Advanced Engineering Physics

Unit 3: Quantum Computing

I. Introduction to Quantum Computing & Qubits

1. Concept of a Quantum Computer

Classical vs. Quantum Computing Models:

- **Classical Computing:** Traditional computers operate using the laws of classical physics. Their fundamental unit of information is the bit, their logic gates are sometimes reversible (but often irreversible), and their mathematical foundation relies on boolean algebra.
- **Quantum Computing:** Quantum computers operate using the laws of quantum physics. Their fundamental unit of information is the quantum bit (qubit). Unlike classical gates, quantum operations (unitary gates) are *always* reversible, and their mathematical foundation relies on linear algebra.

Complexity Classes: P vs. BQP & Computational Speedups:

- **P (Polynomial Time):** The complexity class encompassing all problems that can be efficiently solved by a classical computer (meaning the algorithm runs in polynomial time or faster).
- **BQP (Bounded-Error Quantum Polynomial-Time):** The complexity class of problems that can be efficiently solved by a quantum computer.
- **The Strong Church-Turing Thesis:** This thesis states that any model of computation can be simulated by a probabilistic classical computer with at most a polynomial overhead in time. Classical computing strongly supports this thesis. However, it is believed that quantum computers can efficiently solve certain problems that are hard for classical computers, thereby *violating* the Strong Church-Turing Thesis.
- **Theoretical Speedups:**
  - Because quantum computers can process certain algorithms with far fewer steps or queries than classical computers, they achieve notable speedups.
  - *Exponential Speedup:* Finding a secret XOR mask (Simon's algorithm) takes exponentially fewer queries on a quantum computer.
  - *Subexponential Speedup:* Factoring large prime numbers (Shor's algorithm) is believed to be intractable for classical computers but is efficiently solvable (in BQP) by a quantum computer, threatening modern RSA cryptography.
  - *Polynomial/Quadratic Speedup:* Brute-force searching an unstructured database of size N classically takes $O(N)$ queries, but Grover's algorithm

achieves this in $O(\sqrt{N})$ queries.

2. Classical Bits vs. Qubits

Core Definitions & Physical Implementation:

- **Classical Bits:** The smallest unit of classical information. A bit is deterministic and can only hold one of two distinct states: 0 or 1. Physically, they are represented by systems with two clear states, such as a coin (heads/tails), a switch (off/on), optical disc pits/lands, or distinct voltage levels (0 V / 5 V).
- **Qubits:** The fundamental unit of quantum information. Using Dirac (bra-ket) notation from quantum physics, the two foundational states of a qubit are written as the kets $|0\rangle$ and $|1\rangle$.
- **Physical Qubits:** Physically, any quantum system with two distinct states can serve as a qubit. Examples include the polarization states of photons, the energy levels of trapped ions or cold neutral atoms, the spin states in nuclear magnetic resonance or quantum dots, defect qubits (nitrogen-vacancy centers in diamonds), and superconducting circuits.

3. Superposition & The Bloch Sphere

The Principle of Superposition:

- **Core Concept:** While a classical bit is strictly 0 or 1, the laws of quantum mechanics allow a qubit to exist in a linear combination of both $|0\rangle$ and $|1\rangle$ simultaneously. This is called a **superposition**.
- **Mathematical Expression:** A generic qubit state $|\psi\rangle$ is written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

  where α and β are complex numbers known as *amplitudes*.
- **Measurement & Collapse:** A qubit cannot be directly read as a superposition. Upon measurement, the qubit "collapses" into a single definite value. The probability of measuring $|0\rangle$ is given by the norm-square of its amplitude, $|\alpha|^2$, and the probability of measuring $|1\rangle$ is $|\beta|^2$. For the state to be normalized (meaning the total probability equals 1), the amplitudes must satisfy $|\alpha|^2 + |\beta|^2 = 1$.

Examples of Superposition States:
If a qubit has amplitudes that are exactly equal in magnitude, it has a 50/50 chance of being measured as $|0\rangle$ or $|1\rangle$. By changing the relative phase of the amplitudes, we can construct uniquely different superposition states:

- **The $|+\rangle$ state:** $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- **The $|-\rangle$ state:** $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- **The $|i\rangle$ state:** $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
- **The $|-i\rangle$ state:** $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

The Bloch Sphere:

- **Visualization:** A qubit's state can be mapped geometrically as a point on the surface of a three-dimensional unit sphere known as the **Bloch sphere**.
- The pure states $|0\rangle$ and $|1\rangle$ are plotted at the North pole $(0, 0, 1)$ and South pole $(0, 0, -1)$, respectively.
- Equal superpositions (like $|+\rangle$, $|-\rangle$, $|i\rangle$, and $|-i\rangle$) are distributed entirely along the sphere's equator, halfway between the poles.

