# 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:

|ψ⟩ = α|0⟩ + β|1⟩

where:

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

|ψ⟩ = |0⟩ ⊗ |1⟩ = |01⟩

### 3. Superposition Principle

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

|ψ⟩ = (1/√2)(|0⟩ + |1⟩)

→ the system is in superposition of both |0⟩ and |1⟩.

### 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⟩ = |α|²
  + Probability of measuring |1⟩ = |β|²
* Example: For |ψ⟩ = (1/√2)(|0⟩ + |1⟩),
  + Probability(|0⟩) = 1/2
  + Probability(|1⟩) = 1/2

### 5. Types of Quantum States

* **Pure State**:
  + Described by a single state vector |ψ⟩.
  + Example: |0⟩, (1/√2)(|0⟩ + |1⟩).
* **Mixed State**:
  + Represents statistical uncertainty over pure states.
  + Described by a **density matrix**:

ρ = Σ pᵢ |ψᵢ⟩⟨ψᵢ|

where pᵢ are probabilities.

### 8. Example of a Quantum State

* Consider an electron spin (spin-1/2 particle):
  + State can be |↑⟩ (spin-up) or |↓⟩ (spin-down).
  + General state:

|ψ⟩ = α|↑⟩ + β|↓⟩

* Measurement along z-axis gives outcomes with probabilities |α|² and |β|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**:

iħ (d/dt)|ψ(t)⟩ = H |ψ(t)⟩

where:

* + |ψ(t)⟩ = state of the system at time t
  + H = Hamiltonian operator (represents energy of system)
  + ħ = reduced Planck’s constant
  + I = imaginary unit.

### 3. Solution of Schrödinger Equation

* The general solution is:

|ψ(t)⟩ = U(t) |ψ(0)⟩

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

U(t) = exp(−iHt / ħ)

* U(t) is a **unitary operator** (U†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 |ψ(t)⟩, one can always recover |ψ(0)⟩.
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 Hₐ and system B has state space Hᵦ, then the combined system lives in:

H = Hₐ ⊗ Hᵦ

* If |ψₐ⟩ is a state of A and |ψᵦ⟩ is a state of B, then the joint state is:

|ψ⟩ = |ψₐ⟩ ⊗ |ψᵦ⟩

* Example:  
  If A = |0⟩ and B = |1⟩, then:

|ψ⟩ = |0⟩ ⊗ |1⟩ = |01⟩

### 3. Superposition in Composite Systems

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

|ψ⟩ = (1/√2)(|00⟩ + |11⟩)

### 4. Entanglement

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

|Φ⁺⟩ = (1/√2)(|00⟩ + |11⟩)

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

### 6. Examples of Composite Systems

1. **Two Qubits**: States like |00⟩, |01⟩, |10⟩, |11⟩.
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 |ψ⟩ in Hilbert space.  
  Example: |ψ⟩ = (1/√2)(|0⟩ + |1⟩).
* **Mixed state**: Describes a system when there is **classical uncertainty** about which pure state it is in.  
  Example: A qubit is in |0⟩ with probability 0.6 and in |1⟩ with probability 0.4.

### (b) Density Operator Formalism

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

ρ = Σ pᵢ |ψᵢ⟩⟨ψᵢ|

where pᵢ ≥ 0 and Σ pᵢ = 1.

* Example: If a qubit has 50% chance of being |0⟩ and 50% chance of being |1⟩:

ρ = 0.5 |0⟩⟨0| + 0.5 |1⟩⟨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** (UρU†).
* 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**.

ρ′ = Σ Eᵢ ρ Eᵢ†

where {Eᵢ} are **Kraus operators**, satisfying:  
Σ Eᵢ† Eᵢ = I

### (c) Examples of Quantum Operations

1. **Unitary Evolution**:  
   ρ′ = UρU†  
   (special case of CPTP).
2. **Measurement**:  
   If measurement operators are {Mₘ}, then after outcome m:  
   ρ′ = (Mₘ ρ Mₘ†) / P(m),  
   where P(m) = Tr(Mₘ ρ Mₘ†).
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 |ψ⟩, the probability of measuring outcome m is:

P(m) = ⟨ψ|Pₘ|ψ⟩

where Pₘ is the projector onto the eigenstate.

