TOPICS IN QUANTUM THEORY

Mathematical structures of quantum theory

1. ***States***
   (definition, convexity, boundary, discrimination, Bloch sphere)

2. ***Effects***
   (definition, convexity, Gleason's theorem, ordering)

3. ***Observables and Measurements***
   (definition, convexity, incompatibility, informational completeness, PVM, POVM)

4. ***Channels***
   (definition, convexity, Stinespring's theorem, Choi-Jamiolkowski representation,examples)

5. ***Time evolution***
   (Schrodinger's equation, Lindblad equation, Markovianity)

6. ***Quantum entanglement***
   (definition, LOCC ordering, distillation, bound entanglement, witnesses, PPT criterion)

7. ***Multipartite entanglement***
   (definition, GHZ states, W states, quantum secret sharing)

Introduction to quantum information processing and quantum algorithms

1. ***Qubits***
   (Bloch sphere, superposition vs mixtures, composite systems and subsystems, Bell basis)

2. ***Qubit gates***
   (examples, universality, decoherence)

3. ***Quantum algorithms***
   (Berstein-Vazirani alg., Deutsch-Josza alg., Simon's problem)

4. ***Implementation***
   (ions, photons, qdots, superconducting qubits, diVincenzo criteria)

5. ***Quantum key distribution*** (one-time pad, BB84, E91)

6. ***Bipartite communication protocols***
   (q-teleportation, quantum dense coding, entanglement swapping)

7. ***Fourier transform*** and ***Shor's factorization algorithm***

8. ***Grover's search algorithm***

9. ***Shannon Information theory***
   (information, entropy, communication capacities)

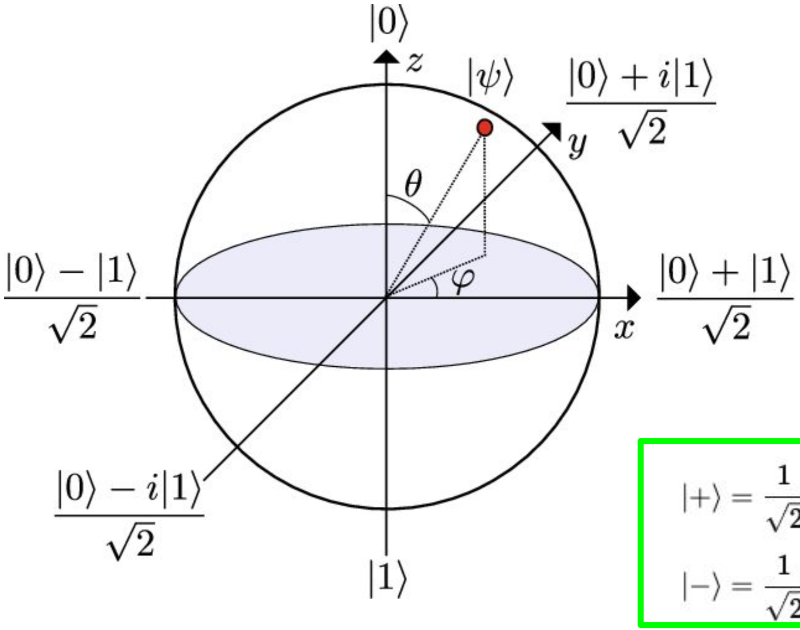
10. ***Quantum error correction***
    (bit flip error correction, Shor's 9 qubit correction code)

Basics.

Qubit: 2-level system

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

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



$|0\rangle$
z
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
y
θ
φ
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
x
$\frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
$|1\rangle$

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

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Superposition: *Linear combination of Basis States*

$$|\psi\rangle = \sum_i c_i|i\rangle$$

orthonormal basis $\{|i\rangle\}$

Born Rule:

$$P(i) = |c_i|^2$$

$$\sum_i |c_i|^2 = 1$$

Matrix elements of Operator O :

$$O_{ij} = \langle b_i|\hat{O}|b_j\rangle$$

$$|\psi\rangle = \sum_i c_i|b_i\rangle$$

(Basis states) $\{|b_i\rangle\}$

$$c_i = \langle b_i|\psi\rangle$$

under the hood...

- Experiments
- interference/wave formalism
- Linear algebra rules, hilbert spaces.
- Group theory

Basis Representation & Conversion

Basis Change for States:

Quantum State psi can be represented in different bases $|\psi\rangle \Longrightarrow \begin{cases} \{|b_i\rangle\} \\ \{|c_j\rangle\} \end{cases}$

$$|\psi\rangle = \sum_i c_i |b_i\rangle$$

Suppose you want to express the same state in a **new basis**

(Basis states)

$\{|b_i\rangle\}$

$$c_i = \langle b_i|\psi\rangle$$

$$|\psi\rangle = \sum_i c_i |b_i\rangle$$

Change of basis is accomplished by expressing the old basis in terms of the new basis: $\Rightarrow$

$$|b_i\rangle = \sum_j U_{ji} |c_j\rangle$$

$$U_{ji} = \langle c_j|b_i\rangle$$

So now new coefficients of the state psi in the new basis are:

$$d_j = \sum_i U_{ji} c_i \Longrightarrow \vec{d} = U\vec{c}$$

(In matrix form)

Basis Change for Operators:

$$O_{ij} = \langle b_i|\hat{O}|b_j\rangle \Longleftarrow$$

Matrix elements in b-basis

In the context of basis changes:
→ **columns** of the matrix represent the old basis vectors (in this case *b_i*)
→ **rows** represent the new basis vectors (in this case *c_k*)

Suppose you want to change to a new basis: $\{|c_k\rangle\}$

Then, old basis can be written in terms of new basis as: $|b_i\rangle = \sum_k U_{ki} |c_k\rangle$

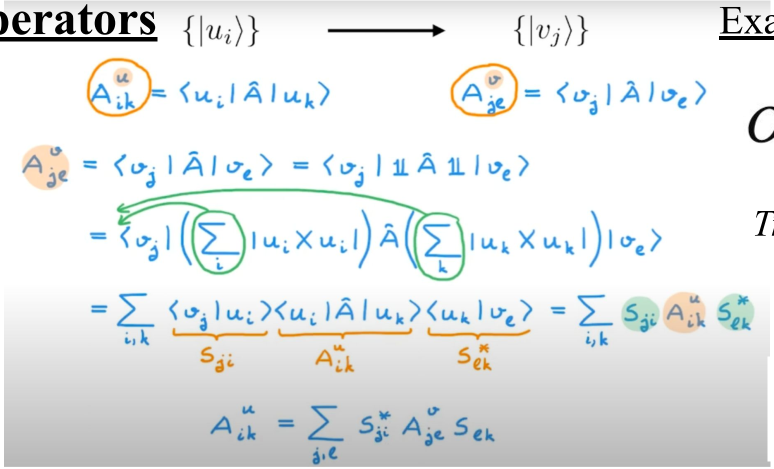
Matrix elements of old Operator *O* are written in the new basis as:

$$\underset{\text{row}\ \ \text{column}}{O'_{kl}} = \sum_{i,j} U_{ki} O_{ij} U^*_{lj} \Longleftrightarrow O' = UOU^\dagger$$

U is the unitary matrix that transforms between the two bases

Re-iterated (Basis change)

Operators



$\{|u_i\rangle\} \longrightarrow \{|v_j\rangle\}$

$\boxed{A^u_{ik}} = \langle u_i|\hat{A}|u_k\rangle \qquad \boxed{A^v_{je}} = \langle v_j|\hat{A}|v_e\rangle$

$$A^v_{je} = \langle v_j|\hat{A}|v_e\rangle = \langle v_j|\mathbb{1}\hat{A}\mathbb{1}|v_e\rangle$$

$$= \langle v_j|\Big(\sum_i |u_i\rangle\langle u_i|\Big)\hat{A}\Big(\sum_k |u_k\rangle\langle u_k|\Big)|v_e\rangle$$

$$= \sum_{i,k} \underbrace{\langle v_j|u_i\rangle}_{S_{ji}}\underbrace{\langle u_i|\hat{A}|u_k\rangle}_{A^u_{ik}}\underbrace{\langle u_k|v_e\rangle}_{S^*_{ek}} = \sum_{i,k} S_{ji}A^u_{ik}S^*_{ek}$$

$$A^u_{ik} = \sum_{j,e} S^*_{ji}A^v_{je}S_{ek}$$

Example: $\{|b_1\rangle, |b_2\rangle\} \Longrightarrow \{|c_1\rangle, |c_2\rangle\}$

$$O_b = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \qquad U^\dagger = U^T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Transformation: $O_c = UO_bU^\dagger$

$$UO_b = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 3 & 4 \\ 1 & -2 \end{pmatrix}$$

$$O_c = \frac{1}{\sqrt{2}}\begin{pmatrix} 3 & 4 \\ 1 & -2 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$O_c = \begin{pmatrix} \frac{7}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix}$$

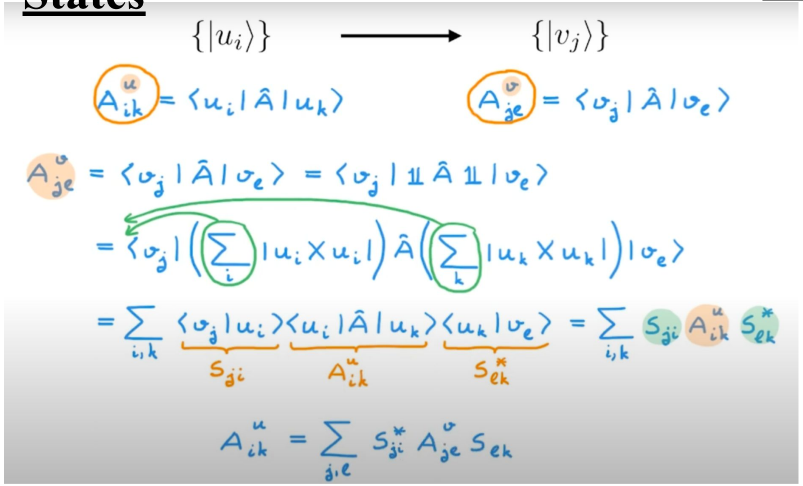
in new basis

Same U for both examples

The transformation matrix U that connects the two bases

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

States



$\{|u_i\rangle\} \longrightarrow \{|v_j\rangle\}$

$\boxed{A^u_{ik}} = \langle u_i|\hat{A}|u_k\rangle \qquad \boxed{A^v_{je}} = \langle v_j|\hat{A}|v_e\rangle$

$$A^v_{je} = \langle v_j|\hat{A}|v_e\rangle = \langle v_j|\mathbb{1}\hat{A}\mathbb{1}|v_e\rangle$$

$$= \langle v_j|\Big(\sum_i |u_i\rangle\langle u_i|\Big)\hat{A}\Big(\sum_k |u_k\rangle\langle u_k|\Big)|v_e\rangle$$

$$= \sum_{i,k} \underbrace{\langle v_j|u_i\rangle}_{S_{ji}}\underbrace{\langle u_i|\hat{A}|u_k\rangle}_{A^u_{ik}}\underbrace{\langle u_k|v_e\rangle}_{S^*_{ek}} = \sum_{i,k} S_{ji}A^u_{ik}S^*_{ek}$$

$$A^u_{ik} = \sum_{j,e} S^*_{ji}A^v_{je}S_{ek}$$

Example:

