Quantum Computing

Dr.Pilli Emmanuel Shubhakar
(Associate Professor)

Department of Computer Science and Engineering
Malaviya National Institute of Technology, Jaipur

December,2023

Table of Contents

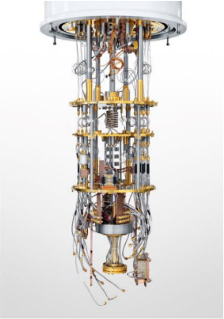
Classical Computers

- Binary System: Classical computers use bits as the basic unit of information, which can exist in one of two states: 0 or 1. These bits process information using classical computation principles.
- Algorithms: Classical computers use classical algorithms, which are step-by-step procedures or formulas for solving specific problems.
- Parallelism: Classical computers rely on parallelism at a higher level, where multiple processors or cores work on different tasks simultaneously.
- Limitations: Classical computers face limitations in solving certain complex problems efficiently, such as factoring large numbers or simulating quantum systems.

Quantum Computers

A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.

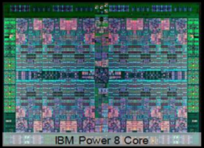
- It computes faster than High performance classical super computers.
- A classical HPC with GHz capacity will take about 317 trillion years to break a 2048 bit RSA key. On other hand a quantum computer of MHz capacity can do the same in 10 Seconds.



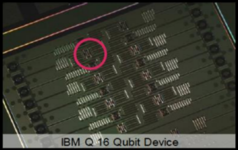
Quantum Computers

The power of Quantum Computing

Classical Computers	Quantum Computers
One-to-one relationship between number of transistors and processing power	Rough equivalent of a transistor is a quantum bit, or a qubit
Potential power doubles when you double the number of transistors	Potential power doubles when you add one additional qubit



$\sim N$



$\sim 2^N$

Quantum Computers

- Qubits: Quantum computers use quantum bits or qubits, which can exist in multiple states simultaneously due to the principles of superposition. This allows quantum computers to perform multiple calculations in parallel.
- Superposition and Entanglement: Superposition enables qubits to exist in multiple states at once, and entanglement allows the state of one qubit to be correlated with the state of another, even if they are physically separated.
- Quantum Speed Limit: Quantum computers are not universally faster than classical computers. Quantum speedup depends on the specific problem and the efficiency of the quantum algorithm.
- Quantum Complexity: Quantum computers are particularly promising for solving certain complex problems, such as integer factorization (Shor's algorithm), optimization problems, and simulating quantum systems.
- Quantum Speedup : Quantum computers have the potential to provide significant speedup for certain types of problems, such as optimization, cryptography, and simulations of quantum systems.
- Challenges: Building and maintaining stable qubits is a significant challenge due to quantum decoherence. Error correction in quantum computers is an active area of research.

Classical Logic

- Binary System: Classical logic is based on the binary system, where information is represented using bits, which can exist in one of two states: 0 or 1. Classical computers process information using classical logic gates that manipulate bits.
- Deterministic: Classical logic is deterministic, meaning that the outcome of any logical operation can be precisely predicted. Each operation follows strict rules, and the result is unambiguous.
- Law of Excluded Middle: Classical logic adheres to the law of excluded middle, stating that a proposition is either true or false. There is no middle ground, and every statement must be assigned one of the two truth values.
- Boolean Algebra: Classical logic is closely related to Boolean algebra, which deals with logical operations such as AND, OR, and NOT. These operations are fundamental building blocks for constructing logical circuits in classical computers.
- Classical Algorithms: Classical algorithms, such as those used in classical computing, are based on classical logic. These algorithms follow step-by-step procedures and are deterministic in nature.
- Classical Circuit: No restrictions exist on copying or measuring signals and well-developed CAD methodologies exist for implementing circuits with fast, scalable, and macroscopic technologies such as CMOS

