The State of a Quantum System

- In quantum mechanics, the state of a system represents all possible information about the system.
- Unlike classical systems (where a particle has a definite position and velocity), in quantum systems the state is probabilistic and described using **state vectors** or **wave functions**.

2. Mathematical Representation

- The state is represented as a **vector in Hilbert space**.
- For a single qubit (two-level system), the general state is:

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

  where:

  - α and β are complex numbers.
  - Normalization condition: $|\alpha|^2 + |\beta|^2 = 1$.
- For multi-qubit systems, states are described using tensor products. Example:

  $|\psi\rangle = |0\rangle \otimes |1\rangle = |01\rangle$

3. Superposition Principle

- A quantum state can exist in a linear combination of basis states.
- Example:

  $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$

  → the system is in superposition of both $|0\rangle$ and $|1\rangle$.

4. Measurement and Probabilities

- Measurement collapses the state into one of the basis states.
- The probability of observing a particular outcome is given by the square of the amplitude:
  - Probability of measuring $|0\rangle = |\alpha|^2$
  - Probability of measuring $|1\rangle = |\beta|^2$
- Example: For $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$,
  - Probability($|0\rangle$) = 1/2
  - Probability($|1\rangle$) = 1/2

5. Types of Quantum States

- **Pure State**:
  - Described by a single state vector $|\psi\rangle$.
  - Example: $|0\rangle$, $(1/\sqrt{2})(|0\rangle + |1\rangle)$.
- **Mixed State**:
  - Represents statistical uncertainty over pure states.
  - Described by a **density matrix**:

    $\rho = \Sigma\, p_i\, |\psi_i\rangle\langle\psi_i|$

    where p_i are probabilities.

8. Example of a Quantum State

- Consider an electron spin (spin-1/2 particle):
  - State can be $|\uparrow\rangle$ (spin-up) or $|\downarrow\rangle$ (spin-down).
  - General state:

    $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$
- Measurement along z-axis gives outcomes with probabilities $|\alpha|^2$ and $|\beta|^2$.

Time-Evolution of a Closed Quantum System

- A **closed quantum system** is one that does not interact with the environment.
- Its time evolution is governed entirely by its **Hamiltonian** (energy operator).
- The evolution is **deterministic** and **reversible**.

2. Schrödinger Equation

- The dynamics of a closed quantum system are described by the **time-dependent Schrödinger equation**:

  $i\hbar\, (d/dt)|\psi(t)\rangle = H\, |\psi(t)\rangle$

  where:

  - $|\psi(t)\rangle$ = state of the system at time t
  - H = Hamiltonian operator (represents energy of system)
  - $\hbar$ = reduced Planck's constant
  - I = imaginary unit.

3. Solution of Schrödinger Equation

- The general solution is:

  $|\psi(t)\rangle = U(t)\, |\psi(0)\rangle$

  where U(t) is the **time-evolution operator**:

  $U(t) = \exp(-iHt / \hbar)$
- U(t) is a **unitary operator** ($U^\dagger U = I$), which ensures probability conservation.

4. Key Properties of Time Evolution

1. **Unitary**: Evolution preserves total probability (norm of state vector remains 1).
2. **Reversible**: Given $|\psi(t)\rangle$, one can always recover $|\psi(0)\rangle$.
3. **Deterministic**: Unlike measurement, time evolution does not involve randomness.
4. **Depends on Hamiltonian**: The Hamiltonian fully determines how the system evolves.

6. Importance

- Time evolution explains how isolated quantum systems behave over time.
- Foundation for **quantum simulation**, **quantum gates**, and **quantum algorithms**.
- Ensures **unitary evolution** before measurement collapses the state.

Composite Quantum Systems

- A **composite system** is a quantum system made up of two or more subsystems.
- The total state is described in a **larger Hilbert space**, which is the **tensor product** of the individual subsystem spaces.
- Composite systems allow the study of **entanglement**, one of the most important features of quantum mechanics.

2. Mathematical Representation

- If system A has state space H_a and system B has state space H_β, then the combined system lives in:

  $H = H_a \otimes H_\beta$

- If $|\psi_a\rangle$ is a state of A and $|\psi_\beta\rangle$ is a state of B, then the joint state is:

  $|\psi\rangle = |\psi_a\rangle \otimes |\psi_\beta\rangle$

- Example:
  If A = $|0\rangle$ and B = $|1\rangle$, then:

  $|\psi\rangle = |0\rangle \otimes |1\rangle = |01\rangle$

3. Superposition in Composite Systems

- Just like single systems, composite systems can exist in **superpositions** of product states.
- Example (two qubits):

  $|\psi\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$

4. Entanglement

- Some composite states cannot be written as a simple product of subsystem states. These are **entangled states**.
- Example (Bell state):

  $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$

- Entanglement shows strong correlations between subsystems, even when separated by large distances.