II. Mathematical Foundations for Quantum Computation

1. Linear Algebra for Quantum Computation

Core Concept:
While elementary algebra can be used to track quantum states, it becomes incredibly tedious for complex circuits. Instead, the mathematics of quantum computing is fundamentally built on **linear algebra**, where numbers are arranged in columns, rows, and tables called matrices.

- **States as Column Vectors:**
  - The fundamental states of a qubit are represented as column vectors of length 2.
  - $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
  - A generic superposition state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is written as the column vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.
- **Quantum Operations as Matrices:**
  - Quantum gates transform basis states into new superpositions. The resulting amplitudes can be arranged side-by-side to form a rectangular array of numbers called a **matrix**.
  - For example, if a gate U maps $|0\rangle$ $\begin{pmatrix} a \\ b \end{pmatrix}$ and $|1\rangle$ $\begin{pmatrix} c \\ d \end{pmatrix}$, the gate is represented by the 2×2 matrix $U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.
- **Unitary Matrices:**
  - To be a valid quantum gate, a matrix must preserve the total probability of the quantum state (meaning it must keep the sum of the norm-squared amplitudes equal to 1).
  - Mathematically, this requires the matrix to be **unitary**, which is defined by the property $U U =$, where U is the conjugate transpose and is the identity matrix.
  - Because $U U =$, every quantum gate is perfectly reversible, and its inverse is simply its conjugate transpose ($U^{-1} = U$).
- **Eigenvalues and Eigenvectors:**

- Typically, applying a matrix to a vector changes it into a different vector. However, for certain special vectors, applying a specific matrix results in the *exact same vector* simply multiplied by a scalar number.
- The special vector is called an **eigenvector** (or **eigenstate** in quantum systems), and the scalar multiplier is called the **eigenvalue**.
- *Example:* If we apply the Pauli-X gate to the $|+\rangle$ state, we get $X|+\rangle = |+\rangle$. Therefore, $|+\rangle$ is an eigenvector of X with an eigenvalue of 1.
- For unitary matrices, eigenvalues always take the form $e^{i\theta}$ for some real number θ (a phase).

2. Dirac's Bra and Ket Notation & Properties

To easily manipulate these linear algebra components, quantum mechanics utilizes Dirac's bra-ket notation.

- **Kets ($|\psi\rangle$):**
  - A **ket** represents a quantum state as a column vector.
- **Bras ($\langle\psi|$):**
  - A **bra** is a row vector representing the **conjugate transpose** of a ket.
  - *Step-by-step process:* To find the bra $\langle\psi|$, you take the ket $|\psi\rangle$, transpose it into a row, and take the complex conjugate of every amplitude.
  - If $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, then $\langle\psi| = (\alpha^*, \beta^*)$. Flipping between a ket and a bra is known as "taking the dual".
- **Inner Products (Bra-Kets):**
  - **Definition:** Multiplying a bra on the left and a ket on the right ($\langle\psi|\rangle$) is called an inner product. The result is always a **scalar** (a single complex number). It calculates the overlap or projection of one state onto another.
  - *Calculation:* To evaluate $\langle\psi|\rangle = (\alpha^*, \beta^*) \begin{pmatrix} \delta \end{pmatrix}$, you multiply the first entry of each vector, multiply the second entry of each vector, and add them together: $\alpha^* + \beta^*\delta$.
  - *Normalization:* If you take the inner product of a state with itself, you get the total probability: $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2$. If the state is normalized, this equals 1.
  - *Orthogonality:* If the inner product of two states is exactly zero (e.g., $\langle 0|1\rangle = 0$), the states are defined as **orthogonal**. Orthogonal states represent completely distinct measurement outcomes.
- **Outer Products:**
  - **Definition:** Multiplying a ket on the left and a bra on the right ($|\psi\rangle\langle|$) is called an outer product. Unlike inner products, the result of an outer product is a **matrix**.
  - *Calculation:* To evaluate $|\psi\rangle\langle|$, you multiply every row element of the ket by every column element of the bra.

$$|\psi\rangle\langle| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}(^*, \delta^*) = \begin{pmatrix}\alpha^* & \alpha\delta^*\beta^* & \beta\delta^*\end{pmatrix}$$

.

- *Creating Operators:* Outer products can be added together to construct quantum gates. For example, the Pauli-X gate can be constructed using outer products of the computational basis: $X = |1\rangle\langle 0| + |0\rangle\langle 1|$.