Quantum Logic

- Probabilistic Nature: Quantum logic is inherently probabilistic. When measured, a quantum system collapses to one of its possible states with probabilities determined by the squared magnitudes of the probability amplitudes.
- Quantum Gates: Quantum logic gates manipulate qubits and are designed to take advantage of quantum superposition and entanglement. Examples include the Hadamard gate, CNOT gate, and others used in quantum algorithms.
- Quantum Algorithms: Quantum algorithms, such as Shor's algorithm and Grover's algorithm, are designed to solve certain problems exponentially faster than the best-known classical algorithms. They leverage the unique features of quantum logic to achieve this speedup.
- Quantum Measurement: Measurement in quantum logic is different from classical measurement. It involves a probabilistic collapse of the quantum state, and the measurement outcome is not known with certainty until the measurement is performed.
- Quantum Circuits: Operations are defined by linear algebra over Hilbert Space and can be represented by unitary matrices with complex elements. Also, severe restrictions exist on copying and measuring signals. Many universal gate sets exist but the best types are not obvious. Circuits must use microscopic technologies that are slow, fragile, and not yet scalable, e.g., NMR

Superposition

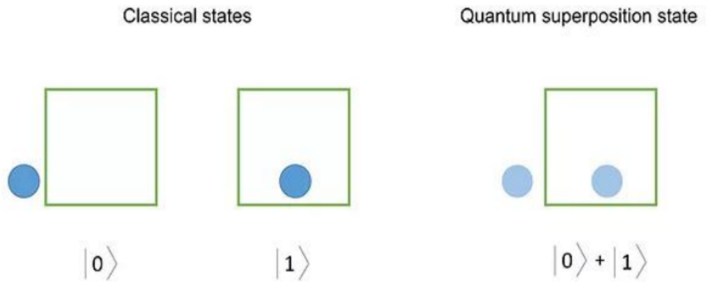
Superposition is a fundamental principle in quantum mechanics that allows quantum systems to exist in multiple states simultaneously. This concept is particularly important in the context of quantum computing, where qubits take advantage of superposition to perform parallel computations.

- In quantum computing, a qubit can exist in a superposition of states. This means that before measured, a qubit can be in a combination of the 0 state, the 1 state, or any linear combination of both. Mathematically, this is represented as $\alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers representing the probability amplitudes of each state.
- Probability Amplitudes: The probability amplitudes (α and β) determine the likelihood of measuring the qubit in the 0 state or the 1 state. The square of the absolute value of these amplitudes gives the probability of finding the qubit in a particular state upon measurement. The unique aspect of quantum superposition is that these probability amplitudes allow for interference effects. This interference is a result of the phases of the complex probability amplitudes, leading to constructive or destructive interference.

Superposition

- Constructive and Destructive Interference: Constructive interference occurs when the probability amplitudes add up, increasing the likelihood of measuring the qubit in a particular state. Destructive interference occurs when the probability amplitudes partially or completely cancel each other out, reducing the likelihood of measuring the qubit in a specific state.
- Quantum Parallelism: Superposition enables quantum parallelism. While classical computers perform calculations sequentially, a quantum computer with qubits in superposition can explore multiple possibilities simultaneously. This parallelism is a key factor in the potential speedup of certain quantum algorithms. For example, in a quantum search algorithm like Grover's algorithm, superposition allows the quantum computer to search through a large database of possibilities in parallel, offering a quadratic speedup over classical algorithms.
- Measurement and Collapse: When a qubit in superposition is measured, it "collapses" into one of its basis states (0 or 1), and the outcome is determined probabilistically based on the squared magnitudes of the probability amplitudes. After measurement, the qubit remains in the state in which it was measured. The act of measurement extracts information from the superposition, leading to the loss of the quantum parallelism.