6. Examples of Composite Systems

1. **Two Qubits**: States like $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
2. **Atom + Photon**: Combined system of matter and light.

1. Mixed States

(a) Pure vs Mixed States

- **Pure state**: A quantum system described by a single state vector $|\psi\rangle$ in Hilbert space. Example: $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$.
- **Mixed state**: Describes a system when there is **classical uncertainty** about which pure state it is in. Example: A qubit is in $|0\rangle$ with probability 0.6 and in $|1\rangle$ with probability 0.4.

(b) Density Operator Formalism

- A mixed state is represented using a **density matrix (ρ)**:

  $\rho = \Sigma\, p_i |\psi_i\rangle\langle\psi_i|$

  where $p_i \geq 0$ and $\Sigma\, p_i = 1$.

- Example: If a qubit has 50% chance of being $|0\rangle$ and 50% chance of being $|1\rangle$:

  $\rho = 0.5\, |0\rangle\langle 0| + 0.5\, |1\rangle\langle 1| =$
  [[0.5, 0],
  [0, 0.5]]

(c) Properties of Density Matrix

1. The **eigenvalues of a density matrix** lie between 0 and 1, and their sum is 1.
2. A density matrix is always **Hermitian**.
3. The **trace of a density matrix is 1**, ensuring total probability is normalized.

(d) Importance of Mixed States

- Describes systems interacting with an **environment** (open quantum systems).
- Models **imperfect knowledge** of a system.

2. General Quantum Operations

A quantum operation describes how a quantum state (density matrix) evolves, not only under unitary gates, but also when noise, measurements, or open-system effects are present.

(a) Time Evolution vs General Evolution

- In a closed system: evolution is **unitary** ($U\rho U^\dagger$).
- In an open system: need more general description because of noise, measurements, and environment effects.

(b) Completely Positive Trace-Preserving (CPTP) Maps

A **CPTP map** is the most general mathematical description of how a quantum state evolves.

It extends beyond unitary evolution to include **noise, measurement, and interactions with the environment**.

$$\rho' = \Sigma E_i \rho E_i^\dagger$$

where $\{E_i\}$ are **Kraus operators**, satisfying: $\Sigma E_i^\dagger E_i = I$

(c) Examples of Quantum Operations

1. **Unitary Evolution**: $\rho' = U\rho U^\dagger$ (special case of CPTP).
2. **Measurement**: If measurement operators are $\{M_m\}$, then after outcome m: $\rho' = (M_m \rho M_m^\dagger) / P(m)$, where $P(m) = Tr(M_m \rho M_m^\dagger)$.
3. **Noise Channels**:
   - Bit-flip channel
   - Phase-damping channel
   - Depolarizing channel

(d) Importance of Quantum Operations

- Needed to describe **realistic systems** (not perfectly isolated).
- Provide the mathematical framework for **quantum algorithms under noise**.
- Essential for **quantum error correction** and **fault-tolerant quantum computing**.

Universal Sets of Quantum Gates

- In classical computing, any computation can be built from a small set of **logic gates** (e.g., AND, OR, NOT).
- Similarly, in **quantum computing**, there exists a small set of **quantum gates** from which any unitary operation can be constructed.
- Such a collection is called a **Universal Set of Quantum Gates**.

2. Quantum Gates Basics

- A quantum gate is a **unitary operator** acting on one or more qubits.
- They transform quantum states while preserving normalization.
- Examples:
  - **Single-qubit gates**: Pauli-X, Y, Z; Hadamard (H).
  - **Multi-qubit gates**: CNOT, Toffoli, Controlled-phase.

3. Definition of Universality

- A set of quantum gates is **universal** if it can approximate any arbitrary unitary operation **U** on n qubits to any desired accuracy.
- Universal gates allow construction of **all quantum algorithms**.

4. Common Universal Gate Sets

(a) {H, T, CNOT}

- **Hadamard (H)**: Creates superposition.
- **T-gate (π/8 gate)**: Adds a specific quantum phase.
- **CNOT (Controlled-NOT)**: Introduces entanglement.
- This set is **universal** because:
  - H + T generate arbitrary single-qubit rotations.
  - CNOT adds entanglement between qubits.