1. **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 Pₘ.
2. **POVM (Positive Operator-Valued Measure)**:  
   Generalized measurement, useful in noisy or practical systems.

### (d) Example

* Measuring a qubit |ψ⟩ = α|0⟩ + β|1⟩ in the computational basis:
  + Probability(0) = |α|², collapses to |0⟩.
  + Probability(1) = |β|², collapses to |1⟩.

### (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:

|Φ⁺⟩ = (1/√2)(|00⟩ + |11⟩)  
|Φ⁻⟩ = (1/√2)(|00⟩ - |11⟩)  
|Ψ⁺⟩ = (1/√2)(|01⟩ + |10⟩)  
|Ψ⁻⟩ = (1/√2)(|01⟩ - |10⟩)

### (c) Properties of Entanglement

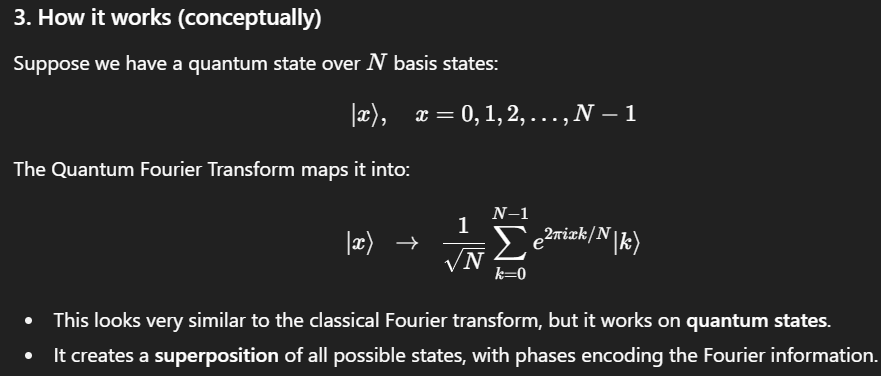
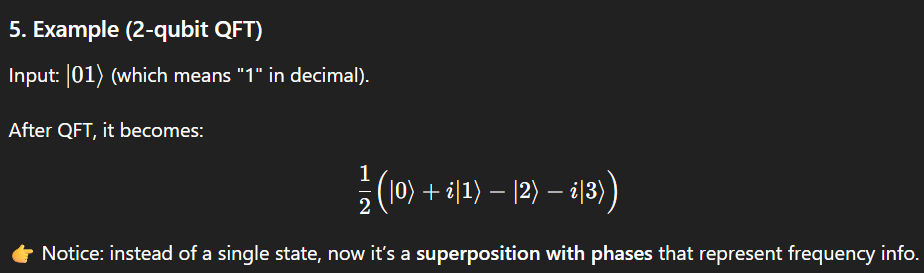
1. **Non-local correlations**: Measurement outcomes are correlated, even across distance.
2. **No classical counterpart**: Cannot be explained by classical probability.
3. **Non-separability**: Entangled states cannot be factored into independent subsystems.

### (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**.
* The QFT is built using **Hadamard gates** + **controlled phase gates**.
* It only needs about O(n^2) gates for n qubits, which is very efficient.

**Working Process or Steps on n qbits:**

 Put **Hadamard** on a qubit → makes superposition.

 Use **controlled phase gates** with smaller and smaller angles → add frequency phases.

 Do this for every qubit.

 At the end, **reverse the order of qubits**.