Superposition



Entanglement

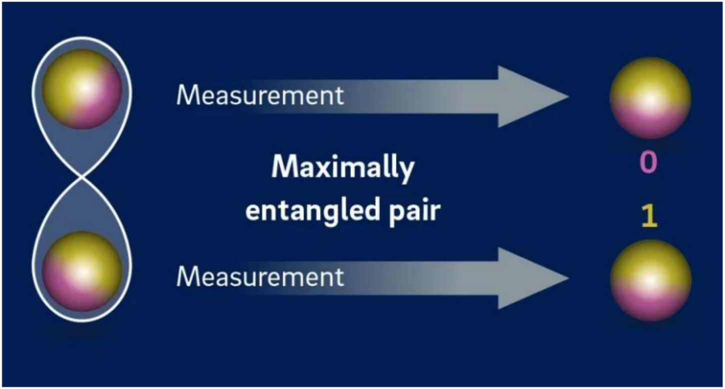
Entanglement describes a strong correlation between quantum particles, such that the state of one particle is directly related to the state of another, regardless of the distance between them. Entanglement is a crucial feature of quantum systems and plays a central role in quantum computing and quantum communication.

- Entangled States: Entanglement arises when two or more quantum particles, such as electrons, photons, or atoms, become correlated in a way that the state of one particle cannot be described independently of the state of the others. The particles are described by an entangled state, which is a quantum superposition of possible states for the entire system.
- Bell States: The most well-known examples of entangled states are the Bell states, which are specific quantum states of two qubits. The four Bell states are maximally entangled and exhibit properties that cannot be explained by classical physics. One example of a Bell state is: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Non-Locality: Even if entangled particles are separated by large distances, the measurement of one particle instantly influences the state of the other, violating the classical concept of locality.

Entanglement

- Quantum Measurement: Entanglement becomes evident when measurements are made on one of the entangled particles. The act of measuring the state of one particle instantaneously determines the state of the other particle, regardless of the spatial separation between them. The outcomes of measurements on entangled particles are correlated in a way that cannot be explained by classical physics.
- Applications in Quantum Computing: In quantum computing, entanglement is harnessed to perform certain quantum algorithms and computations more efficiently. Quantum gates can entangle qubits, creating entangled states that enable quantum parallelism and facilitate the execution of quantum algorithms such as quantum teleportation and quantum error correction.
- Quantum Entanglement in Quantum Cryptography: Quantum entanglement is also utilized in quantum key distribution (QKD) protocols, a form of quantum cryptography. Entangled particles can be used to create secure cryptographic keys, as any attempt to eavesdrop on the quantum communication would disturb the entanglement, revealing the presence of an eavesdropper.

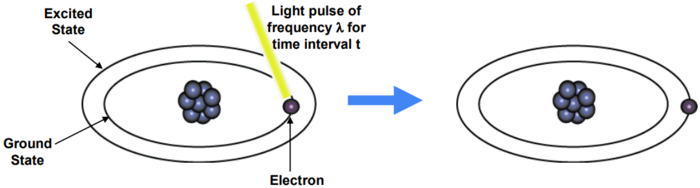
Entanglement



Qubit (Quantum Bit)

- Qubit: A classical bit is the basic unit of classical information and can exist in one of two states: 0 or 1. In contrast, a qubit is the basic unit of quantum information and can exist in a superposition of states, representing both 0 and 1 simultaneously.
- Quantum States: A qubit can be described by a quantum state vector. In a standard basis, a qubit's state can be represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers and $|0\rangle$ and $|1\rangle$ are the basis states.
- Quantum Gates: Quantum gates are operations that manipulate the state of qubits. They can perform transformations like rotations on the Bloch sphere. Common gates include the Hadamard gate, Pauli-X, Pauli-Y, and Pauli-Z gates.
- Measurement: When a qubit is measured, it collapses to one of the basis states. The probability of measuring $|0\rangle$ is α^2 and $|1\rangle$ is β^2 .