$\{|b_1\rangle, |b_2\rangle\} \Longrightarrow \{|c_1\rangle, |c_2\rangle\}$

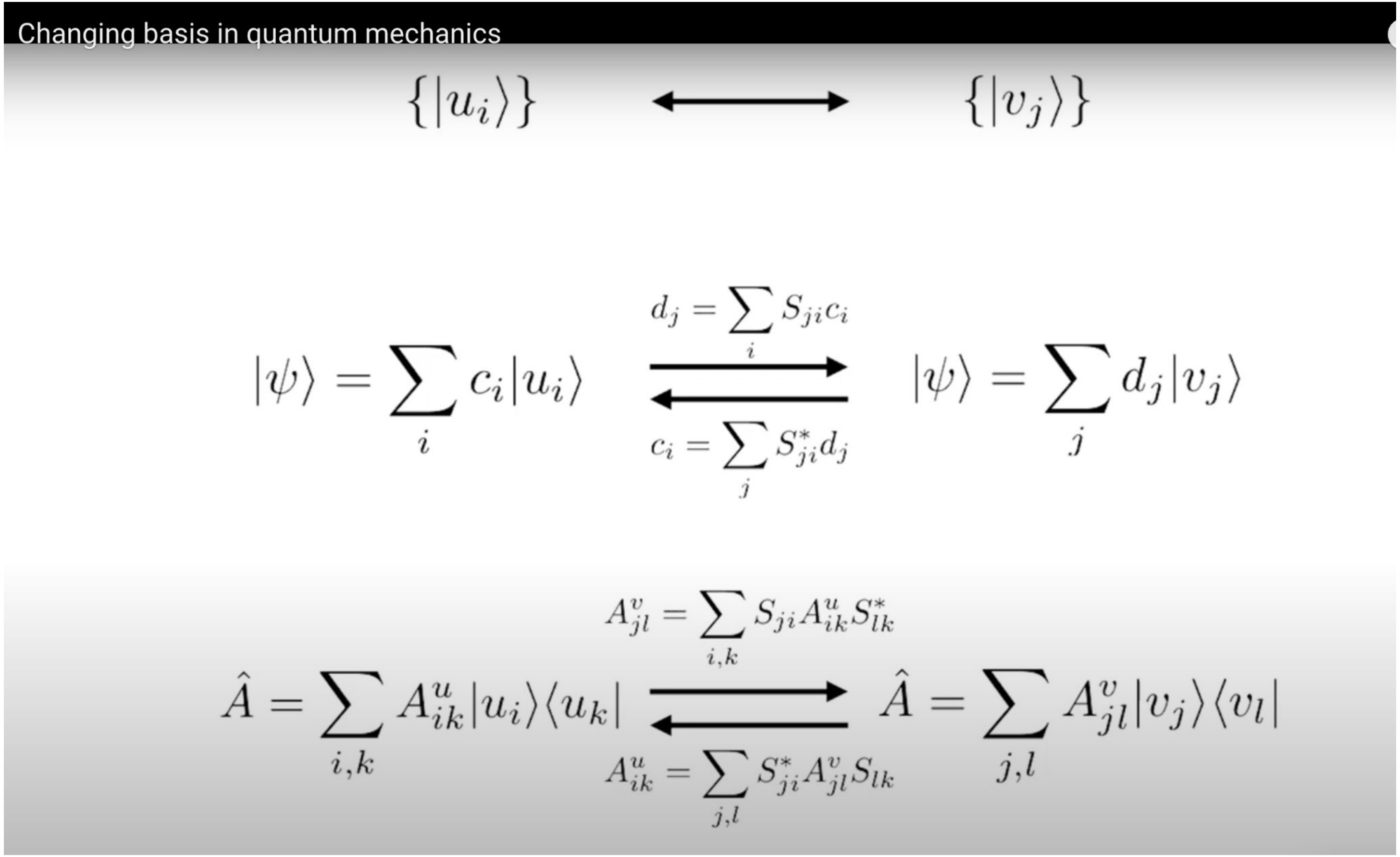
$$|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_b$$

So, $|\psi\rangle_c = U|\psi\rangle_b$

$$|\psi\rangle_c = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

So in new basis: $|\psi\rangle_c = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Summary of basis transformation



Changing basis in quantum mechanics

$$\begin{tikzcd}\{|u_i\rangle\} \arrow[r, leftrightarrow] & \{|v_j\rangle\}\end{tikzcd}$$

$$\begin{tikzcd}|\psi\rangle = \sum_i c_i|u_i\rangle \arrow[r, shift left, "d_j = \sum_i S_{ji}c_i"] & |\psi\rangle = \sum_j d_j|v_j\rangle \arrow[l, shift left, "c_i = \sum_j S^*_{ji}d_j"]\end{tikzcd}$$

$$\begin{tikzcd}\hat{A} = \sum_{i,k} A^u_{ik}|u_i\rangle\langle u_k| \arrow[r, shift left, "A^v_{jl} = \sum_{i,k} S_{ji}A^u_{ik}S^*_{lk}"] & \hat{A} = \sum_{j,l} A^v_{jl}|v_j\rangle\langle v_l| \arrow[l, shift left, "A^u_{ik} = \sum_{j,l} S^*_{ji}A^v_{jl}S_{lk}"]\end{tikzcd}$$

Convexity:

convex set *is a set of points such that, for any two points within the set, the* ***line connecting them*** *is also entirely within/part of the set.*

pick any two points inside the shape and draw a straight line between them, that line will be ***entirely inside*** *the shape.*

a ***real-number*** *set like the interval [0,1], any point between 0 and 1 (such as 0.5) is also in the set. So, the* ***interval [0,1]*** *is convex.*

A set of quantum states is convex:

⇒ Pure States >> *Surface*

⇒ Mixed States >> *Interior*

— Any point inside ball is a probabilistic mixture of pure states

MIXED STATES & Density Operators

In quantum mechanics, **convexity** for quantum states refers to the idea that **mixed states** can be expressed as a **convex combination** (weighted sum) of **pure states**. This concept is central to the description of mixed states and represents how they can be viewed as statistical mixtures of different pure states.

Mixed States: Convexity applies to **mixed states**, which represent a system being in different pure states with certain probabilities. Mixed states are distinguished from pure states, which cannot be decomposed into a convex combination.

Pure States: A **pure state** is an extreme point of the convex set of states, meaning that it cannot be decomposed further as a mixture of other states.

Convex Set of Quantum States: The set of all valid quantum states (density matrices) forms a **convex set**, meaning any convex combination of valid quantum states is also a valid quantum state.

$$\rho_{\text{pure}} = |\psi\rangle\langle\psi|$$

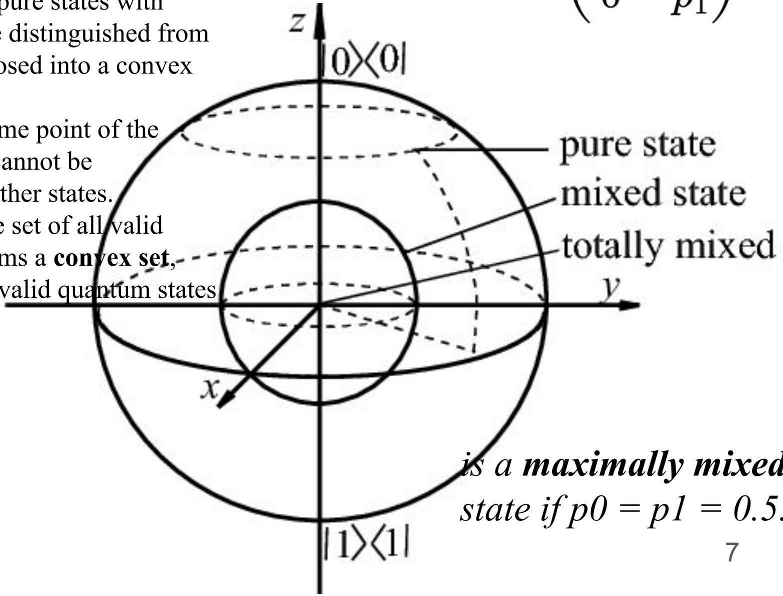
$$\rho_{\text{mixed}} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$$\rho_{\text{mixed}} = p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1|$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho_{\text{mixed}} = \begin{pmatrix} p_0 & 0 \\ 0 & p_1 \end{pmatrix}$$



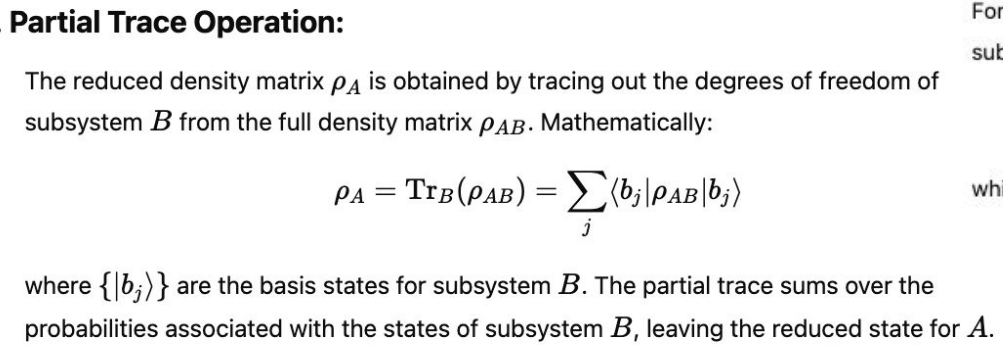
is a ***maximally mixed*** *state if p0 = p1 = 0.5.*

Reduced Density Operator & Trace

Consider a bipartite system *A* and *B*. The state of the system is described by a density matrix (either mixed or pure): ρ_{AB}

Reduced Density Matrix is obtained by tracing out the degrees of freedom of subsystem *B*

$$\rho_A = \mathrm{Tr}_B(\rho_{AB})$$

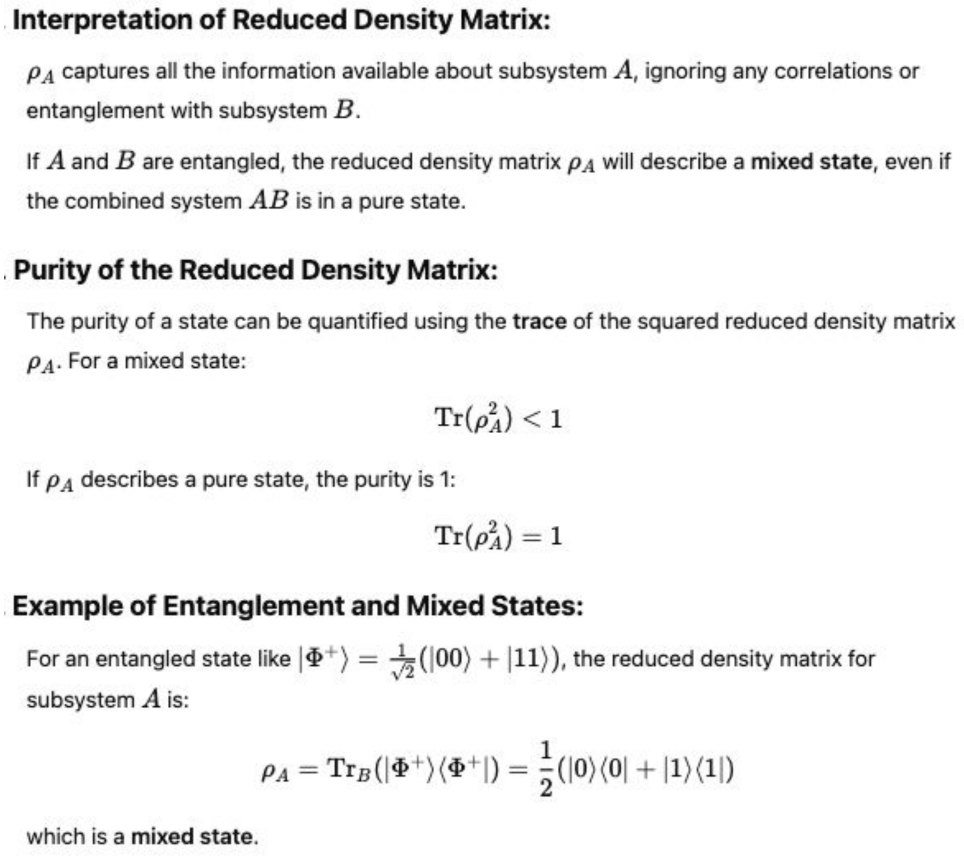


Partial Trace Operation:

The reduced density matrix ρ_A is obtained by tracing out the degrees of freedom of subsystem B from the full density matrix ρ_{AB}. Mathematically:

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \sum_j \langle b_j|\rho_{AB}|b_j\rangle$$

where $\{|b_j\rangle\}$ are the basis states for subsystem B. The partial trace sums over the probabilities associated with the states of subsystem B, leaving the reduced state for A.