## 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

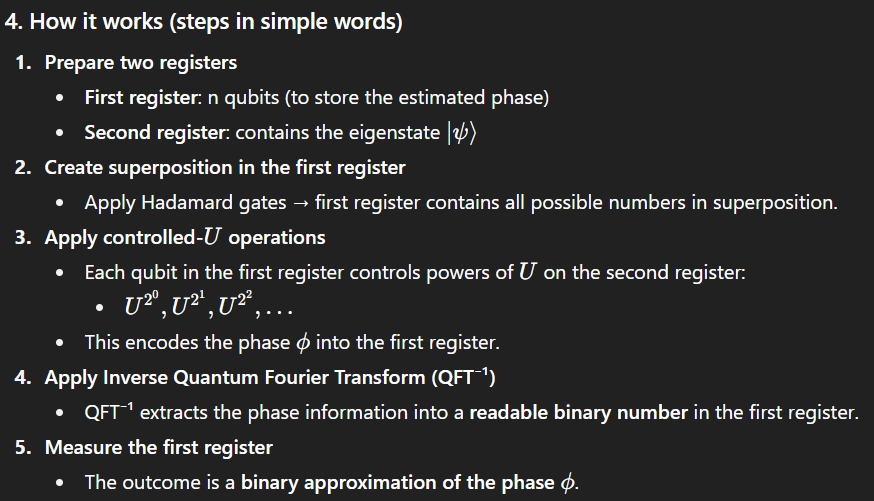
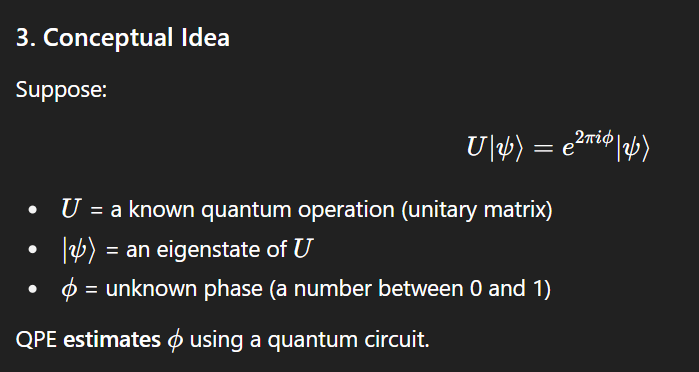
* Provides **exponential speedup** compared to classical Fourier transform.
* The backbone of many powerful quantum algorithms.
* Showcases **quantum parallelism**.

**Quantum Phase Estimation (QPE)**

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

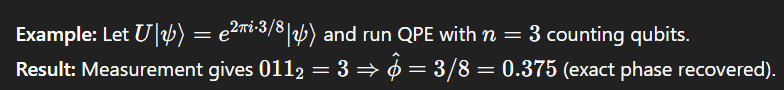
 Its goal: **find the phase (angle) associated with an eigenvalue of a unitary operator**.

 In simpler terms: if a quantum operation U rotates a state ∣ψ⟩| by some angle ϕ, QPE tells you **what ϕ is**.



### **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**

* **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**.
* For integers N and a (where gcd(a,N)=1), the **order r** of a mod  N is the **smallest positive integer** such that:
* a^ r ≡1(mod N).

## ****2. Order-Finding Problem****

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:

**aʳ ≡ 1 (mod N)**

### **Example**

Let N = 15, a = 2.

* Compute powers:  
  2¹ = 2 mod 15=2  
  2² = 4 mod 15=4  
  2³ = 8 mod 15=8  
  2⁴ = 16 ≡ 1 mod 15=0

So, order **r = 4**.

## Factoring Using Order-Finding (Simple Explanation)

## The goal is to factor a big number N (find its prime factors). Quantum computers use order-finding to do this fast.

## Steps:

## Pick a random number

## Choose a<N such that gcd (a,N)=1

## (Means a and N have no common divisor).

## Find the order r

## The order rrr is the smallest number such that:a^r ≡ 1(mod N)

## Quantum computers find this rrr efficiently using Quantum Phase Estimation (QPE) + Quantum Fourier Transform (QFT).

## Use the order to get factors

## 

## 

# **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.