Qubit



Excited State
Light pulse of frequency λ for time interval t
Ground State
Electron

Superposed Qubit

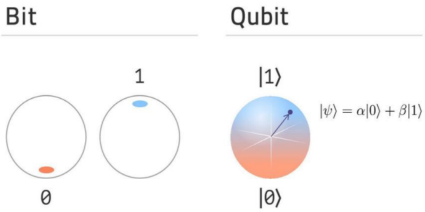
- Superposition in Qubits: A superposed qubit is a qubit that exists in a superposition of states. In the context of a single qubit, it means that the qubit is in a linear combination of $|0\rangle$ and $|1\rangle$.
- Interference: The probability amplitudes α and β can interfere constructively or destructively when combining different quantum states. This interference is a unique quantum phenomenon and contributes to the power of quantum computation.
- Applications: Superposed qubits are fundamental to the functioning of quantum computers. They are harnessed in quantum algorithms like Shor's algorithm and Grover's algorithm to achieve exponential speedup in certain computational tasks.

Superposed Qubit

A single qubit can be forced into a ***superposition*** of the two states denoted by the addition of the state vectors:

$$|\psi\rangle = \alpha_1 |0\rangle + \alpha_2 |1\rangle$$

Where α_1 **and** α_2 are complex numbers and $|\alpha_1| + |\alpha_2| = 1$



A qubit in superposition is in both of the states |1> and |0 at the same time

Dirac Notation

Dirac notation, also known as bra-ket notation, is a mathematical notation used in quantum mechanics to describe the states of quantum systems. It was introduced by the physicist Paul Dirac and has become a standard and concise way to represent quantum states, operators, and other quantities. The notation uses "bras" and "kets," which are denoted by angle brackets.

- The Dirac notation or the bra-ket notation is used to describe quantum states using angular brackets $\langle$ and $\rangle$ and a vertical bar $|$ to construct "bras" and "kets".
- A ket looks like $|a\rangle$. Mathematically it denotes a vector v, in an abstract (complex) vector space V, and physically it represents a state of some quantum system.
- A bra looks like $\langle b|$, and mathematically it denotes a linear form $b : \mathbf{V} \to \mathbf{C}$, i.e., a linear map that maps each vector in **V** to a number in the complex plane **C**.

Dirac Notation

- Eg: $a, b \in \mathbb{C}^2$
  - **Ket:**
    $$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$
  - **Bra-ket:**
    $$\langle b|a\rangle = (b_1{}^* \quad b_2{}^*) \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$
    $$= b_1{}^* a_1 + b_2{}^* a_2$$
    $$= \langle b|a\rangle^* \in \mathbb{C}^2$$
  - **Bra:**
    $$\langle b| = |b\rangle^\dagger$$
    $$= \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}^\dagger = (b_1{}^* \quad b_2{}^*)$$
    Suppose, $x = c + id$, then $x^* = c - id$, where $c, d \in \mathbb{R}$)
  - **Ket-bra:**
    $$|a\rangle\langle b| = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \cdot (b_1{}^* \quad b_2{}^*)$$
    $$= \begin{pmatrix} a_1 b_1{}^* & a_1 b_2{}^* \\ a_2 b_1{}^* & a_2 b_2{}^* \end{pmatrix}$$

Dirac Notation

- We define the pure states $|\mathbf{0}\rangle = \begin{pmatrix}\mathbf{1}\\ \mathbf{0}\end{pmatrix}$ and $|\mathbf{1}\rangle = \begin{pmatrix}\mathbf{0}\\ \mathbf{1}\end{pmatrix}$, which are orthogonal (inner product of two states will be equal to zero).

$$\langle \mathbf{0}|\mathbf{1}\rangle = (\mathbf{1} \quad \mathbf{0})\begin{pmatrix}\mathbf{0}\\ \mathbf{1}\end{pmatrix} = (\mathbf{1}\times\mathbf{0}) + (\mathbf{0}\times\mathbf{1}) = \mathbf{0}$$

