling the fundamental principles that distinguish quantum computing from classical computing.

We delved into the principles of superposition, entanglement, and quantum bits (qubits), highlighting their significance in exponentially expanding computational possibilities. Additionally, we explored the promising concept of quantum parallelism and its potential to revolutionize problem-solving in various fields, from cryptography to optimization. Ongoing research and development hold the promise of overcoming existing challenges and unlocking unprecedented computational power. As we navigate through this quantum landscape, it is essential for beginners to grasp the foundational concepts and appreciate the potential paradigm shift in computing that quantum technologies may bring.

The journey into quantum computing opens the door to information processing, challenges our understanding of classical limits and offering exciting possibilities. As technology advances, continued exploration and collaboration will be crucial in harnessing the full potential of quantum computing for the benefit of science, industry, and society as a whole.

References

[1] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J. M. Leimeister, "Quantum computing," *Electronic Markets*, vol. 32, no. 4, 2022, doi: 10.1007/s12525-022-00570-y.

[2] M. Bharti and T. Garg, "Quantum Computing," in *Wireless Communication Security*, 2023. doi: 10.1002/9781119777465.ch4.

[3] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing

ecosystem," *IET Quantum Communication*, vol. 1, no. 1, 2020, doi: 10.1049/iet-qtc.2020.0002.

[4] T. Li and Z. Q. Yin, "Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator," *Sci Bull (Beijing)*, vol. 61, no. 2, 2016, doi: 10.1007/s11434-015-0990-x.

[5] X. You *et al.*, "Quantum interference with independent single-photon sources over 300 km fiber," *Advanced Photonics*, vol. 4, no. 6, 2022, doi: 10.1117/1.AP.4.6.066003.

[6] M. Niknam *et al.*, "Quantum control of spin qubits using nanomagnets," *Commun Phys*, vol. 5, no. 1, 2022, doi: 10.1038/s42005-022-01041-8.

[7] Y. Chu *et al.*, "Quantum acoustics with superconducting qubits," *Science (1979)*, vol. 358, no. 6360, 2017, doi: 10.1126/science.aao1511.

[8] B. M. Terhal, "Detecting quantum entanglement," *Theor Comput Sci*, vol. 287, no. 1, 2002, doi: 10.1016/S0304-3975(02)00139-1.

[9] J. Mahecha-Gómez and H. Vinck-Posada, "IMPORTANCE OF QUANTUM ENTANGLEMENT," *Momento*, vol. 2023, no. 66. 2023. doi: 10.15446/mo.n66.106560.

[10] D. N. Makarov, "Quantum entanglement of photons on free electrons," *Results Phys*, vol. 49, 2023, doi: 10.1016/j.rinp.2023.106515.

[11] P. De, S. Ranwa, and S. Mukhopadhyay, "Intensity and phase encoding for realization of integrated Pauli X, Y and Z gates using 2D photonic crystal," *Opt Laser Technol*, vol. 152, 2022, doi: 10.1016/j.optlastec.2022.108141.

[12] P. Rakyta and Z. Zimborás, "Approaching the theoretical limit in quantum gate decomposition," *Quantum*, vol. 6, 2022, doi: 10.22331/Q-2022-05-11-710.

[13] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," *Phys Rev Lett*, vol. 75, no. 25, 1995, doi: 10.1103/PhysRevLett.75.4714.

[14] V. Kasirajan, "The Quantum Superposition Principle and Bloch Sphere Representation," in *Fundamentals of Quantum Computing*, 2021. doi: 10.1007/978-3-030-63689-0_3.

[15] M. Bataille, "Quantum circuits of CNOT gates," *arXiv:2009.13247*, 2020.

[16] M. Bataille, "Quantum circuits of CNOT gates: optimization and entanglement," *Quantum Inf Process*, vol. 21, no. 7, 2022, doi: 10.1007/s11128-022-03577-8.

[17] S. Ru, Y. Wang, M. An, F. Wang, P. Zhang, and F. Li, "Realization of a deterministic quantum Toffoli gate with a single photon," *Phys Rev A (Coll Park)*, vol. 103, no. 2, 2021, doi: 10.1103/PhysRevA.103.022606.