Interpretation of Reduced Density Matrix:

ρ_A captures all the information available about subsystem A, ignoring any correlations or entanglement with subsystem B.

If A and B are entangled, the reduced density matrix ρ_A will describe a **mixed state**, even if the combined system AB is in a pure state.

Purity of the Reduced Density Matrix:

The purity of a state can be quantified using the **trace** of the squared reduced density matrix ρ_A. For a mixed state:

$$\mathrm{Tr}(\rho_A^2) < 1$$

If ρ_A describes a pure state, the purity is 1:

$$\mathrm{Tr}(\rho_A^2) = 1$$

Example of Entanglement and Mixed States:

For an entangled state like $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the reduced density matrix for subsystem A is:

$$\rho_A = \mathrm{Tr}_B(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

which is a **mixed state**.

More on density matrix:

Hermitian:
(so eigenvalues are real numbers)

$$\rho = \rho^\dagger$$

Normalization:
(probability sums to 1)

$$\mathrm{Tr}(\rho) = 1$$

Positivity:
(density matrix must be a ***positive semi-definite****, so probabilities aren't negative)*

$$\langle\psi|\rho|\psi\rangle \geq 0$$

For Pure State

$$\rho^2 = \rho$$

$$\mathrm{Tr}(\rho^2) = 1$$

For Mixed State

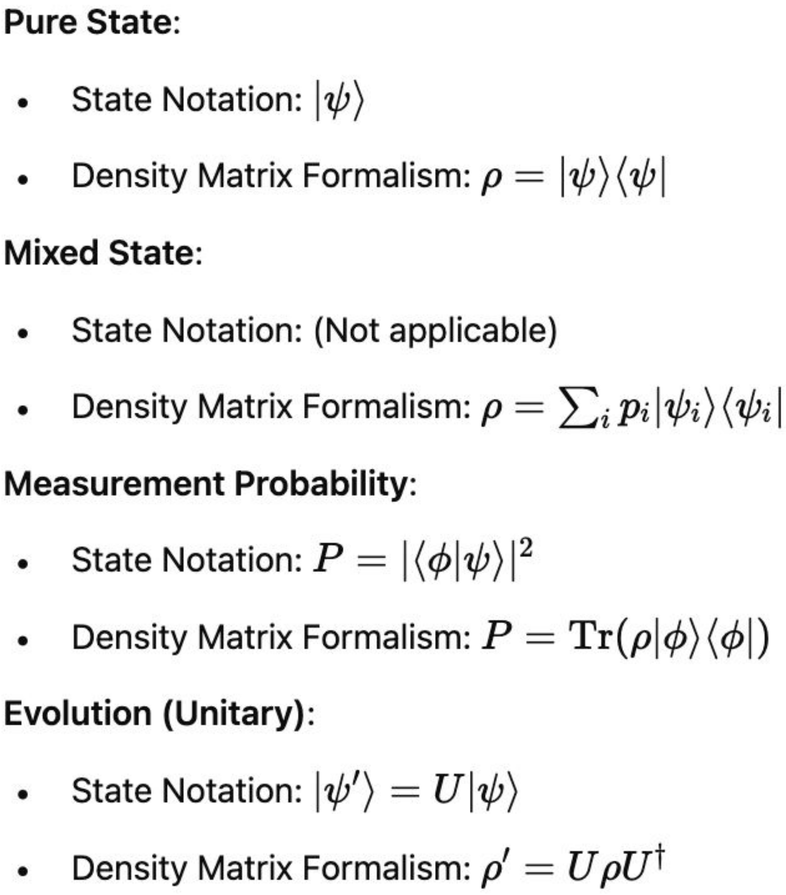
$$\mathrm{Tr}(\rho^2) < 1$$

Distinguishing pure and mixed:

Pure state: There will always be a basis in which you will get measurement outcome being the same values (so, 100%)

Mixed state will be always be less than 100% because its not

Formalism Comparison:



Pure State:

- State Notation: $|\psi\rangle$
- Density Matrix Formalism: $\rho = |\psi\rangle\langle\psi|$

Mixed State:

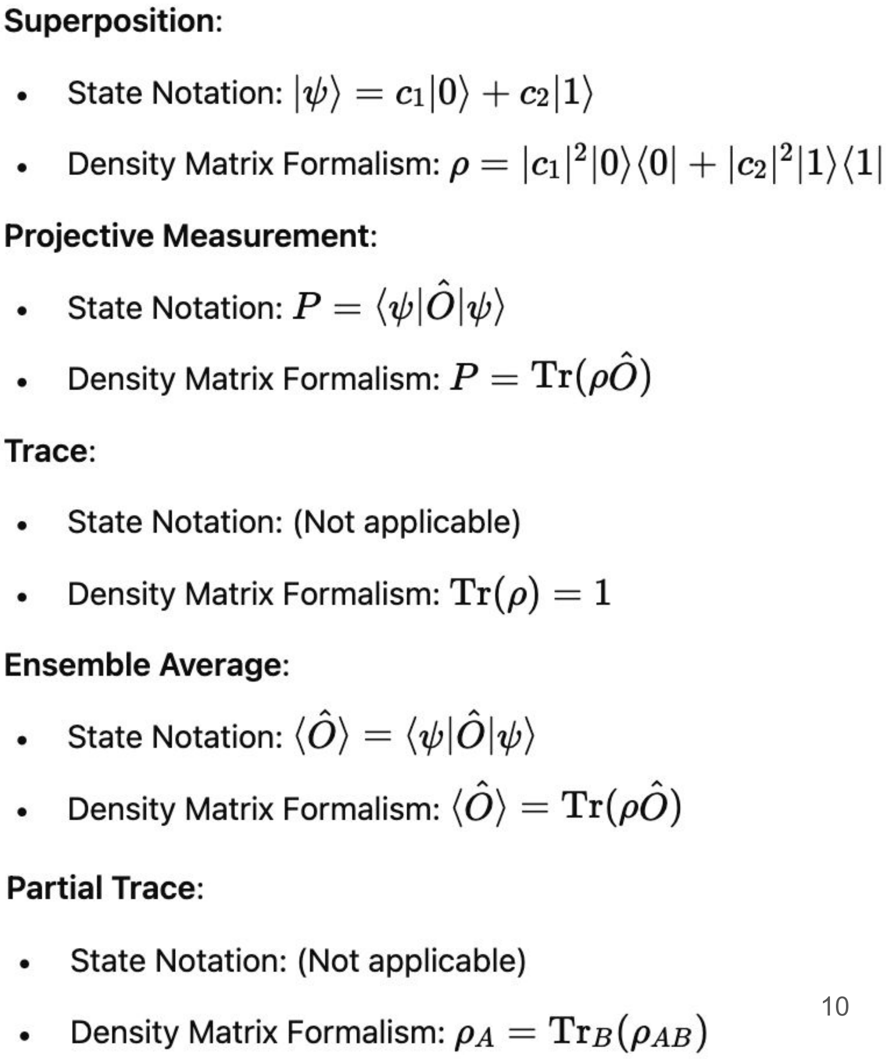
- State Notation: (Not applicable)
- Density Matrix Formalism: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

Measurement Probability:

- State Notation: $P = |\langle\phi|\psi\rangle|^2$
- Density Matrix Formalism: $P = \mathrm{Tr}(\rho|\phi\rangle\langle\phi|)$

Evolution (Unitary):

- State Notation: $|\psi'\rangle = U|\psi\rangle$
- Density Matrix Formalism: $\rho' = U\rho U^\dagger$



Superposition:

- State Notation: $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$
- Density Matrix Formalism: $\rho = |c_1|^2|0\rangle\langle 0| + |c_2|^2|1\rangle\langle 1|$

Projective Measurement:

- State Notation: $P = \langle\psi|\hat{O}|\psi\rangle$
- Density Matrix Formalism: $P = \mathrm{Tr}(\rho\hat{O})$

Trace:

- State Notation: (Not applicable)
- Density Matrix Formalism: $\mathrm{Tr}(\rho) = 1$

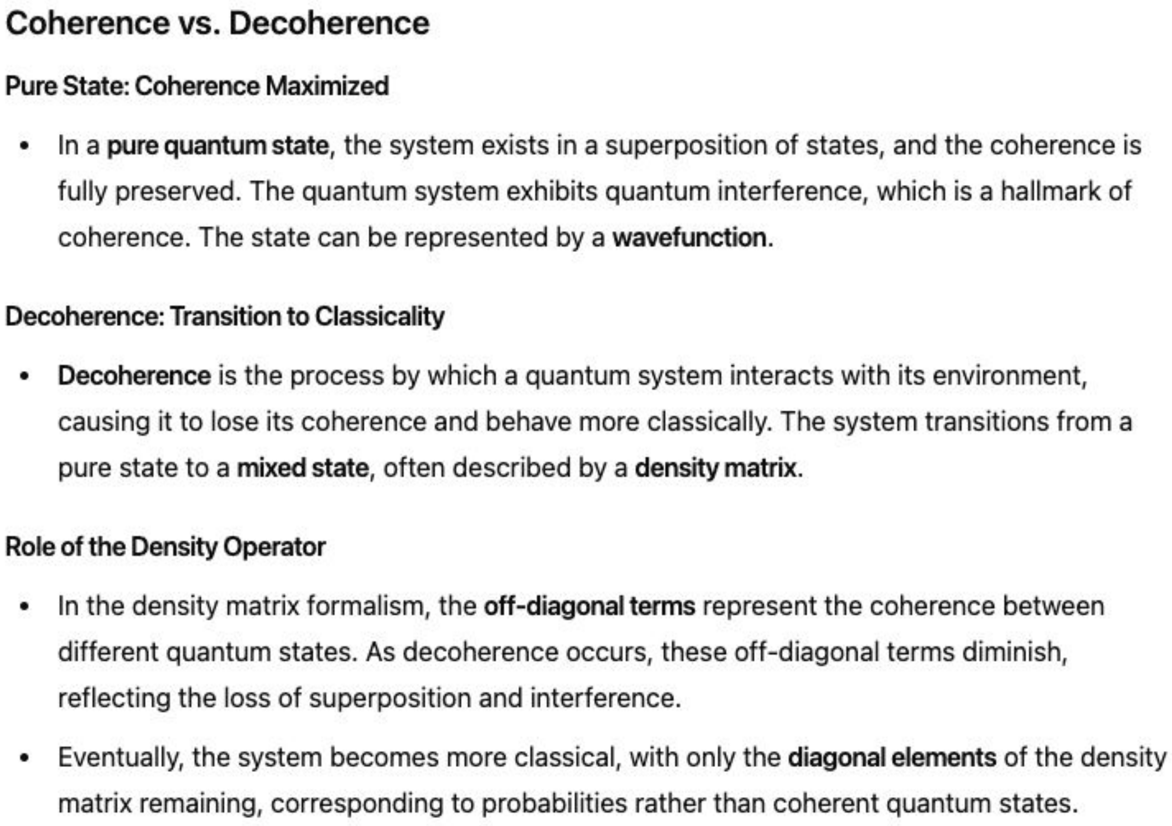
Ensemble Average:

- State Notation: $\langle\hat{O}\rangle = \langle\psi|\hat{O}|\psi\rangle$
- Density Matrix Formalism: $\langle\hat{O}\rangle = \mathrm{Tr}(\rho\hat{O})$

Partial Trace:

- State Notation: (Not applicable)
- Density Matrix Formalism: $\rho_A = \mathrm{Tr}_B(\rho_{AB})$

Coherence vs. Decoherence.