(b) {Clifford + T}

The **Clifford group** is a special set of gates that map **Pauli operators (X, Y, Z)** to other Pauli operators under conjugation.

When you combine **Clifford gates** with the **T gate**, you get a **universal gate set**.

This means **any unitary transformation** on qubits can be approximated to arbitrary precision using just H, S, CNOT, and T.

(c) Toffoli + Hadamard

- Toffoli gate (controlled-controlled-NOT) + H can also form a universal set.

 Toffoli gate alone is **classically universal**, but not quantum universal (no superpositions).

 Hadamard introduces **superposition and interference**, enabling access to the full power of quantum mechanics.

 Together, **Toffoli + H form a universal gate set**:

- Toffoli provides nonlinear classical control.
- Hadamard provides quantum parallelism.

6. Importance of Universal Gate Sets

1. Provide the **building blocks** for quantum algorithms (Shor's, Grover's, QFT, etc.).
2. Allow implementation of **arbitrary unitary operations** on qubits.
3. Simplify hardware design: only need to implement a small set of gates in physical quantum computers.
4. Essential for **fault-tolerant quantum computing** (error correction works best with certain universal sets).

1. Quantum Measurement

- Measurement in quantum mechanics is the process of extracting **classical information** from a quantum system.
- Unlike classical measurement, quantum measurement **disturbs** the state being measured.
- Quantum measurement is fundamentally **probabilistic**, unlike classical measurement.
- It is described by a set of **measurement operators** {Mm}, where each operator corresponds to a possible outcome.

Postulates of Measurement

1. **Probabilities**:
   If state is $|\psi\rangle$, the probability of measuring outcome m is:

   $P(m) = \langle\psi|P_m|\psi\rangle$

   where P_m is the projector onto the eigenstate.

2. **State Collapse**:
   After measurement, the system collapses to the eigenstate corresponding to the observed outcome.

(c) Types of Measurements

1. **Projective (von Neumann) Measurement**: Standard measurement with projection operators P_m.
2. **POVM (Positive Operator-Valued Measure)**: Generalized measurement, useful in noisy or practical systems.

(d) Example

- Measuring a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the computational basis:
    - Probability(0) = $|\alpha|^2$, collapses to $|0\rangle$.
    - Probability(1) = $|\beta|^2$, collapses to $|1\rangle$.

(e) Importance

- Connects the **quantum world to classical information**.
- Essential for running quantum algorithms (final output must be measured).
- Provides randomness in quantum systems.

2. Quantum Entanglement

- **Entanglement** is a uniquely quantum phenomenon where the state of one particle is **inseparably linked** to the state of another, even when separated by large distances.
- An entangled state cannot be written as a product of single-qubit states.

(b) Example: Bell States (Maximally Entangled States)

Four common entangled two-qubit states:

$|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$
$|\Phi^-\rangle = (1/\sqrt{2})(|00\rangle - |11\rangle)$
$|\Psi^+\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle)$
$|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$

(c) Properties of Entanglement

1. **Non-local correlations**: Measurement outcomes are correlated, even across distance.
2. **No classical counterpart**: Cannot be explained by classical probability.
3. **Non-separability**: Entangled states cannot be factored into independent subsystems.

(d) Applications of Entanglement

1. **Quantum teleportation** (transfer of quantum state using entanglement + classical communication).
2. **Superdense coding** (sending 2 classical bits with 1 qubit).
3. **Quantum cryptography** (security from entanglement correlations).
4. **Quantum algorithms and quantum error correction**.

The Quantum Fourier Transform (QFT)

- The **Quantum Fourier Transform (QFT)** is the quantum analogue of the **Discrete Fourier Transform (DFT)**.
- It transforms quantum states from the **computational basis** to the **frequency basis**.
- QFT is a central tool in many quantum algorithms such as **Shor's Algorithm** and **Phase Estimation**.

2. Mathematical Definition

For an **n-qubit system**, let

- The number of possible states be $\mathbf{N = 2^n}$
- A computational basis state be **|x⟩**, where $\mathbf{x \in \{0,1,\dots,N-1\}}$

Then the Quantum Fourier Transform is defined as:

QFT(|x⟩) = (1 / √N) Σ (from y = 0 to N-1) [e^(2πi·x·y / N) |y⟩]

3. Matrix Form of QFT

The QFT is represented by an **N × N unitary matrix**:

QFT = (1 / √N) ⌈ 1, 1, 1, …, 1
1, ω, ω², …, ω^(N-1)
1, ω², ω⁴, …, ω^(2(N-1))
…
1, ω^(N-1), ω^(2(N-1)), …, ω^((N-1)(N-1)) ⌉

where

ω = e^(2πi / N) (the primitive N-th root of unity).