[18] A. Khrennikov, "Roots of quantum computing supremacy: superposition, entanglement, or complementarity?," *European Physical Journal: Special Topics*, vol. 230, no. 4, 2021, doi: 10.1140/epjs/s11734-021-00061-9.

[19] T. M. Forcer, A. J. G. Hey, D. A. Ross, and P. G. R. Smith, "Superposition, entanglement and quantum computation," *Quantum Inf Comput*, vol. 2, no. 2, 2002, doi: 10.26421/qic2.2-1.

[20] O. Romero-Isart, "Coherent inflation for large quantum superpositions of levitated microspheres," *New J Phys*, vol. 19, no. 12, 2017, doi: 10.1088/1367-2630/aa99bf.

[21] J. Carmesin and J. Kurkofka, "Entanglements," *Journal of Combinatorial Theory. Series B*, vol. 164, 2024, doi: 10.1016/j.jctb.2023.08.007.

[22] O. Gühne and G. Tóth, "Entanglement detection," *Physics Reports*, vol. 474, no. 1–6. 2009. doi: 10.1016/j.physrep.2009.02.004.

[23] X. M. Hu, Y. Guo, B. H. Liu, C. F. Li, and G. C. Guo, "Progress in quantum teleportation," *Nature Reviews Physics*, vol. 5, no. 6. 2023. doi: 10.1038/s42254-023-00588-x.

[24] J. Su, Y. Liu, and T. Hu, "Quess operations at chinese space science mission center," in *15th International Conference on Space Operations, 2018*, 2018. doi: 10.2514/6.2018-2329.

[25] D. Cavalcanti, P. Skrzypczyk, and I. Šupić, "All Entangled States can Demonstrate Nonclassical Teleportation," *Phys Rev Lett*, vol. 119, no. 11, 2017, doi: 10.1103/PhysRevLett.119.110501.

[26] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, "Long Distance Quantum Teleportation in a Quantum Relay Configuration," *Phys Rev Lett*, vol. 92, no. 4, 2004, doi: 10.1103/PhysRevLett.92.047904.

[27] H. Weinfurter, "From EPR to quantum computing: Experiments on entangled quantum systems," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 38, no. 9, 2005, doi: 10.1088/0953-4075/38/9/009.

[28] C. M. Li, K. Chen, Y. N. Chen, Q. Zhang, Y. A. Chen, and J. W. Pan, "Genuine High-Order Einstein-Podolsky-Rosen Steering," *Phys Rev Lett*, vol. 115, no. 1, 2015, doi: 10.1103/PhysRevLett.115.010402.

[29] L. Zhang, Z. Li, D. Liu, C. Wu, H. Xu, and Z. Li, "Entangled X-Ray Photon Pair Generation by Free-Electron Lasers," *Phys Rev Lett*, vol. 131, no. 7, 2023, doi: 10.1103/PhysRevLett.131.073601.

[30] T. J. Steiner *et al.*, "Ultrabright Entangled-Photon-Pair Generation from an AlGaAs -On-Insulator Microring Resonator," *PRX Quantum*, vol. 2, no. 1, 2021, doi: 10.1103/PRXQuantum.2.010337.

[31] R. J. Liu, M. Q. Bai, F. Wu, and Y. C. Zhang, "Cyclic-controlled quantum operation teleportation in noisy environment," *International Journal of Quantum Information*, vol. 17, no. 7, 2019, doi: 10.1142/S0219749919500527.

[32] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *International Journal of Advanced*

Computer Science and Applications, vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090354.
[33] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2968985.
[34] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Network Security*, vol. 2020, no. 9, 2020, doi: 10.1016/S1353-4858(20)30105-7.
[35] L. Alchieri, D. Badalotti, P. Bonardi, and S. Bianco, "An introduction to quantum machine learning: from quantum logic to quantum deep learning," *Quantum Machine Intelligence*, vol. 3, no. 2. 2021. doi: 10.1007/s42484-021-00056-8.
[36] N. Mishra *et al.*, "Quantum Machine Learning: A Review and Current Status," in *Advances in Intelligent Systems and Computing*, 2021. doi: 10.1007/978-981-15-5619-7_8.
[37] S. S. Gill *et al.*, "Quantum computing: A taxonomy, systematic review and future directions," *Softw Pract Exp*, vol. 52, no. 1, 2022, doi: 10.1002/spe.3039.