Coherence vs. Decoherence

Pure State: Coherence Maximized

- In a **pure quantum state**, the system exists in a superposition of states, and the coherence is fully preserved. The quantum system exhibits quantum interference, which is a hallmark of coherence. The state can be represented by a **wavefunction**.

Decoherence: Transition to Classicality

- **Decoherence** is the process by which a quantum system interacts with its environment, causing it to lose its coherence and behave more classically. The system transitions from a pure state to a **mixed state**, often described by a **density matrix**.

Role of the Density Operator

- In the density matrix formalism, the **off-diagonal terms** represent the coherence between different quantum states. As decoherence occurs, these off-diagonal terms diminish, reflecting the loss of superposition and interference.
- Eventually, the system becomes more classical, with only the **diagonal elements** of the density matrix remaining, corresponding to probabilities rather than coherent quantum states.

Effects.

Represents possible outcomes of a quantum measurement

- Each outcome is described by:

effect operator E_m

A “Positive Semi-Definite” Operator

$$\langle\psi|A|\psi\rangle \geq 0 \quad \text{for all} \quad |\psi\rangle$$

- Set $\{E_m\}$ for all possible outcomes:

“POVM”

Positive operator-valued Measurement

Useful for ***state discrimination***

“PVM”

Projection-Valued Measurement

- specific case of a POVM
- operators correspond to orthogonal projectors.
- do not necessarily correspond to the eigenstates of a particular observable
- may be of higher rank (i.e., could project onto subspaces rather than single states)

$$\{P_m\}$$

Completeness

$$\sum_m P_m = I$$

Orthogonality

$$P_m P_n = \delta_{mn} P_m$$

“Von Neumann Measurement”

- specific case of a PVM
- Operators are: rank-1, orthogonal, *that correspond to a **specific observable**.*
- measurement outcomes correspond to the **eigenstates** of the observable being measured, and the system **collapses** to one of those eigenstates.

Z-basis (Computational) : $P_0 = |0\rangle\langle 0|, \quad P_1 = |1\rangle\langle 1|$

X-basis (Superposition) : $P_+ = |+\rangle\langle +|, \quad P_- = |-\rangle\langle -|$

Y-basis (Superposition + i) : $P_i = |i\rangle\langle i|, \quad P_{-i} = |-i\rangle\langle -i|$

Effects 2

***Projective Measurements* (PVM)**

Completeness Relation: $\sum_i \hat{P}_i = I$

Forms a complete set of orthogonal projectors.
Every possible outcome is accounted for by one of the projectors.

Orthogonality: $\hat{P}_i\hat{P}_j = \delta_{ij}\hat{P}_i$

Orthogonality reflects the fact that measurement outcomes are mutually exclusive in projective measurements

Also,
(P_i)2 = (P_i)**

Positive Semi-Definite Operators: $\langle\psi|\hat{P}_i|\psi\rangle \geq 0$

$$\hat{P}_i > 0$$

⇒ eigenvalues are non-negative
⇒ ensures the probabilities derived from measurement outcomes are non-negative

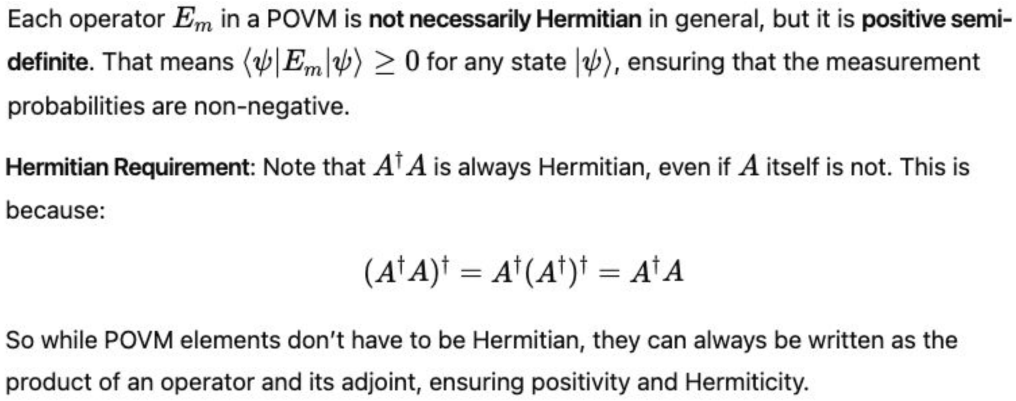
***Positive Operator-Valued Measurements* (POVM)**

POVMs allow for more general outcomes that do not necessarily correspond to eigenstates of observables

$$\sum_i \hat{E}_i = I$$

Orthogonality not necessary!

Each POVM element is **positive semi-definite operator!**



Each operator E_m in a POVM is **not necessarily Hermitian** in general, but it is **positive semi-definite**. That means $\langle\psi|E_m|\psi\rangle \geq 0$ for any state $|\psi\rangle$, ensuring that the measurement probabilities are non-negative.

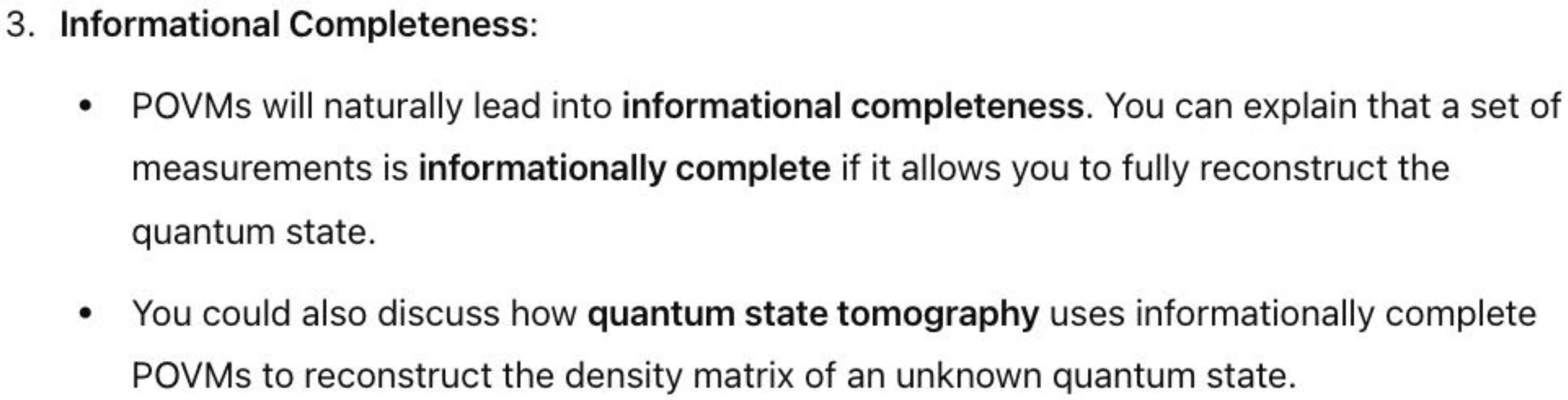
Hermitian Requirement: Note that $A^\dagger A$ is always Hermitian, even if A itself is not. This is because:

$$(A^\dagger A)^\dagger = A^\dagger(A^\dagger)^\dagger = A^\dagger A$$

So while POVM elements don't have to be Hermitian, they can always be written as the product of an operator and its adjoint, ensuring positivity and Hermiticity.

- PVMs return eigenvalues of the corresponding observable. When you measure, the system is projected onto one of the eigenstates, and the measurement outcome corresponds to that eigenstate.
- PVMs represent a special case of measurements where outcomes correspond to projectors onto orthogonal eigenstates.

Example & Difference of POVM, PVM, Von Neumann



3. **Informational Completeness**:

- POVMs will naturally lead into **informational completeness**. You can explain that a set of measurements is **informationally complete** if it allows you to fully reconstruct the quantum state.
- You could also discuss how **quantum state tomography** uses informationally complete POVMs to reconstruct the density matrix of an unknown quantum state.

Gleason's Theorem

For any separable **Hilbert space** $\mathcal{H}$ with dimension **greater than 2** (i.e., $\dim(\mathcal{H}) \geq 3$), any **measure** on the set of **projective measurements** (also known as **projection operators**) can be uniquely represented by a **density matrix** ρ.

The probability p of observing the system in a state corresponding to a projection operator ***P*** (which represents an observable) is given by:

$$p = \langle\psi|P|\psi\rangle$$

In the case of a pure state

*Gleason's Theorem shows that **any rule for assigning probabilities** to measurement outcomes must follow this form — that is, there is no other way to consistently assign probabilities to measurements other than the **<u>Born rule</u>** using a **density matrix** to represent quantum states.*

When the system is described by a **density matrix**, the probability *p* of measuring a specific outcome associated with a **projection operator *P*** (associated ith the measurement outcome you're interested in) is given by:

$$p = \mathrm{Tr}(\rho P)$$

$$\mathrm{Tr}(A) = \sum_i \langle i|A|i\rangle$$

Trace operation essentially sums over the contributions from each possible pure state in the ensemble, weighted by the classical probabilities
– shows how each pure state interacts with the measurement operator *P*

$$\rho = 0.5|\psi_1\rangle\langle\psi_1| + 0.5|\psi_2\rangle\langle\psi_2|$$

$$p = \mathrm{Tr}\left(0.5|\psi_1\rangle\langle\psi_1|P\right) + \mathrm{Tr}\left(0.5|\psi_2\rangle\langle\psi_2|P\right)$$

!!!!

Observables.

Observables = Matrices:

- Observables are ***Hermitian*** Operators

$$\hat{A} = \hat{A}^\dagger \longrightarrow$$

$\Rightarrow$ **all eigenvalues of the observable** are **real numbers**

(i.e. measurement number must be real)

Measuring observable $\hat{A}$ *projects* the system into one the *eigenstates* $|\psi_n\rangle$ with associated eigenvalue a_n

$$\hat{A}|\psi_n\rangle = a_n|\psi_n\rangle$$

Eigenvalue Equation!