- All quantum states are **normalized** i.e., $\langle \boldsymbol{\Psi}|\boldsymbol{\Psi}\rangle = \mathbf{1}$. For instance:

$$|\boldsymbol{\Psi}\rangle = (|\mathbf{0}\rangle + |\mathbf{1}\rangle) = \begin{pmatrix}\mathbf{1}\\ \mathbf{0}\end{pmatrix} + \begin{pmatrix}\mathbf{0}\\ \mathbf{1}\end{pmatrix} = \begin{pmatrix}\mathbf{1}\\ \mathbf{1}\end{pmatrix}$$

$$\therefore \langle \boldsymbol{\Psi}|\boldsymbol{\Psi}\rangle = (\mathbf{1} \quad \mathbf{1})\begin{pmatrix}\mathbf{1}\\ \mathbf{1}\end{pmatrix} = (\mathbf{1}\times\mathbf{1}) + (\mathbf{1}\times\mathbf{1}) = \mathbf{2}$$

$$\therefore |\boldsymbol{\Psi}\rangle\ \boldsymbol{is\ NOT\ normalized}$$

Hilbert Spaces

In mathematics, Hilbert spaces allow generalizing the methods of linear algebra and calculus from the two-dimensional and three-dimensional Euclidean spaces to spaces that may have an infinite dimension.

- A Hilbert space is a vector space equipped with an inner product operation, which allows defining a distance function and perpendicularity (known as orthogonality in this context).
- Hilbert spaces are complete for this distance, which means that there are enough limits in the space to allow the techniques of calculus to be used.
- Hilbert space can finally be defined as a complex multi-dimensional space where the inner product of any pair of elements is defined, i.e.
- Extrapolation of a 2D space to n-dimensions and complex coefficients.
- The state of a quantum system is defined by a unit vector in a complex, inner product space, more generally known as the Hilbert space.

Hilbert Spaces

Inner product:

- Say, $\boldsymbol{V}$ is a complex vector space.

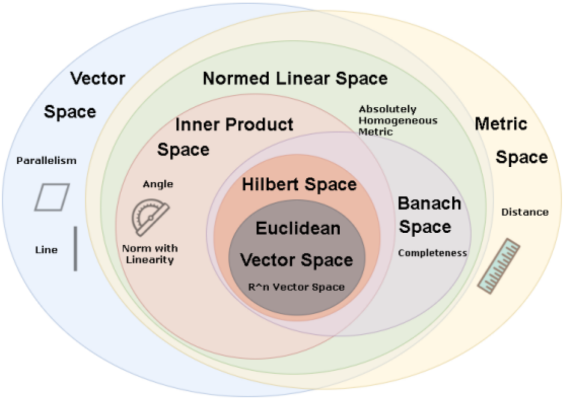
- $(\boldsymbol{v_1} \cdot \boldsymbol{v_2}): V \times V \to \mathbb{C}$ is called an inner product on V if:
  - ✓ $(\boldsymbol{x} \cdot)$ is linear for $\boldsymbol{x} \in \boldsymbol{V}$
  - ✓ $(\boldsymbol{x} \cdot \boldsymbol{y}) = \overline{(\boldsymbol{y} \cdot \boldsymbol{x})}\ \forall\, \boldsymbol{x} \in \boldsymbol{V}$

Inner product space:

- $(\cdot)$ is an inner product on $\boldsymbol{V}$ is called inner product space. If we write $\|x\| = \sqrt{(x \cdot x)}$, then$\|\cdot\|$ is a norm on $\boldsymbol{V}$.

- Hence, $\boldsymbol{V}$ is a normed vector space.