4. Properties of QFT

1. **Unitary** → QFT · QFT† = I
2. **Efficient** → Implemented with $O(n^2)$ quantum gates vs. $O(N^2)$ in classical DFT.
3. **Reversible** → Inverse QFT exists, given by:

$$\mathbf{QFT^{-1}(|x\rangle) = (1 / \sqrt{N})\ \Sigma\ (from\ y=0\ to\ N-1)\ [\ e\text{^}(-2\pi i \cdot x \cdot y / N)\ |y\rangle\ ]}$$

---

5. Circuit Implementation

For an **n-qubit register** $|x_1x_2\ldots x_n\rangle$:

- Apply a **Hadamard (H)** on the first qubit.
- Apply controlled **phase shift gates (Rk)**:

$$R_k = |0\rangle\langle 0| + e\text{^}(2\pi i / 2^k)\ |1\rangle\langle 1|$$

- Repeat for all qubits.
- Apply **SWAP gates** at the end to reverse qubit order.

---

6. Example (QFT on 2 qubits, N=4)

Let input = |x⟩ = |1⟩ (binary 01, decimal 1).

QFT(|1⟩) = (1/2) [|0⟩ + i|1⟩ – |2⟩ – i|3⟩]

This spreads amplitudes in the frequency basis.

---

7. Applications of QFT

1. **Shor's Algorithm** → integer factoring.
2. **Quantum Phase Estimation (QPE)** → finding eigenvalues of unitary operators.
3. **Period Finding** → crucial for factoring.
4. **Hidden Subgroup Problem** → general algorithmic framework.

---

8. Importance

- Provides **exponential speedup** compared to classical Fourier transform.
- The backbone of many powerful quantum algorithms.
- Showcases **quantum parallelism**.

1. Definition

Quantum Phase Estimation (QPE) is a quantum algorithm used to estimate the **phase (φ)** in the eigenvalue equation of a unitary operator.

If **U |u⟩ = e^(2πi·φ) |u⟩**, then the goal of QPE is to find the value of **φ**, where $0 \le \varphi < 1$.

---

2. Basic Idea

- QPE uses **two quantum registers**:
    1. **First register (m qubits):** stores the phase information.
    2. **Second register:** contains the eigenvector |u⟩.
- The algorithm encodes φ into the first register using controlled operations, then applies the **Inverse Quantum Fourier Transform (QFT^{-1})** to extract the binary digits of φ.

---

3. Steps of the Algorithm

1. **Initialize:**
   State = |0…0⟩ ⊗ |u⟩
2. **Hadamard Gates:**
   Apply H to each qubit in the first register → creates superposition:
   $(1/\sqrt{(2^m)})\ \Sigma\ (k=0\ to\ 2^m-1)\ |k\rangle \otimes |u\rangle$
3. **Controlled-U operations:**
   Apply controlled-U^(2^j) → introduces phase shift:
   $(1/\sqrt{(2^m)})\ \Sigma\ (k=0\ to\ 2^m-1)\ e\text{^}(2\pi i\cdot\varphi\cdot k)\ |k\rangle \otimes |u\rangle$
4. **Inverse QFT:**
   Apply QFT^{-1} on first register → converts phase information into binary representation.
5. **Measurement:**
   Measure first register → gives an **m-bit approximation of φ**.

---

4. Formula

- Eigenvalue relation:
  U |u⟩ = e^(2πi·φ) |u⟩
- Final superposition before inverse QFT:
  $(1/\sqrt{(2^m)})\ \Sigma\ (k=0\ to\ 2^m-1)\ e\text{^}(2\pi i\cdot\varphi\cdot k)\ |k\rangle \otimes |u\rangle$
- After QFT^{-1}:
  First register ≈ |φ in binary⟩

---

5. Example

If U|u⟩ = e^(2πi·(3/8)) |u⟩, then φ = 3/8.

- Binary expansion: $\varphi = 0.011_2$
- QPE with 3 qubits in the first register gives output 011.

- Hence measurement result ≈ 3/8.

---

6. Applications

1. **Shor's Algorithm** → used for order finding and factoring.
2. **Quantum Simulation** → estimating energy levels of molecules.
3. **Quantum Chemistry** → eigenvalue computation of Hamiltonians.
4. **Hidden Subgroup Problems** and **Discrete Logarithms**.