Ex; 3x3 matrix

$$\hat{A} = \begin{pmatrix} a & b+ic & d+ie \\ b-ic & f & g+ih \\ d-ie & g-ih & k \end{pmatrix}$$

- *a, f, k are REAL*

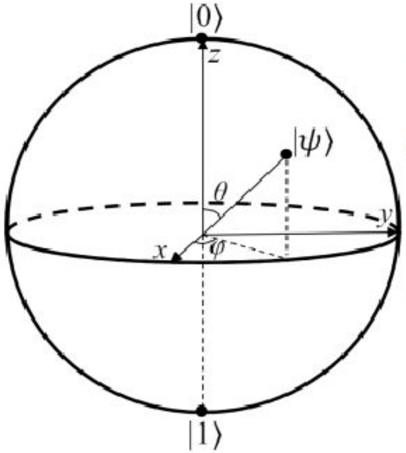
diagonal elements of a Hermitian matrix must be real

Basis Representation:

Gates = Matrices = Operators

(Qubits = Vectors = States)

- **X-Gate (NOT Gate):** Flips the qubit between 0 and 1 state
- **Z-Gate (Phase Flip):** Adds phase shift (a π - rotation about Z-axis)
- **Y-Gate**: Applies π- rotation around the Y-axis, combines bit + phase flip
- **Hadamard Gate:** Creates superpositions from computational basis states –i.e converts to +/- basis
- **S/T Gates**: Apply phase shifts
- **CNOT**: Entangles qubits



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

$\alpha = \cos\frac{\theta}{2}$

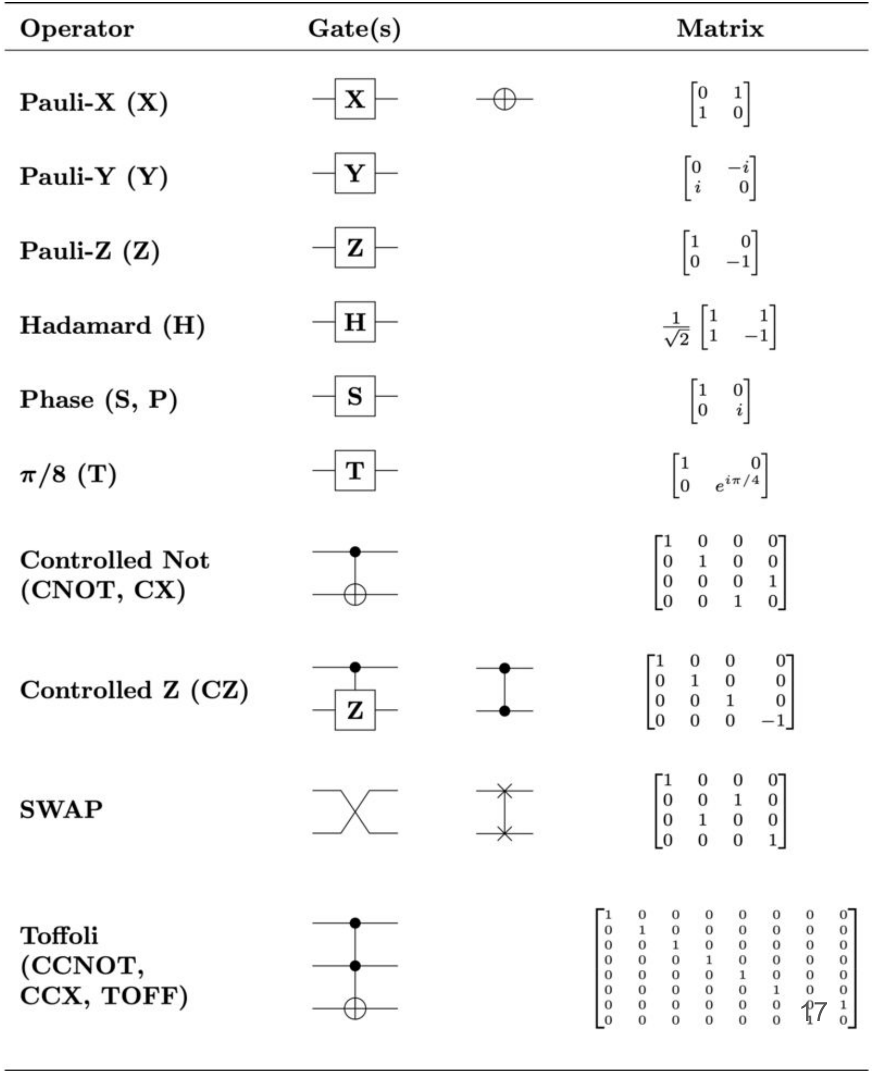
$\beta = e^{i\varphi}\sin\frac{\theta}{2}$

$\alpha|0\rangle + \beta|1\rangle \xrightarrow{X} \beta|0\rangle + \alpha|1\rangle$

$\alpha|0\rangle + \beta|1\rangle \xrightarrow{Z} \alpha|0\rangle - \beta|1\rangle$

$\alpha|0\rangle + \beta|1\rangle \xrightarrow{Y} \text{-}\beta i|0\rangle + \alpha i|1\rangle$

$\alpha|0\rangle + \beta|1\rangle \xrightarrow{H} \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$



Operator	Gate(s)		Matrix
Pauli-X (X)	X	⊕	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
Pauli-Y (Y)	Y		$\begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$
Pauli-Z (Z)	Z		$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$
Hadamard (H)	H		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$
Phase (S, P)	S		$\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$
$\pi/8$ (T)	T		$\begin{bmatrix}1 & 0\\0 & e^{i\pi/4}\end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$
Controlled Z (CZ)	Z		$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & -1\end{bmatrix}$
SWAP			$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$

More on Gates

Universality : *Universal Quantum Gate Set*

$R_x(\theta), R_y(\theta), R_z(\theta)\ P(\varphi)$ CNOT

{CNOT, *H*, *S*} + *T* gate

Toffoli gate + Hadamard

General Rotation about any arbitrary axis,

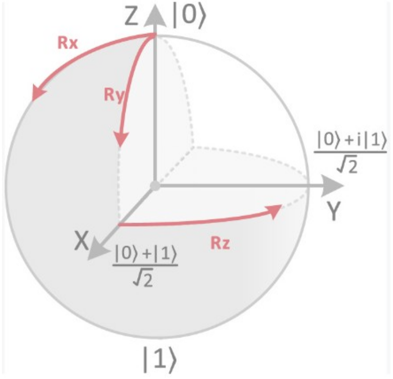
$$\hat{n} = (n_x, n_y, n_z)$$

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)}$$

σ_x, σ_y, and σ_z are the Pauli matrices

Rotate a qubit state by theta around *n*-axis,

$$|\psi(\theta)\rangle = e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}}|\psi(0)\rangle$$


Z
|0⟩
Rx
Ry
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
Y
X
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
Rz
|1⟩

rotates the state **around the Z-axis** by an angle *phi*

Phase Shift
Gate maps:

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

$|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\varphi}|1\rangle$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P(\pi)$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = P\left(\frac{\pi}{2}\right) = \sqrt{Z}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = P\left(\frac{\pi}{4}\right) = \sqrt{S} = \sqrt[4]{Z}$$

square root of the NOT gate is any gate U such that $U^2 = X$

√NOT gate twice is equivalent to applying the NOT gate once

Example:

***Pauli matrices** are used as generators of rotations for qubits:*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Rotation Operations for Spin-½ Systems (Qubits):

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_y = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = e^{-i\frac{\theta}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)}$$

$$e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)$$

$$\hat{n}\cdot\vec{\sigma} = n_x\sigma_x + n_y\sigma_y + n_z\sigma_z$$

$$R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$R_x(\theta) = \cos\left(\frac{\theta}{2}\right)(|0\rangle\langle 0| + |1\rangle\langle 1|) - i\sin\left(\frac{\theta}{2}\right)(|0\rangle\langle 1| + |1\rangle\langle 0|)$$

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

$$R_y(\theta) = \cos\left(\frac{\theta}{2}\right)(|0\rangle\langle 0| + |1\rangle\langle 1|) + \sin\left(\frac{\theta}{2}\right)(|1\rangle\langle 0| - |0\rangle\langle 1|)$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}}|0\rangle\langle 0| + e^{i\frac{\theta}{2}}|1\rangle\langle 1|$$

Example:

Pauli matrices *are used as generators of rotations for qubits:*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Computational Basis

$$H = \frac{1}{\sqrt{2}} \left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \right)$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

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

Superposition Basis

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

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H = \frac{1}{\sqrt{2}} \left(|0\rangle\langle +| + |1\rangle\langle -| \right)$$

$$H = \frac{1}{\sqrt{2}} \left(|+\rangle\langle +| + |-\rangle\langle -| \right)$$

$$H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{matrix} H|+\rangle = |+\rangle \\ H|-\rangle = |-\rangle \end{matrix}$$

Swap operator, S and T gates, explain CU

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x$$

Examples of Gate Combinations to know

Hadamard + CNOT = *entanglement*

Initialize: $|00\rangle$

$\Big\downarrow$ H

Superposition: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

$\Big\downarrow$ CNOT

Entanglement:* *(Bell Basis) $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Hadamard + Z = *Phase Flip Superposition*

H = Superposition: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

$\Big\downarrow$ Z

Phase Flip: $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$HZH = \sigma_X$$

Grover's Oracle

$$U_s = H^{\otimes n} Z H^{\otimes n}$$

$$H\sqrt{X}\,H = \sqrt{Z} = S$$

Hadamard Transform:

$$\bigotimes_0^{n-1}(H|0\rangle) = \frac{1}{\sqrt{2^n}}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix} = \frac{1}{\sqrt{2^n}}\Big(|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle\Big) = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$$

$$\mathrm{SWAP} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{bmatrix}$$

Hadamard + Phase (S, T) = *Phase Kickback*

Introduces controlled phase shifts between basis states (phase rotations .critical for interference) Used in phase estimation in Shor’s factoring algorithm, Quantum Fourier Transform (QFT)...

Mathematics Slide

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \longrightarrow |\psi(t)\rangle = e^{-\frac{i}{\hbar}Ht}|\psi(0)\rangle$$

$$U(t) = e^{-i\hat{H}t/\hbar}$$

Taylor Series:

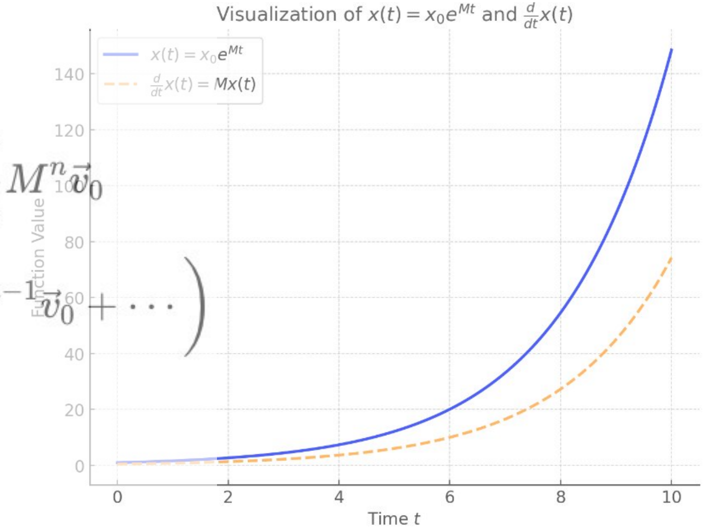
$$e^{Mt} = \sum_{n=0}^{\infty}\frac{(Mt)^n}{n!} = I + tM + \frac{t^2}{2!}M^2 + \cdots \longrightarrow e^{-\frac{i}{\hbar}Ht} = I - \frac{i}{\hbar}Ht + \frac{1}{2!}\left(-\frac{i}{\hbar}Ht\right)^2 + \cdots$$