Hilbert Spaces



Bloch Sphere

The Bloch sphere is a geometric representation used in quantum mechanics to visualize the state space of a single qubit. Named after the physicist Felix Bloch, this sphere provides an intuitive way to understand the quantum states of a qubit and their evolution under certain quantum operations

- Bloch Sphere Construction: The Bloch sphere is a unit sphere, and the Bloch vector is located on its surface. The probabilities of measuring $|0\rangle$ and $|1\rangle$ are given by the lengths of the projections of the Bloch vector onto the poles. The equator of the sphere represents equal superpositions, and points inside the sphere represent states with complex probability amplitudes.
- Pure States and Mixed States: Pure quantum states, such as ψ, are represented by points on the surface of the Bloch sphere. Mixed states, which are statistical ensembles of pure states, are represented by density matrices and correspond to points inside the sphere.

Bloch Sphere

- Measurement Outcomes: When a qubit is measured, the Bloch vector collapses to one of the poles, representing the outcome of the measurement.
- Quantum operations: Operations such as rotations and gates, are represented as rotations of the Bloch vector. Unitary operations correspond to rotations around the Bloch vector, and non-unitary operations, such as measurements, may cause a collapse of the Bloch vector to one of the poles.
- Quantum Gates: Perform transformations on qubits, which are visualized as rotations on the Bloch sphere. For example, the Hadamard gate corresponds to a rotation of the Bloch vector about the equator.
- Visualization of Quantum States: The Bloch sphere provides an intuitive way to visualize the evolution of quantum states and the effects of quantum operations. It is particularly useful for understanding the behavior of single qubits.

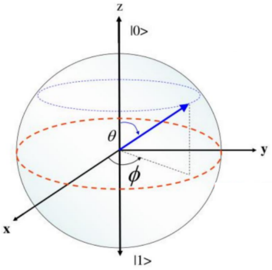
Bloch Sphere

- Consider one qubit with energy eigenstates $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$.
- We will need to be able to put it into superposition states:

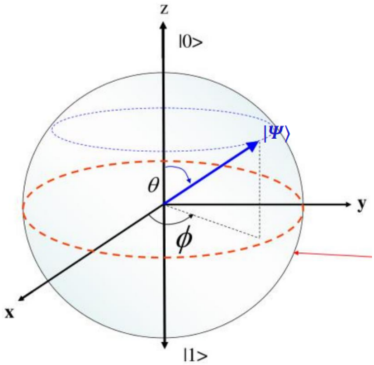
$$|\boldsymbol{\Psi}\rangle = \boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle$$

  - Probability amplitudes $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ can be complex numbers.
  - State must be normalized to unity so $|\alpha|^2 + |\beta|^2 = 1$.
  - An overall phase factor has no effect, so we can choose $\boldsymbol{\alpha}$ to be real.
  - Then define: $\boldsymbol{\alpha} = \cos\left(\frac{\theta}{2}\right)$ and $\boldsymbol{\beta} = \boldsymbol{e}^{i\phi}\sin\left(\frac{\theta}{2}\right)$
    - ✓ $|\boldsymbol{\alpha}|^2 + |\boldsymbol{\beta}|^2 = \left|\cos\left(\frac{\theta}{2}\right)\right|^2 + \left|\boldsymbol{e}^{i\phi}\sin\left(\frac{\theta}{2}\right)\right|^2 = cos^2\left(\frac{\theta}{2}\right) + sin^2\left(\frac{\theta}{2}\right) = \mathbf{1}$
    - ✓ Can always write a superposition state in the form:

$$|\boldsymbol{\Psi}\rangle = \boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle = \cos\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)|\mathbf{0}\rangle + \boldsymbol{e}^{i\phi}\sin\left(\frac{\boldsymbol{\theta}}{\mathbf{2}}\right)|\mathbf{1}\rangle$$



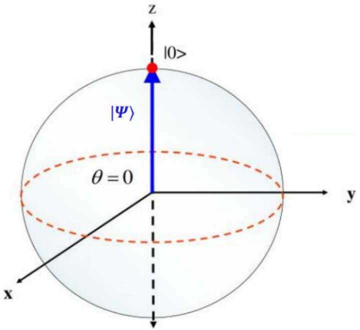
Bloch Sphere



$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

- The sphere with radius of unit length is called the **Bloch Sphere**.
- Wave function $|\Psi\rangle$ being depicted on it.