Order-Finding and Factoring in Quantum Computing

---

1. Introduction

- **Factoring**: The problem of finding prime factors of a large integer **N**.
- **Order-finding**: A related mathematical problem, used as a subroutine in **Shor's algorithm** for factoring.
- Classical algorithms for factoring are slow (sub-exponential), while **quantum algorithms using order-finding are exponentially faster**.

---

2. Order-Finding Problem

Definition

Given two integers:

- A positive integer **N**
- An integer **a**, where gcd(a, N) = 1

The **order r of a modulo N** is the smallest positive integer **r** such that:

$\mathbf{a^r \equiv 1 \ (\mathrm{mod}\ N)}$

Example

Let N = 15, a = 2.

- Compute powers:
  $2^1 = 2 \bmod 15$
  $2^2 = 4 \bmod 15$
  $2^3 = 8 \bmod 15$
  $2^4 = 16 \equiv 1 \bmod 15$

So, order **r = 4**.

---

3. Factoring Using Order-Finding

Key Idea

Factoring a number **N** can be reduced to finding the order of a random number **a** modulo N.

1. Choose random **a** < N with gcd(a, N) = 1.
2. Find order **r** of **a mod N** using **Quantum Phase Estimation** + modular exponentiation.
3. If **r** is even, compute:

   p = gcd(a^(r/2) – 1, N)
   q = gcd(a^(r/2) + 1, N)

   These give non-trivial factors of **N**.

Example (Factoring N = 15)

1. Pick a = 2.
2. Order r = 4 (as shown earlier).
3. Compute:
   - $a^{(r/2)} = 2^2 = 4$
   - gcd(4 – 1, 15) = gcd(3, 15) = 3
   - gcd(4 + 1, 15) = gcd(5, 15) = 5

Thus, factors of 15 are **3 and 5**.

---

4. Quantum Algorithm for Order-Finding

1. **Superposition**: Create uniform superposition of states.
2. **Modular Exponentiation**: Apply U: $|x\rangle \to |a^x \bmod N\rangle$.
3. **Quantum Phase Estimation (QPE)**: Extract the phase related to order **r**.
4. **Classical Post-Processing**: Use **continued fractions** to recover r from measured phase.

5. Importance

- Order-finding is the **core quantum subroutine** of Shor's factoring algorithm.
- Factoring large integers is hard for classical computers (basis of RSA cryptography).
- Quantum order-finding allows efficient factoring, **breaking RSA security**.

Applications of the Quantum Fourier Transform (QFT)

The QFT is a key mathematical tool in quantum computing. Its main applications arise from its ability to **detect periodicity** in quantum states. Many important quantum algorithms are built upon this property.

1. Period-Finding

Concept

- Period-finding means determining the **repeating pattern (period)** in a function.
- If a function f(x) is periodic with period r, then f(x) = f(x + r).
- The QFT helps to extract this period efficiently from a quantum state encoding the function values.

Steps

1. Encode function f(x) into quantum states.
2. Apply **superposition** over inputs.
3. Perform **QFT** to convert the state into frequency space.
4. Measurement gives information about the **period r**.

Importance

- **Shor's Algorithm** for factoring integers uses period-finding.
- Classical methods for period-finding are exponential time, but QFT makes it polynomial time.

---

2. Discrete Logarithms

Concept

- The **discrete logarithm problem**: Given g and h = g^x (mod p), find the integer x.
- This is very hard for classical computers (basis of many cryptosystems).
- QFT helps solve it by turning it into a **hidden period problem**.

Steps

1. Encode powers of g into quantum states.
2. Use QFT to find the hidden periodicity between powers of g and the value h.
3. From the period, extract the discrete logarithm x.

Importance

- Breaks cryptographic systems like **Diffie–Hellman key exchange** and **ElGamal encryption**.
- Shows how quantum computing threatens classical cryptography.

3. Hidden Subgroup Problem (HSP)

Concept

- A general problem in group theory: Suppose we have a function f defined on a group G.
- The function is constant on cosets of a **hidden subgroup H** ⊆ G, and different on different cosets.
- Goal: Find the hidden subgroup H.

Steps

1. Encode the group elements into quantum states.
2. Apply superposition over the group.
3. Use **QFT** to reveal information about the subgroup structure.
4. Measurement yields generators of the hidden subgroup.

Importance

- **Period-finding** and **discrete logarithms** are special cases of HSP.
- Shor's algorithm and many other quantum algorithms can be understood as solving HSP.
- Generalizing HSP helps design new quantum algorithms.