3. Hilbert Space

- **Core Concept:** The abstract, complex vector space where all of these bra and ket vectors reside and are manipulated is governed by the strict rules of linear algebra.
- **Completeness Relation:** A defining property of this space is that any valid quantum state can be fully expressed in terms of an orthonormal basis (e.g., $|0\rangle$ and $|1\rangle$, or $|+\rangle$ and $|-\rangle$).
- **Mathematical Expression:** If $|a\rangle, |b\rangle$ forms a complete orthonormal basis, the sum of their outer products with themselves will always equal the identity matrix :

$$|a\rangle\langle a| + |b\rangle\langle b| =$$

This relation guarantees the "completeness" of the space, meaning no quantum information is lost outside of these basis vectors.

III. Single Qubit Systems & Visualization

1. Bloch's Sphere: Geometric Representation of a Qubit

Core Definitions & Concepts:

- **The Bloch Sphere:** The Bloch sphere is a geometric visualization tool where any single qubit state is mapped as a point on the surface of a three-dimensional sphere with a radius of 1.
- **Coordinate System Convention:** Following standard physics conventions, the z-axis points straight up, the y-axis points to the side, and the x-axis points out of the page.
- **The Poles (Z-Basis):** The fundamental classical states are located at the poles. The state $|0\rangle$ corresponds to the north pole at Cartesian coordinates $(0, 0, 1)$, and the state $|1\rangle$ corresponds to the south pole at $(0, 0, -1)$.
- **The Equator (Superpositions):** States that are equal parts $|0\rangle$ and $|1\rangle$ (50/50 probability) lie entirely on the equator of the sphere. Changing the relative phase between the amplitudes moves the point around this equator:
  - $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$**:** Located on the positive x-axis at $(1, 0, 0)$.
  - $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$**:** Located on the negative x-axis at $(-1, 0, 0)$.
  - $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$**:** Located on the positive y-axis at $(0, 1, 0)$.
  - $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$**:** Located on the negative y-axis at $(0, -1, 0)$.

- **Universal Mapping:** A qubit is not restricted to the poles or the equator; a valid qubit state can be **any point** on the surface of the Bloch sphere.

2. Global vs. Relative Phase

Core Explanations & Theoretical Breakdowns:

- **Global Phase:** A global phase is an overall complex phase multiplier, such as $e^{i\theta}$, applied to the entire quantum state.
  - *Physical Irrelevance:* When calculating the probability of a measurement outcome, we take the norm-square of the amplitude. Because the norm-square of any phase $e^{i\theta}$ is exactly 1 ($|e^{i\theta}|^2 = 1$), a global phase has zero effect on the measurement probabilities in *any* basis.
  - *Conclusion:* **Global phases are physically irrelevant** and can be entirely dropped or ignored. Quantum states that differ only by a global phase correspond to the exact same point on the Bloch sphere.
- **Relative Phase:** A relative phase is the complex phase difference *between* the $|0\rangle$ and $|1\rangle$ amplitudes within the superposition.
  - *Physical Significance:* Unlike global phases, relative phases are physically significant because they dictate the exact longitude of the state on the Bloch sphere.
  - *Example:* The states $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ have different relative phases. While they yield the same 50/50 statistics if measured in the Z-basis, they yield entirely different results if measured in the X-basis (measuring $|+\rangle$ yields $|+\rangle$ 100% of the time, while measuring $|i\rangle$ yields $|+\rangle$ or $|-\rangle$ 50% of the time).

3. Spherical Coordinates: Parameterizing the Qubit State

Mathematical Formulas & Angle Definitions:

- To precisely map any normalized generic state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to the Bloch sphere, we parameterize the complex amplitudes α and β using two angles:
  1. **Polar Angle (θ):** Measures the angle straight down from the north pole ($|0\rangle$). It is restricted to the range $0 \ \theta \ \pi$.
  2. **Azimuthal Angle ():** Measures the rotation across from the positive x-axis in the xy-equatorial plane. It is restricted to $0 \ < 2\pi$.
- **The Parameterization Equation:** Because the global phase is irrelevant, we can factor it out to ensure the amplitude of $|0\rangle$ is strictly real and positive. The state is then mathematically written as:

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

.

(Note: The angles in the amplitudes are halved ($\theta/2$), but the physical angle mapped on the 3D Bloch sphere is θ).