Bloch Sphere



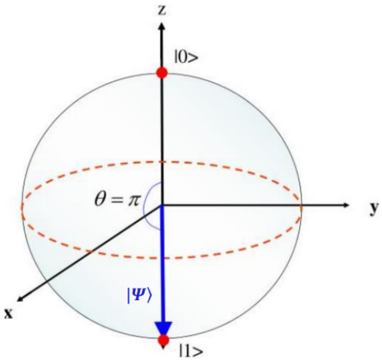
Example: $\boldsymbol{\theta = 0}$

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$= \cos\left(\frac{0}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{0}{2}\right)|1\rangle$$

$$= |0\rangle$$

Bloch Sphere



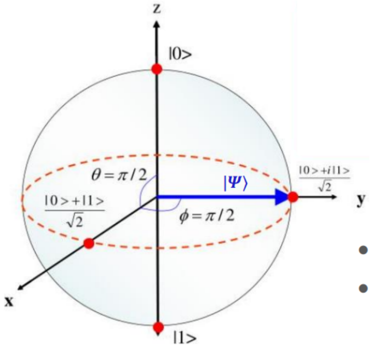
Example: $\theta = \pi, \phi = 0$

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i0}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$= |1\rangle$$

Bloch Sphere



- There are an infinite number of states on Bloch sphere, but we can choose a "digital" subset for computing:

$$\Psi_0 = |0\rangle \qquad \Psi_1 = |1\rangle$$

$$\Psi_X = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \Psi_{-X} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$\Psi_Y = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \qquad \Psi_{-Y} = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

- Note: One classical bit 2^1 possible states (0 and 1).
- One of these qubits has of order $\sim 2^{2^1}$ accessible states.

Quantum Gates

Quantum gates are fundamental building blocks of quantum circuits, the analogs of classical logic gates in quantum computation. These gates manipulate quantum bits, or qubits, using the principles of quantum mechanics. Here are some commonly used quantum gates and their functions:

- Hadamard Gate (H): Creates a superposition of the $|0\rangle$ and $|1\rangle$ states.
- Pauli X Gate (X): Performs a classical NOT operation, flipping the $|0\rangle$ state to $|1\rangle$ and vice versa.
- Pauli Y Gate (Y): Similar to the Pauli X gate with a phase flip.
- Pauli Z Gate (Z): Introduces a phase flip without changing the basis states.
- CNOT Gate (Controlled-X or CX): Performs a NOT operation on the target qubit if the control qubit is in state $|1\rangle$.
- SWAP Gate: Swaps the states of two qubits.
- Toffoli Gate (CCX): A controlled-controlled-X gate, performing a NOT operation on the target qubit if both control qubits are in state $|1\rangle$.

GATES WITHOUT SUPERPOSITION

- All classical input-consuming reversible gates can be represented as unitary transformations!
- *E.g.*, input-consuming NOT gate (inverter)

in	out
0	1
1	0

$$|0\rangle :\equiv \begin{array}{cc} \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \end{array} \qquad |1\rangle :\equiv \begin{array}{cc} \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \end{array}$$

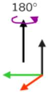
$$N :\equiv \begin{array}{cc} \begin{array}{cc} 0 & 1 \end{array} & \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \end{array}$$

$$N|0\rangle = |1\rangle$$

$$N|1\rangle = |0\rangle$$

SINGLE QUBIT GATE

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S^2$$



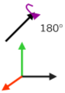
Phase flip

$$|a\rangle \; -\boxed{Z}- \; (-1)^a |a\rangle$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2$$

$$|a\rangle \; -\boxed{S}- \; i^a |a\rangle$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Hadamard

$$|a\rangle \; -\boxed{H}- \; (|0\rangle + (-1)^a |1\rangle)/\sqrt{2}$$

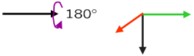
$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$|a\rangle \; -\boxed{T}- \; e^{ia\pi/4} |a\rangle$$