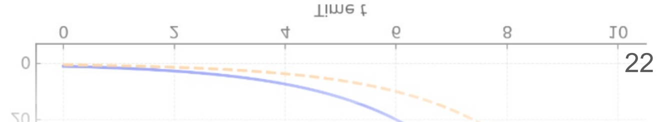
Differential Equation: $\vec{v}(t) = e^{Mt}\vec{v}_0$

$$e^{tM}\vec{v}_0 = t^0M^0\vec{v}_0 + t^1M^1\vec{v}_0 + \frac{t^2}{2}M^2\vec{v}_0 + \frac{t^3}{6}M^3\vec{v}_0 + \cdots + \frac{t^n}{n!}M^n\vec{v}_0$$

$$\frac{d}{dt}e^{tM}\vec{v}_0 = M\left(t^0M^0\vec{v}_0 + t^1M^1\vec{v}_0 + \frac{t^2}{2}M^2\vec{v}_0 + \cdots + \frac{t^{n-1}}{(n-1)!}M^{n-1}\vec{v}_0 + \cdots\right)$$

$$\frac{d}{dt}e^{tM}\vec{v}_0 = M\left(e^{tM}\vec{v}_0\right)$$





Incompatibility

Two observables are said to be **incompatible** if they ***do not commute***

$$[\hat{A},\hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} \begin{cases} \textit{Commutes} & [\hat{A},\hat{B}] = 0 \\ \textit{Does not commute} & [\hat{A},\hat{B}] \neq 0 \end{cases}$$

measures the extent to which the two operators fail to commute with each other (i.e. order of their measuring matters)

$\Rightarrow$ cannot be measured simultaneously with arbitrary precision

Note:
*Operators that commute with each other share a common **set of eigenstates**, meaning they can be measured simultaneously.*

Heisenberg Uncertainty Principle

... gives a lower bound on the product of the uncertainties (or *standard deviations*) in measuring two observables simultaneously

$$\Delta A \cdot \Delta B \geq \frac{1}{2} \left| \langle [\hat{A},\hat{B}] \rangle \right|$$

- ΔA is the **uncertainty** in observable A, defined as $\Delta A = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}$.
- ΔB is the **uncertainty** in observable B.
- $[\hat{A},\hat{B}]$ is the **commutator** of the two operators $\hat{A}$ and $\hat{B}$.
- $\langle [\hat{A},\hat{B}] \rangle$ is the **expectation value** of the commutator in a given quantum state.

$$[\hat{x},\hat{p}] = \hat{x}\hat{p} - \hat{p}\hat{x} = i\hbar \quad \Longrightarrow \quad \Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

Informational Completeness

A **set of measurements is informationally complete** if it provides enough information to fully reconstruct the quantum state.

Example:
Projective Measurements on Mutually Unbiased Bases (MUBs)

For qubits, measurements in **three orthogonal bases** (z, x, y) to provide complete information about the quantum state

$$\rho = \frac{1}{2}\left(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\right)$$

I is identity matrix

Pauli Matrices

$\vec{r}$ Is the bloch vector: r_x, r_y, r_z

crucial in quantum state tomography, where multiple measurements on different bases can fully determine the quantum state.

for informational completeness, we need to measure different observables, often represented by incompatible ones

CHANNELS

Mathematical Definition

A quantum channel is a mathematical map $\mathcal{E}$

that takes a density matrix ρ

and transforms it into a new density matrix $\mathcal{E}(\rho)$

Definition:

A quantum channel models the evolution of a quantum system under the influence of noise or interaction with an environment

Purpose:

to understand how a quantum state (represented by a density matrix) changes when subjected to this noise or interaction.

Properties:

1. **Completely Positive**
2. **Trace Preserving**

A completely positive, trace-preserving map can be described as:

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger$$

K_i Kraus Operators,
describing specific action of the channel

$$\sum_i K_i^\dagger K_i = I$$

A quantum channel can be seen as a "pipeline" that transfers quantum states (or information) from one system to another, while possibly subjecting the state to noise, decoherence, or interaction with an environment.

Complete-Positive (CP)

- if it ensures the positivity of density matrices even when it acts on part of a larger entangled system

- Positivity Condition: $\mathcal{E}(\rho) \geq 0$

- Complete Positivity:

If you extend the channel Epsilon to an Identity operation on an auxiliary channel system, the output will still preserve positivity.

$$(\mathbb{I} \otimes \mathcal{E})(\rho_{AB}) \geq 0$$

Extended system

Auxiliary system

Trace-Preserving (TP)

- ensures that the quantum state remains properly normalized after the channel acts on it:

$$\mathrm{Tr}(\mathcal{E}(\rho)) = 1$$

- In terms of Kraus operators:

$$\sum_i K_i^\dagger K_i = I$$

Trace preserving is like completeness relation–its so it doesn't "lose probability"

Types/Examples of Channels

State after applied channel

$$\rho' = \sum_i K_i \rho K_i^\dagger$$

Dephasing Channel: This type of channel causes a system to lose coherence in its phase. Essentially, it destroys the relative phase information between quantum states, while keeping their populations (probabilities) unchanged.

For a single qubit, he channel can be described using the following Kraus operators:

$$K_0 = \sqrt{1-p}\, I, \quad K_1 = \sqrt{p}\, Z$$

where p is the probability of a phase flip, I is the identity matrix, and Z is the Pauli-Z matrix

The action of the dephasing channel on a density matrix ρ is given by:

$$\rho' = (1-p)\rho + pZ\rho Z$$

Amplitude Damping Channel: This channel models the loss of energy in a quantum system, typically represented in systems that interact with their environment (like photon loss or spontaneous emission in quantum optics).

This channel tends to map excited states to ground states over time, leading to energy loss.

$$K_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad K_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

γ is the probability of the system losing energy (damping rate)

The action of the amplitude damping channel on a density matrix ρ is given by:

$$\rho' = K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger$$

Depolarizing Channel: In this channel, the quantum system becomes more mixed over time. This channel acts to bring the quantum state closer to a maximally mixed state, meaning that the system loses any preference for being in a particular quantum state and becomes maximally disordered.

The depolarizing channel can be seen as adding random noise to a quantum system.

For a qubit, the depolarizing channel acts as:

$$\rho' = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

Probability of bit-flip occurring (i.e. error)

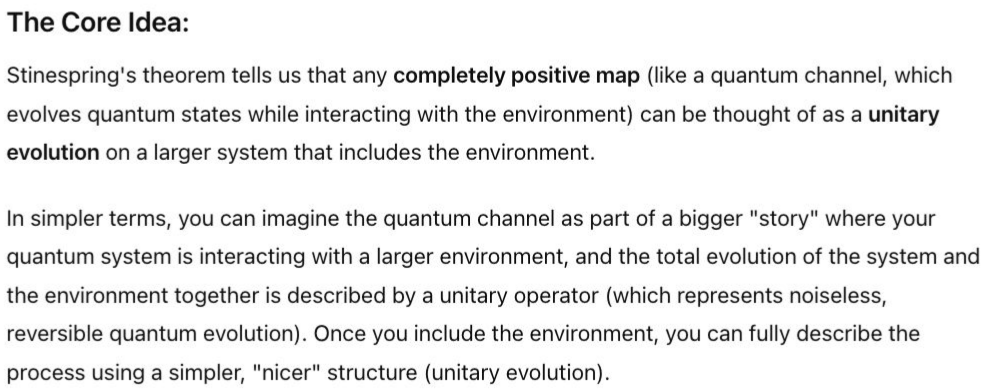
Entanglement-breaking Channels: These channels completely destroy the entanglement between quantum states. Once a quantum state passes through such a channel, it no longer holds any quantum correlations with other states, making it completely classical.

Bit-flip Channel:

$$B(\rho) = \pi X \rho X^\dagger + (1-\pi)\rho$$

Stinespring’s Theorem

Stinespring’s theorem asserts that every completely positive map can be represented as **unitary evolution** on a **larger Hilbert space** (the system plus environment), followed by a **partial trace** over the environment. This result is foundational because it links noisy, potentially irreversible quantum evolutions to a deterministic, reversible evolution in a larger context.

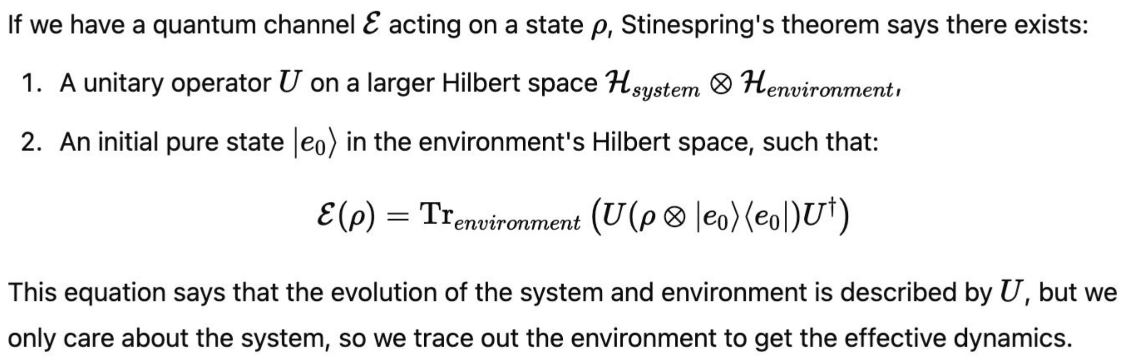


The Core Idea:

Stinespring's theorem tells us that any **completely positive map** (like a quantum channel, which evolves quantum states while interacting with the environment) can be thought of as a **unitary evolution** on a larger system that includes the environment.

In simpler terms, you can imagine the quantum channel as part of a bigger "story" where your quantum system is interacting with a larger environment, and the total evolution of the system and the environment together is described by a unitary operator (which represents noiseless, reversible quantum evolution). Once you include the environment, you can fully describe the process using a simpler, "nicer" structure (unitary evolution).

I.e. Stinesprings Theorem helps model quantum noise as a **unitary evolution** on a larger system (system + environment), followed by tracing out the environment – i.e. even if we focus on a noisy, open system, we can view the overall system (including the environment) as undergoing **unitary evolution**. The noise is a result of our lack of access to the environment, and this is mathematically modeled by tracing out the environmental degrees of freedom.



If we have a quantum channel $\mathcal{E}$ acting on a state ρ, Stinespring's theorem says there exists:

1. A unitary operator U on a larger Hilbert space $\mathcal{H}_{system} \otimes \mathcal{H}_{environment}$,
2. An initial pure state $|e_0\rangle$ in the environment's Hilbert space, such that:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{environment}\left(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right)$$

This equation says that the evolution of the system and environment is described by U, but we only care about the system, so we trace out the environment to get the effective dynamics.

Imagine your quantum system as a ship in a sea of waves (the environment). On its own, the ship is rocked and battered by the waves (noise), and its trajectory looks complicated. But if you zoom out and consider the whole ocean (the system + environment), the ship’s movement and the waves are part of a larger, coherent motion.
This is what **Stinespring’s theorem** shows: even noisy processes can be viewed as part of a larger, unitary evolution when you include the environment.

Shannon Information Theory

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

Shannon's Entropy

For a discrete random variable *X*, which can take on values $x_1, x_2, \ldots, x_n$ with corresponding probabilities $p(x_1), p(x_2), \ldots, p(x_n)$

Measures the **uncertainty** or **information content** of a random variable or a message.
i.e: quantifies how much "surprise" or "uncertainty" there is in the outcomes of a probabilistic system

- Highly probable ⇒ provides **little new information** = *low entropy*
- Highly uncertain ⇒ provides **lots of new information** = *high entropy*

$$\boxed{\log_2(8) = 3}$$

Shannon's entropy gives a way to quantify the "average" amount of information produced by a random process.

PROPERTIES

$H(X) \geq 0$ is always non-negative because probabilities are between 0 and 1

And minimal entropy when outcome is certain

Maximal Entropy = when all outcomes are equally probable (maximum uncertainty)

$$\Longrightarrow \quad p(x_i) = \frac{1}{n} \text{ for all } i \quad \Longrightarrow \quad H(X) = \log_2 n$$

$$b^y = x$$
$$\log_b(x) = y$$

continued….

Example: $H(\text{coin flip}) = -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right) = 1 \text{ bit}$

quantum-analogue,

Von Neumann Entropy

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$$

Density matrix

Measures the **mixedness** of a quantum state.