- **Mapping to Cartesian Coordinates:** Once θ and are known, the exact (x, y, z) coordinates on the sphere are calculated using:
  - $x = \sin\theta\cos$
  - $y = \sin\theta\sin$
  - $z = \cos\theta$

Step-by-Step Example Process:
To map a complex state like $\frac{3+i\sqrt{3}}{4}|0\rangle - \frac{1}{2}|1\rangle$ to the Bloch sphere:

1. **Make the $|0\rangle$ amplitude real:** Convert $\frac{3+i\sqrt{3}}{4}$ to polar form, which is $\frac{\sqrt{3}}{2}e^{i\pi/6}$. Factor out the global phase $e^{i\pi/6}$, leaving the state equivalent to $\frac{\sqrt{3}}{2}|0\rangle - e^{-i\pi/6}\frac{1}{2}|1\rangle$.
2. **Ensure the equation matches the standard format (+ sign):** Convert the minus sign on the $|1\rangle$ amplitude to a phase using $-1 = e^{i\pi}$. The $|1\rangle$ amplitude becomes $e^{i\pi}e^{-i\pi/6}\frac{1}{2} = e^{i5\pi/6}\frac{1}{2}$. The fully formatted state is:

$$\frac{\sqrt{3}}{2}|0\rangle + e^{i5\pi/6}\frac{1}{2}|1\rangle$$

.
3. **Solve for θ and :**
   - Compare to $\cos(\theta/2)|0\rangle$: $\cos(\theta/2) = \frac{\sqrt{3}}{2}$ $\theta/2 = \pi/6$ $\theta = \pi/$ (or 60°).
   - Compare to $e^{i}\sin(\theta/2)|1\rangle$: $e^{i} = e^{i5\pi/6}$ $= \pi/$ (or 150°).
4. **Conclusion:** The qubit is located 60° down from the north pole and rotated 150° around the xy-plane from the x-axis.

IV. Multiple Qubit Systems & Entanglement

1. Multiple Qubit Systems

Core Definitions & Concepts:

- **The Tensor Product / Kronecker Product:** When dealing with multiple qubits, their combined state is mathematically represented using the **tensor product** (denoted by). For example, if we have two qubits both in the $|0\rangle$ state, their combined state is written as $|0\rangle$ $|0\rangle$. In practice, this notation is often compressed to $|0\rangle|0\rangle$ or simply $|00\rangle$.
- **Vector Representation (Kronecker Product Math):** In linear algebra, the tensor product is calculated as the Kronecker product, which is obtained by multiplying every term of the first column vector by the entire second column vector.
  - *Step-by-step Example:* To find the vector for $|01\rangle$ (which is $|0\rangle$ $|1\rangle$), we multiply the vector for $|0\rangle$ by the vector for $|1\rangle$:

$$|01\rangle = \begin{pmatrix}10\end{pmatrix} \begin{pmatrix}01\end{pmatrix} = 1\begin{pmatrix}01\end{pmatrix}0\begin{pmatrix}01\end{pmatrix} = 0100$$

.

Scaling to n-Qubit Systems (2^n):

- **Exponential Vector Size:** With a single qubit, there are 2 basis states. With n qubits, the number of basis states scales exponentially to $N = 2^n$. The general state of an n-qubit system is a superposition of all these 2^n basis states, meaning its column vector will have exactly 2^n complex amplitudes.
- *Significance:* Because the vector size doubles with every added qubit, a system of just 300 qubits requires tracking 2^{300} amplitudes—a number greater than the total number of atoms in the visible universe. This exponential scaling is evidence of why simulating quantum systems on classical computers becomes rapidly intractable, hinting at the boundary between the P and BQP complexity classes.

2. Entanglement

When multiple qubits interact, their states can either remain independent or become fundamentally linked.

A. Product States (Separable States):

- **Core Concept:** A multi-qubit state is called a **product state** (or separable state) if it can be perfectly factored into the tensor products of individual, independent single-qubit states.
- **Properties:** In a product state, the qubits have no entanglement. If you measure one qubit in a product state, it collapses independently and has absolutely zero effect on the state of the other qubit.
- *Example:* The state $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$ can be factored into $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which is precisely the product state $|+\rangle|-\rangle$.

B. Entangled States & Bell States:

- **Core Concept:** Quantum states that *cannot* be factored into the product of individual single-qubit states are called **entangled states**. Because they cannot be factored, the condition of one qubit is fundamentally intertwined with the condition of the other.
- **Measurement Effect:** If you measure a single qubit in an entangled state, it instantly affects the state of the other qubit.
- **Maximally Entangled States (The Bell States):** When measuring one qubit *completely* determines the outcome of the other qubit, the system is maximally entangled. For two qubits, there are exactly four maximally entangled states, known

as the **Bell states** or **EPR pairs** (named after Einstein, Podolsky, and Rosen). They are:

1. $|^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. $|^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.
3. $|^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.
4. $|^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

- *Theoretical Breakdown (Proof of Entanglement):* To prove $|^+\rangle$ is entangled, attempt to factor it into $(\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_0|0\rangle + \beta_0|1\rangle)$. Expanding this yields $\alpha_1\alpha_0|00\rangle + \alpha_1\beta_0|01\rangle + \beta_1\alpha_0|10\rangle + \beta_1\beta_0|11\rangle$. Matching coefficients with $|^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, we find $\alpha_1\beta_0 = 0$ (meaning either $\alpha_1 = 0$ or $\beta_0 = 0$). However, if $\alpha_1 = 0$, then $\alpha_1\alpha_0 = 0$ $\frac{1}{\sqrt{2}}$, which is a contradiction. Thus, no such factorization exists.