Quantum Gates

SINGLE QUBIT GATE

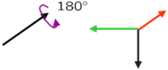
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = HZH$$



Bit flip

$$|a\rangle \; -\!\boxed{X}\!- \; |a \oplus 1\rangle \quad = \quad -\!\boxed{H}\!-\!\boxed{Z}\!-\!\boxed{H}\!- \qquad X^2 = Y^2 = I$$

$$iY = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = ZX$$



Phase-bit flip

$$|a\rangle \; -\!\boxed{iY}\!- \; (-1)^{a+1}|a \oplus 1\rangle$$

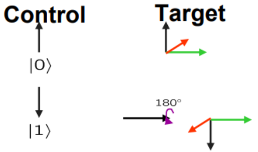
$$= \; -\!\boxed{X}\!-\!\boxed{Z}\!- \quad = \quad -\!\boxed{H}\!-\!\boxed{Z}\!-\!\boxed{H}\!-\!\boxed{Z}\!-$$

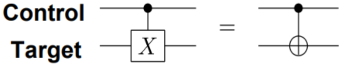
Quantum Gates

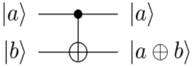
CNOT GATE

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$







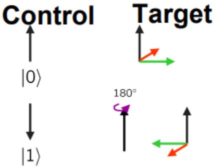
$$(\text{C-NOT})^2 = I$$

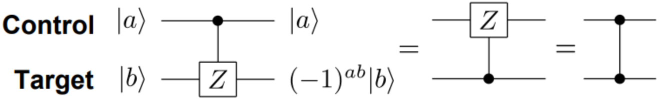
Quantum Gates

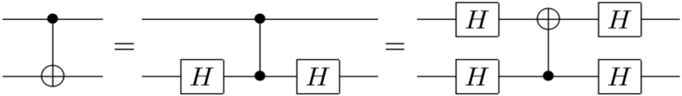
C-PHASE GATE

$$\text{C-PHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

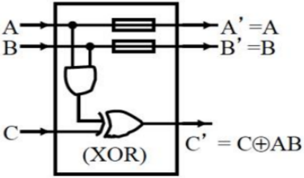


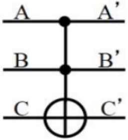




Quantum Gates

TOFFOLI GATE (CCNOT)





A	B	C		A'	B'	C'
0	0	0	→	0	0	0
0	0	1	→	0	0	1
0	1	0	→	0	1	0
0	1	1	→	0	1	1
1	0	0	→	1	0	0
1	0	1	→	1	0	1
1	1	0		1	1	0
1	1	1		1	1	1

$$X := \begin{array}{c} \begin{array}{cccccccc} \scriptstyle 000 & \scriptstyle 001 & \scriptstyle 010 & \scriptstyle 011 & \scriptstyle 100 & \scriptstyle 101 & \scriptstyle 110 & \scriptstyle 111 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array} \begin{array}{c} \scriptstyle 000 \\ \scriptstyle 001 \\ \scriptstyle 010 \\ \scriptstyle 011 \\ \scriptstyle 100 \\ \scriptstyle 101 \\ \scriptstyle 110 \\ \scriptstyle 111 \end{array}$$

Now, what happens if the unitary matrix elements are *not* always 0 or 1?

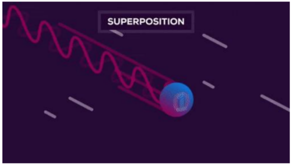
Quantum Gates

THE HADAMARD TRANSFORM

- A randomizing "square root of identity" gate.
- Used frequently in quantum logic networks.

$$H := \begin{array}{c c} & \begin{array}{cc} 0 & 1 \end{array} \\ & \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{array}{c} 0 \\ 1 \end{array} \end{array}$$

$$H^2 = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



THANK YOU