– A *pure state* has entropy 0

– A *mixed state* (which represents uncertainty about the quantum state) has positive entropy.

quantum systems, where uncertainty arises due to the mixedness of quantum states

$$S(\rho_A) = -\mathrm{Tr}(\rho_A \log_2 \rho_A)$$

- If $S(\rho_A) = 0$, System is **not entangled**, and subsystem *A is in a pure state*
- If $S(\rho_A) > 0$, System is **entangled**, meaning that the state of subsystem *A* depends on state of subsystem *B* – larger the entropy, greater the entanglement

Holevo bound:
Know that quantum systems can encode classical information, and the **Holevo bound** gives an upper limit on the amount of classical information that can be extracted from quantum states

Entanglement entropy: measures the degree of entanglement between subsystems of a q- system

For bipartite quantum system, the entanglement entropy is the Von Neumann entropy of the reduced density matrix of one subsystem. –i.e. how much information you gain about one subsystem by observing the other subsystem.

Quantum Relative Entropy: measures the "distance" between two quantum states

$$S(\rho||\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma))$$

Seperable States vs. Product States

Product State: ***no entanglement*** *between them.*

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \xrightarrow{\textit{Pure product state}} \rho_A \otimes \rho_B$$

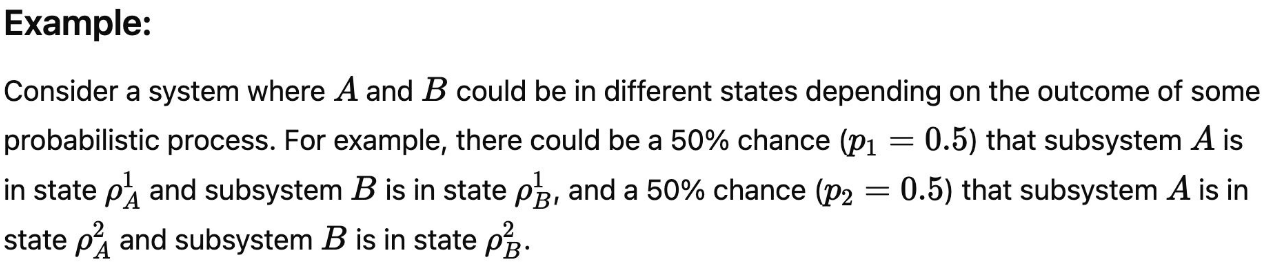
A **product state** is a quantum state of a composite system that can be written as a tensor product of the states of individual subsystems.

Seperable State: *separable states are* ***not entangled***

A **separable state** is a state that is **not entangled**, but it may not necessarily be a pure product state. It can be written as a **convex combination** (i.e., probabilistic mixture) of product states.

$$\rho_{AB} = \sum_i p_i \left(\rho_A^i \otimes \rho_B^i\right)$$

separable states can be **classical mixtures** of more than one product state



Example:

Consider a system where A and B could be in different states depending on the outcome of some probabilistic process. For example, there could be a 50% chance ($p_1 = 0.5$) that subsystem A is in state ρ_A^1 and subsystem B is in state ρ_B^1, and a 50% chance ($p_2 = 0.5$) that subsystem A is in state ρ_A^2 and subsystem B is in state ρ_B^2.

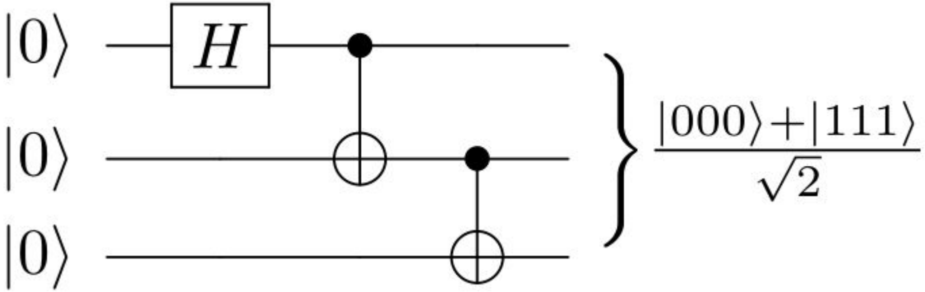
Thus, the total density matrix for the system would be:

$$\rho_{AB} = 0.5 \cdot (\rho_A^1 \otimes \rho_B^1) + 0.5 \cdot (\rho_A^2 \otimes \rho_B^2)$$

In this example, iii takes two values, 1 and 2, corresponding to the two possible product states.

Entangled States

GHZ–
"bell state in 3 particle entanglement"



The W state is the representative of one of the two non-biseparable classes of three-qubit states, the other being GHZ

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

Bell Basis:

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

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

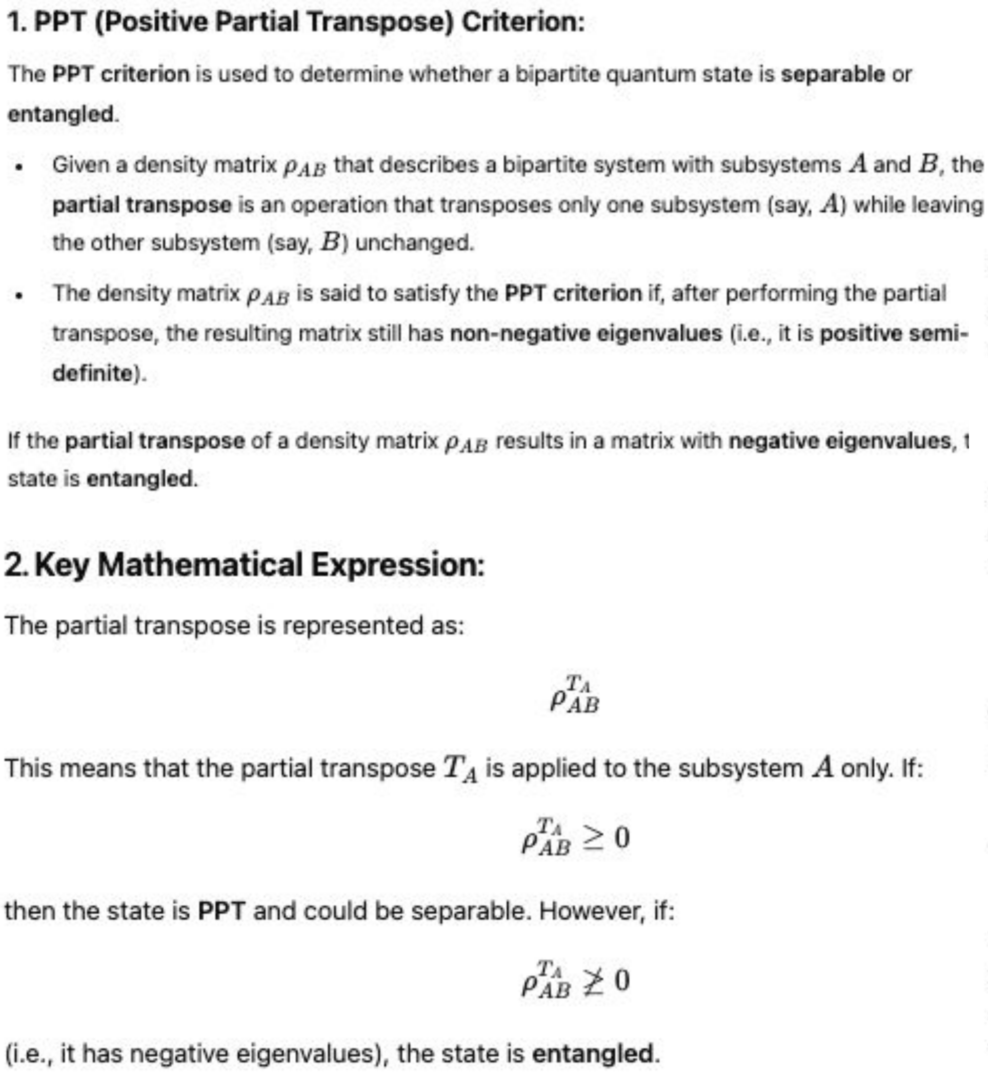
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Maximally entangled

PPT Criteria

Checks for entanglement



1. PPT (Positive Partial Transpose) Criterion:

The **PPT criterion** is used to determine whether a bipartite quantum state is **separable** or **entangled**.

- Given a density matrix ρ_{AB} that describes a bipartite system with subsystems A and B, the **partial transpose** is an operation that transposes only one subsystem (say, A) while leaving the other subsystem (say, B) unchanged.
- The density matrix ρ_{AB} is said to satisfy the **PPT criterion** if, after performing the partial transpose, the resulting matrix still has **non-negative eigenvalues** (i.e., it is **positive semi-definite**).

If the **partial transpose** of a density matrix ρ_{AB} results in a matrix with **negative eigenvalues**, t state is **entangled**.

2. Key Mathematical Expression:

The partial transpose is represented as:

$$\rho_{AB}^{T_A}$$

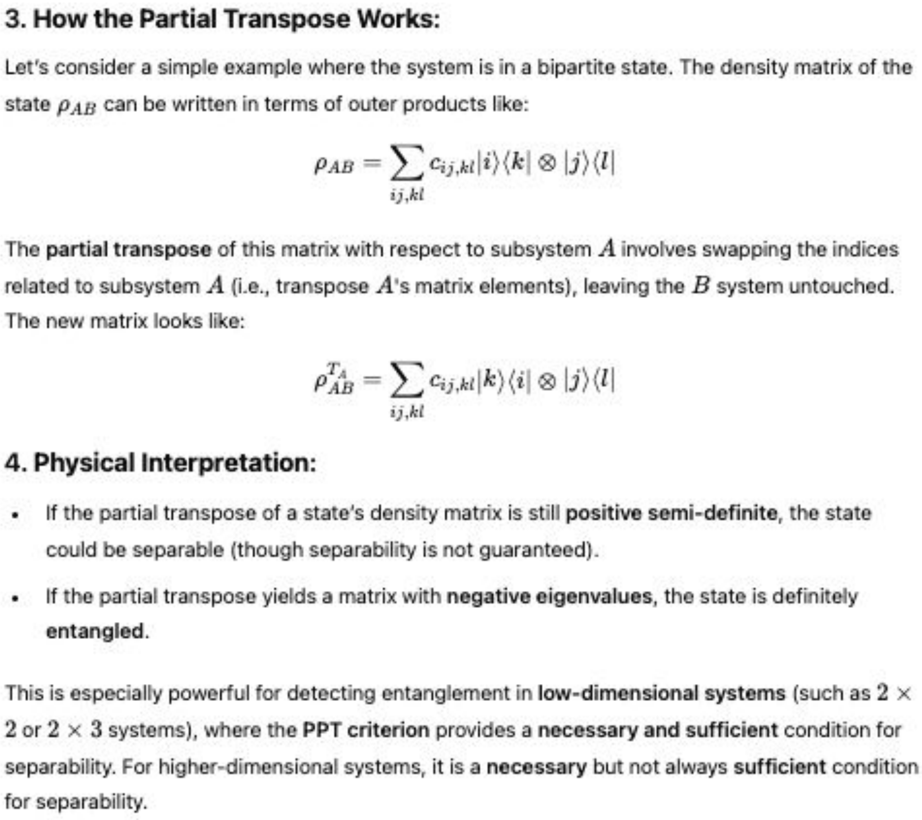
This means that the partial transpose T_A is applied to the subsystem A only. If:

$$\rho_{AB}^{T_A} \geq 0$$

then the state is **PPT** and could be separable. However, if:

$$\rho_{AB}^{T_A} \ngeq 0$$

(i.e., it has negative eigenvalues), the state is **entangled**.