C. Monogamy of Entanglement:

- **Core Concept:** Classically, information can be perfectly correlated among multiple parties (e.g., Alice, Bob, and Charlie can all share the exact same bit value perfectly). Quantum entanglement, however, does not behave this way.
- **The Principle:** Entanglement is strictly **monogamous**. The principle dictates that if two qubits (Alice and Bob) are maximally entangled with each other (such as being in the $|^+\rangle$ state), they cannot be entangled *at all* with a third qubit (Charlie).
- **Implication:** Like an exclusive relationship, the correlation between Alice and Bob in a maximally entangled state is fully exhausted between the two of them, forbidding any quantum correlation with a third party.

V. Quantum Information Processing & System Evolution

1. Quantum Computing System & Evolution of Quantum Systems

- **Unitary Evolution:**
  - **Core Concept:** In linear algebra, quantum states are represented as vectors, and quantum gates are represented as matrices. For a matrix to represent a valid quantum gate, it must ensure that the total probability of the quantum state remains equal to 1 after the transformation.
  - **Mathematical Breakdown:** Mathematically, a matrix U preserves this probability if it satisfies the condition $UU =$, where U is the conjugate transpose of U, and is the identity matrix. Matrices that satisfy this exact property are called **unitary matrices**. Therefore, the evolution of a closed quantum system is governed strictly by unitary matrices.
- **Reversibility:**
  - **Core Concept:** A matrix is considered reversible (or invertible) if there exists an inverse matrix U^{-1} such that $U^{-1}U = UU^{-1} =$.

- **Quantum vs. Classical:** In classical computing, gates like AND or OR are irreversible because information is lost (you cannot uniquely determine the inputs from the output). In quantum computing, because every valid gate must be a unitary matrix ($UU =$), the inverse of the gate is simply its conjugate transpose: $U^{-1} = U$.
- **Conclusion:** This guarantees that **all quantum gates are perfectly reversible**. You can always undo a quantum operation by applying U to the system: $UU|\psi\rangle = |\psi\rangle = |\psi\rangle$.

2. Quantum Gates

A. Single-Qubit Gates

All single-qubit quantum gates can be geometrically interpreted as rotations of the qubit's state around the Bloch sphere.

- **Pauli X (NOT) Gate:** Turns $|0\rangle$ into $|1\rangle$, and $|1\rangle$ into $|0\rangle$. It is represented by the matrix $\begin{pmatrix} 0 & 11 & 0 \end{pmatrix}$ and is geometrically equivalent to a 180° rotation about the x-axis of the Bloch sphere.
- **Pauli Y Gate:** Turns $|0\rangle$ into $i|1\rangle$, and $|1\rangle$ into $-i|0\rangle$. It is represented by the matrix $\begin{pmatrix} 0 & -ii & 0 \end{pmatrix}$ and is a 180° rotation about the y-axis.
- **Pauli Z Gate:** Keeps $|0\rangle$ as $|0\rangle$ but flips the sign of $|1\rangle$ to $-|1\rangle$. It is represented by the matrix $\begin{pmatrix} 1 & 00 & -1 \end{pmatrix}$ and is a 180° rotation about the z-axis.
- **Phase (S) Gate:** The square root of the Z gate ($S^2 = Z$). It turns $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $i|1\rangle$. It corresponds to a 90° rotation about the z-axis and its matrix is $\begin{pmatrix} 1 & 00 & i \end{pmatrix}$.
- **T Gate:** The square root of the S gate ($T^2 = S$). It turns $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $e^{i\pi/4}|1\rangle$. It is a 45° rotation about the z-axis.
- **Hadamard (H) Gate:** Creates superpositions by turning $|0\rangle$ into the $|+\rangle$ state and $|1\rangle$ into the $|-\rangle$ state. It is represented by the matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 11 & -1 \end{pmatrix}$ and is a 180° rotation about the diagonal x+z axis.

B. Multi-Qubit Gates

- **Controlled-NOT (CNOT / CX) Gate:** A two-qubit gate that inverts the target (right) qubit if the control (left) qubit is 1; otherwise, it does nothing.
  - *Mathematical Operation:* It acts as a quantum XOR gate: $CNOT|a\rangle|b\rangle = |a\rangle|a\ b\rangle$.
  - *Significance:* CNOT is incredibly important because applying it to a superposition can create **entangled states** (e.g., $CNOT|+\rangle|0\rangle$ produces the maximally entangled Bell state $|^+\rangle$).
- **SWAP Gate:** A two-qubit gate that simply swaps the states of two qubits: $SAP|a\rangle|b\rangle = |b\rangle|a\rangle$. It cannot generate entanglement on its own and can be

constructed using three sequential CNOT gates.

- **Toffoli (CCNOT) Gate:** A three-qubit gate (controlled-controlled-NOT) that flips the third (target) qubit if and only if both the first and second (control) qubits are 1: $Toffoli|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|ab\ c\rangle$.
    - *Significance:* Because the Toffoli gate is universal for classical computing, its existence as a valid, reversible quantum gate proves that quantum computers can efficiently compute anything a classical computer can.

3. Quantum Measurements

- **Collapsing the Wave Function:**
    - **Core Concept:** While the laws of quantum mechanics allow a qubit to exist in a superposition (a linear combination like $\alpha|0\rangle + \beta|1\rangle$), a qubit cannot be observed as a superposition.
    - **The Collapse:** Upon measurement, the qubit instantly "collapses" into a single, definite basis state (either $|0\rangle$ or $|1\rangle$). Once measured, the original superposition is permanently destroyed.
- **Calculating Probabilities:**
    - **The Rule:** The probability of getting a specific measurement outcome is mathematically defined as the **norm-square of its amplitude**.
    - **Formula & Example:** For a normalized state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the probability of measuring $|0\rangle$ is exactly $|\alpha|^2$, and the probability of measuring $|1\rangle$ is exactly $|\beta|^2$.
    - *Step-by-Step Breakdown:* If a qubit is in the superposition $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$:
        1. Identify the amplitude of $|0\rangle$: $\frac{\sqrt{3}}{2}$.
        2. Square the norm: $|\frac{\sqrt{3}}{2}|^2 = \frac{3}{4}$. The probability of getting $|0\rangle$ is 75%.
        3. Identify the amplitude of $|1\rangle$: $\frac{1}{2}$.
        4. Square the norm: $|\frac{1}{2}|^2 = \frac{1}{4}$. The probability of getting $|1\rangle$ is 25%.

VI. Challenges and Advantages Over Classical Computation

1. Advantages of Quantum Computation

- **Quantum Parallelism and Speedups:**
    - *Core Concept:* It is a common misconception that quantum computers simply compute all answers at once in a "massively parallel" way; if a superposition of answers is measured, only one result is obtained. Instead, quantum algorithms manipulate the amplitudes of these superpositions to amplify the correct answer before measurement.
    - *Polynomial & Quadratic Speedups:* For brute-force searching an unstructured database of size N, classical computers require $O(N)$ queries. Quantum computers use Grover's algorithm to find the target in exactly $O(\sqrt{N})$ queries, representing a provable quadratic speedup.
    - *Exponential Speedups:* For certain oracular problems, such as finding a secret XOR mask (Simon's algorithm), quantum computers can solve the problem in

$O(n)$ queries compared to a classical computer's $O(2^{n/2})$, demonstrating an exponential speedup.

- **Phase Kickback:**
  - *Mechanism:* When querying a quantum oracle U_f, the standard operation maps the input and answer qubits as $|x\rangle|y\rangle \ \ |x\rangle|y \ f(x)\rangle$. However, if the answer qubit is prepared in the $|-\rangle$ state, querying the oracle leaves the answer qubit unchanged while the input qubit acquires a phase: $|x\rangle|-\rangle \ \ (-1)^{f(x)}|x\rangle|-\rangle$.
  - *Significance:* This "phase kickback" allows quantum algorithms (like Deutsch-Jozsa and Bernstein-Vazirani) to encode the function's output directly into the phase of the input qubit, enabling problem-solving in significantly fewer queries.
- **Amplitude Amplification:**
  - *Mechanism:* Used centrally in Grover's Algorithm, this process involves repeatedly applying the oracle U_f followed by a reflection operator R_s (which reflects the state about the uniform superposition $|s\rangle$).
  - *Effect:* Each rotation step geometrically moves the state closer to the "winner" state $|\rangle$ in the coordinate plane, amplifying the amplitude (and thus the measurement probability) of the correct answer while suppressing the others.
- **Solving Intractable Problems (Shor's Algorithm):**
  - *The Problem:* Factoring large numbers is the basis of modern RSA cryptography because no known classical algorithm can factor large integers efficiently (the best classical algorithm, the Number Field Sieve, takes subexponential time).
  - *The Quantum Solution:* Peter Shor invented a quantum algorithm in 1994 that utilizes the Quantum Fourier Transform to find the period of modular exponents.
  - *Impact:* Shor's algorithm provides a subexponential speedup over classical computers, rendering RSA vulnerable and suggesting that quantum computers may overturn the Strong Church-Turing Thesis (which states that any computer can be efficiently simulated by a classical probabilistic Turing machine).

2. Challenges in Quantum Computation

- **Decoherence:**
  - *Core Concept:* Qubits are highly sensitive to their environment, and it is extremely difficult to isolate them while still keeping them accessible for gates and measurements. Interaction with the environment causes "decoherence," shifting the qubit away from its intended state.
  - *Bit-Flip Errors:* Instead of a complete flip from $|0\rangle$ to $|1\rangle$, a physical qubit may experience a partial bit-flip error where it rotates only slightly toward the opposite pole on the Bloch sphere.

    - *Phase-Flip Errors:* A qubit can also experience a phase flip, which corresponds to an unintended rotation around the z-axis (e.g., drifting from $|+\rangle$ toward $|-\rangle$ along the equator).
- **The No-Cloning Theorem:**
    - *Core Concept:* Classically, error correction relies on creating copies of data (like the repetition code). In quantum mechanics, however, it is physically impossible to create an identical copy of a general, unknown quantum state.
    - *Theoretical Breakdown:* If a quantum cloning gate U existed, it would have to perform the operation $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$. Because $|\psi\rangle|\psi\rangle$ scales quadratically rather than linearly, this violates the fundamental linear algebra governing quantum mechanics (unitary matrices are strictly linear operators).
    - *Consequence:* Because unknown states cannot be copied, classical repetition codes cannot be used directly for quantum error correction.
- **Quantum Error Correction:**
    - *Parity Measurements (The Workaround):* Because measuring a qubit collapses its superposition, we cannot read the data directly to look for errors. Instead, we use CNOT gates and an extra "ancilla" qubit to calculate the parity of adjacent qubits. This reveals the "error syndrome" (e.g., indicating which specific qubit flipped) without measuring and collapsing the actual encoded quantum information.
    - *The Shor Code:* Invented by Peter Shor, this error-correcting code combines the 3-qubit phase-flip code and the 3-qubit bit-flip code via a method called concatenation.
    - *Mechanism:* It uses exactly 9 physical qubits to securely encode 1 logical qubit (e.g., $|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$).
    - *Result:* By alternating between correcting bit-flip and phase-flip errors using parity measurements, the Shor code can successfully correct all quantum errors, provided no more than one error of each type occurs per triplet in a correction cycle. Building hardware where errors accumulate slowly enough for these codes to keep up—a "fault-tolerant" quantum computer—remains the ultimate goal.

Based strictly on the provided textbook *Introduction to Classical and Quantum Computing* by Thomas G. Wong, here are your comprehensive, detailed study notes for **VII. Quantum Algorithms**.

VII. Quantum Algorithms

1. Deutsch-Jozsa Algorithm

- **Purpose & Core Concept:**
    - The algorithm is designed to evaluate a boolean function $f(x)$ that takes an n-bit binary string x and outputs either 0 or 1.

    - We are given the promise that the function is either **constant** (outputs 0 all the time or 1 all the time) or **balanced** (outputs 0 half the time and 1 half the time). The goal is to determine which category the function falls into.
- **Computational Speedup:**
    - *Classical Runtime:* To be absolutely certain whether the function is constant or balanced classically, one must query the oracle in the worst-case scenario $2^{n-1}+1$ times.
    - *Quantum Runtime:* The Deutsch-Jozsa algorithm determines the answer with 100% certainty in exactly **1 query**. This represents an **exponential speedup** over exact classical algorithms, though it provides no speedup over bounded-error probabilistic classical algorithms (which require $O(1)$ queries).
- **Mechanism & Theoretical Breakdown:**
    - **Step 1:** Begin with n input qubits all in the $|0\rangle$ state and apply a Hadamard gate (H) to each. This creates a uniform superposition over all possible n-bit strings: $\frac{1}{\sqrt{2^n}} \, _{x0,1^n} |x\rangle$.
    - **Step 2:** Query the phase oracle U_f, which uses phase kickback (by keeping the answer qubit in the $|-\rangle$ state) to multiply each state by $(-1)^{f(x)}$. The state becomes $\frac{1}{\sqrt{2^n}} \, _x (-1)^{f(x)} |x\rangle$.
    - **Step 3:** Apply the Hadamard gate to all n qubits again. Mathematically, this transforms the state into a sum over all possible outcomes $|z\rangle$, where the amplitude of measuring the specific all-zeros state $|0..00\rangle$ is exactly $\frac{1}{2^n} \, _x (-1)^{f(x)}$.
- **Measurement Conclusion:**
    - If f is constant, all $f(x)$ values are the same, making the sum evaluate to ± 1. The probability of measuring $|0..00\rangle$ is $|\pm 1|^2 = 1$ (100%).
    - If f is balanced, exactly half of the outputs are 1 and half are 0, causing the positive and negative terms to perfectly cancel out. The amplitude is 0, making the probability of measuring $|0..00\rangle$ exactly 0%.
    - *Conclusion:* If you measure the n qubits and get $|0..00\rangle$, the function is constant; if you get anything else, the function is balanced.

2. Grover's Algorithm

- **Purpose & Core Concept:**
    - The algorithm performs brute-force searching of an unstructured database. Given a function $f(x)$ that outputs 0 for all inputs except one special "winner" input where $f() = 1$, the goal is to find .
- **Computational Speedup & Optimality:**
    - *Classical Runtime:* Classically, one must check the inputs one by one, requiring $O(N)$ queries (where $N = 2^n$) to find the winner on average.
    - *Quantum Runtime:* Grover's algorithm finds the winner in $O(\sqrt{N})$ **queries**, delivering a provable **quadratic speedup** over classical searches.

- *Optimality:* It has been mathematically proven that quantum computers cannot solve this brute-force problem faster than $O(\sqrt{N})$. Therefore, Grover's algorithm is optimally efficient, and proves that quantum computers cannot magically brute-force NP-complete problems in polynomial time by simply checking all answers in superposition.

- **Mechanism & Amplitude Amplification:**
  - **Step 1:** Initialize the system by applying Hadamards to all qubits, creating a uniform superposition $|s\rangle$ of all states. We define $|r\rangle$ as the superposition of all non-winner states.
  - **Step 2:** Query the phase oracle U_f. Because $f() = 1$ and $f(r) = 0$, phase kickback flips the sign (amplitude) of the winner state $|\rangle$ while leaving $|r\rangle$ unchanged. Geometrically, this reflects the state across the $|r\rangle$ axis.
  - **Step 3:** Apply the reflection operator $R_s = 2|s\rangle\langle s| -$, which reflects the state about the uniform superposition state $|s\rangle$.
  - **Result:** Together, U_f and R_s rotate the quantum state vector by exactly 2θ toward the winner state $|\rangle$ in the 2D plane.
  - By repeating this process t $\frac{\pi}{4}\sqrt{N}$ times, the state aligns almost perfectly with $|\rangle$, meaning a measurement will yield the winner with near 100% probability.

3. Shor's Algorithm

- **Purpose & Core Concept:**
  - Shor's algorithm efficiently solves the problem of prime factorization: given a large integer N that is the product of two prime numbers p and , find p and .
  - Because modern RSA public-key cryptography relies on the fact that factoring is practically impossible for classical computers, Shor's algorithm theoretically breaks RSA encryption.
- **Computational Speedup:**
  - *Classical Runtime:* The best known classical factoring method (the number field sieve) takes subexponential time (roughly $e^{n^{1/3}}$).
  - *Quantum Runtime:* Shor's algorithm provides a **subexponential speedup** over classical algorithms (running in polynomial time $O(n^3)$), serving as strong evidence against the Strong Church-Turing thesis.
- **Mechanism & Theoretical Breakdown:**
  - The algorithm reduces the problem of factoring to finding the period r of a modular exponential function $a^x \bmod N$. It contains three primary steps:
  - **Step 1 (Classical):** Pick a random number $1 < a < N$. Check the greatest common divisor $\mathrm{cd}(a, N)$. If it is > 1, you got extremely lucky and found a factor. If $\mathrm{cd}(a, N) = 1$, proceed to Step 2.
  - **Step 2 (Quantum Period Finding):** Use a quantum computer to find the period r of the function $f(x) = a^x \bmod N$.
    - This is done by preparing an equal superposition of eigenstates using a modular multiplication gate.

        - By utilizing the **Quantum Phase Estimation** algorithm, the quantum computer evaluates the phase of these eigenstates.
        - An **Inverse Quantum Fourier Transform (IQFT)** is applied to the eigenvalue register to extract an m-bit approximation of s/r (where s is an integer).
        - A classical continued fractions algorithm is then used on this approximation to deduce the exact period r. Ensure r is even and $a^{r/2}\ \ N-1 \bmod N$; otherwise pick a new a.
    - **Step 3 (Classical):** With the correct period r found, calculate the factors using elementary number theory: $p = \mathrm{cd}(a^{r/2}-1, N)$ and $\ = \mathrm{cd}(a^{r/2}+1, N)$.