3. How the Partial Transpose Works:

Let's consider a simple example where the system is in a bipartite state. The density matrix of the state ρ_{AB} can be written in terms of outer products like:

$$\rho_{AB} = \sum_{ij,kl} c_{ij,kl} |i\rangle\langle k| \otimes |j\rangle\langle l|$$

The **partial transpose** of this matrix with respect to subsystem A involves swapping the indices related to subsystem A (i.e., transpose A's matrix elements), leaving the B system untouched. The new matrix looks like:

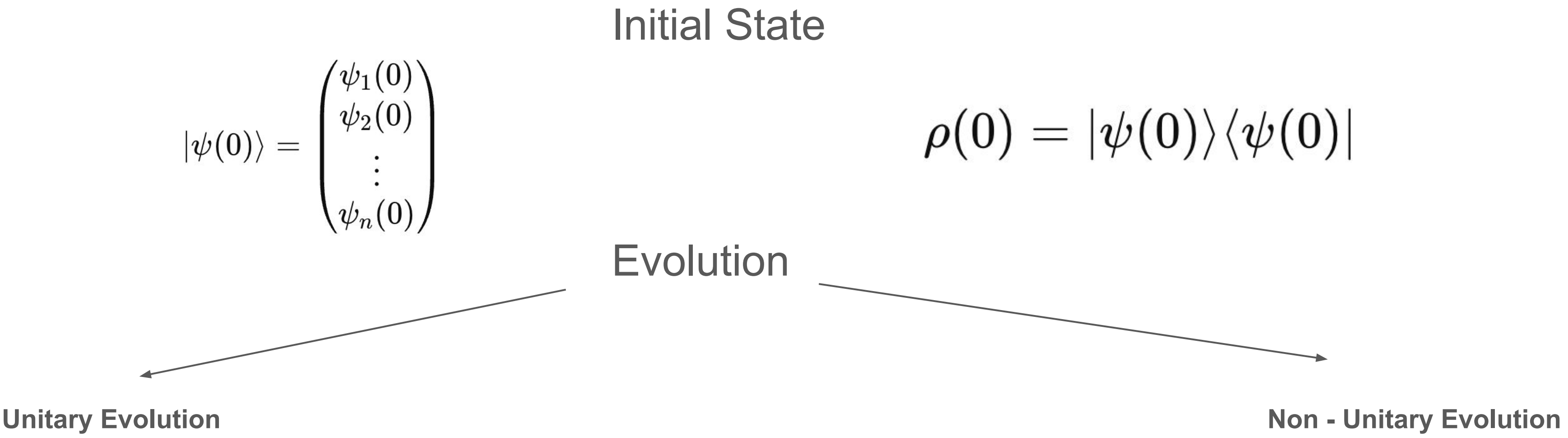
$$\rho_{AB}^{T_A} = \sum_{ij,kl} c_{ij,kl} |k\rangle\langle i| \otimes |j\rangle\langle l|$$

4. Physical Interpretation:

- If the partial transpose of a state's density matrix is still **positive semi-definite**, the state could be separable (though separability is not guaranteed).
- If the partial transpose yields a matrix with **negative eigenvalues**, the state is definitely **entangled**.

This is especially powerful for detecting entanglement in **low-dimensional systems** (such as 2×2 or 2×3 systems), where the **PPT criterion** provides a **necessary and sufficient** condition for separability. For higher-dimensional systems, it is a **necessary** but not always **sufficient** condition for separability.

Flowchart for Unitary vs Non-Unitary Evolution:



Initial State

$$|\psi(0)\rangle = \begin{pmatrix} \psi_1(0) \\ \psi_2(0) \\ \vdots \\ \psi_n(0) \end{pmatrix}$$

$$\rho(0) = |\psi(0)\rangle\langle\psi(0)|$$

Evolution

Unitary Evolution

- State evolves according to the Schrödinger equation
- State remains *pure*, no information is lost.

Non - Unitary Evolution

- State evolves according to the Lindblad equation
- State is affected by environmental interactions (e.g., noise), leading to decoherence or loss of quantum coherence.

Choi-Jamiolkowsi Isomporphism

nahh…

Time Evolution.

- For a *closed system*, time evolution of the state is governed by **Schrödinger's equation**:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle$$

Unitary Evolution: $U(t) = e^{-i\hat{H}t/\hbar}$

- **Properties**: Norm-preserving, deterministic, reversible, no information loss

$\hat{L}_i$ Lindblad Operators:

- For an *open system*, they evolve according to **Lindblad Equation**:

$$\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[\hat{H},\rho(t)] + \sum_i\left(\hat{L}_i\rho(t)\hat{L}_i^\dagger - \frac{1}{2}\{\hat{L}_i^\dagger\hat{L}_i,\rho(t)\}\right)$$

Non - Unitary Evolution:

- **Properties**: Norm is generally not preserved, irreversible, information loss (decoherence)

Lindblad Eqn models **Markovian noise**: the system has no memory of past interactions.

Continuous vs. Discrete Pt. 1

***Continuous** spectrum of eigenvalues,
and set of eigenstates*

Position Operator ($\hat{x}$)

$$\hat{x}|x\rangle = x|x\rangle$$

“infinite dimensional” matrices & vectors

$$\hat{x} = \begin{pmatrix} x_1 & 0 & 0 & \dots \\ 0 & x_2 & 0 & \dots \\ 0 & 0 & x_3 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\hat{x}\psi(x) = x\psi(x)$$

$\psi(x)$ → **“wavefunction”**

$$\psi(x) = \langle x|\psi\rangle$$

$$\langle x|\hat{x}|x'\rangle = x\delta(x - x')$$

$$\langle p|\hat{p}|p'\rangle = p\delta(p - p')$$

Example: **free particles** (not bound in a potential well)

Continuous vs. Discrete Pt. 2

Continuous *spectrum of eigenvalues,*
and set of eigenstates

Position Operator ($\hat{x}$)

$$\hat{x}|x\rangle = x|x\rangle$$

$$\hat{x} = \begin{pmatrix} x_1 & 0 & 0 & \dots \\ 0 & x_2 & 0 & \dots \\ 0 & 0 & x_3 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

“infinite dimensional” matrices & vectors

$$\hat{x}\psi(x) = x\psi(x)$$

$\psi(x)$ → **“wavefunction”**

$$\psi(x) = \langle x|\psi\rangle$$

$$\langle x|\hat{x}|x'\rangle = x\delta(x - x')$$

$$\langle p|\hat{p}|p'\rangle = p\delta(p - p')$$

Example: **free particles** (not bound in a potential well)

Continuous Case

- **State**:

$$|\psi\rangle = \int_{-\infty}^{\infty} \psi(x)|x\rangle \, dx$$

- **Wavefunction**:

$$\psi(x) = \langle x|\psi\rangle$$

- **Orthogonality**:

$$\langle x|x'\rangle = \delta(x - x')$$

- **Normalization**:

$$\int_{-\infty}^{\infty} |\psi(x)|^2 \, dx = 1$$

- **Basis Change (Position to Momentum)**:

$$\psi(p) = \frac{1}{\sqrt{2\pi\hbar}} \int_{-\infty}^{\infty} e^{-ipx/\hbar}\psi(x) \, dx$$

Discrete Case

- **State**:

$$|\psi\rangle = \sum_i \psi_i|x_i\rangle$$

- **Wavefunction**:

$$\psi_i = \langle x_i|\psi\rangle$$

- **Orthogonality**:

$$\langle x_i|x_j\rangle = \delta_{ij}$$

- **Normalization**:

$$\sum_i |\psi_i|^2 = 1$$

- **Basis Change (Discrete)**:

$$\psi_i = \sum_n U_{in} c_n$$

Schrodinger Equation:

Time Dependent

$$i\hbar\frac{d}{dt}\psi(t) = \hat{H}\psi(t)$$

Time In-Dependent

$$\hat{H}\psi(x) = E\psi(x)$$

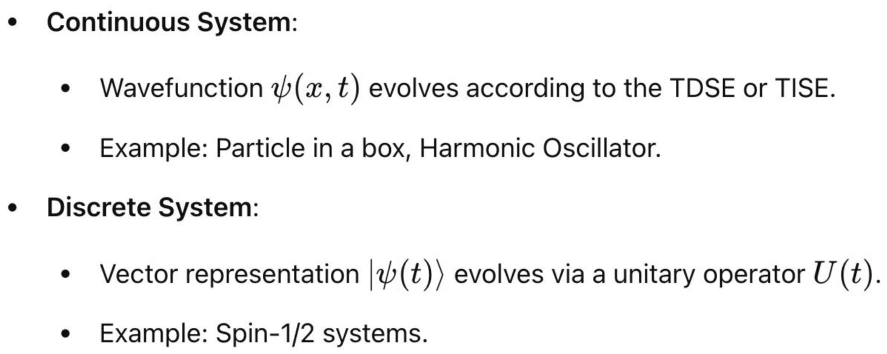
Continuous

$$\psi(t) = e^{-i\hat{H}t/\hbar}\psi(0)$$

$$i\hbar\frac{\partial}{\partial t}\psi(x,t) = \hat{H}\psi(x,t)$$

$$\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[\hat{H},\rho(t)]$$

Discrete



- **Continuous System**:
  - Wavefunction $\psi(x,t)$ evolves according to the TDSE or TISE.
  - Example: Particle in a box, Harmonic Oscillator.
- **Discrete System**:
  - Vector representation $|\psi(t)\rangle$ evolves via a unitary operator $U(t)$.
  - Example: Spin-1/2 systems.

Examples

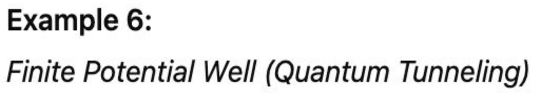
Example 1:
Infinite Potential Well (Particle in a Box)

Example 2:
Quantum Harmonic Oscillator

Example 3:
Free Particle (Time-Dependent Case)

Example 4:
Spin-1/2 Particle (Discrete System)

Example 5:
Quantum Scattering (Barrier Problem)

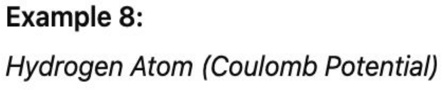


Example 6:

Finite Potential Well (Quantum Tunneling)

Example 7:

Quantum Harmonic Oscillator in Three Dimensions



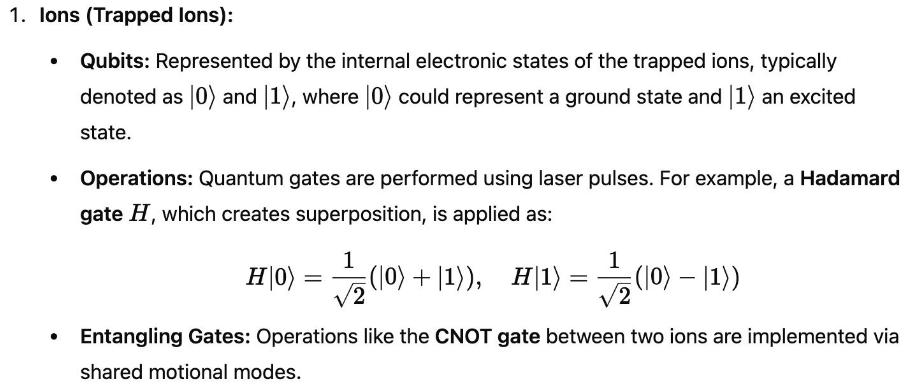
Example 8:

Hydrogen Atom (Coulomb Potential)

APPLICATIONS

(algorithms, implementation etc.)

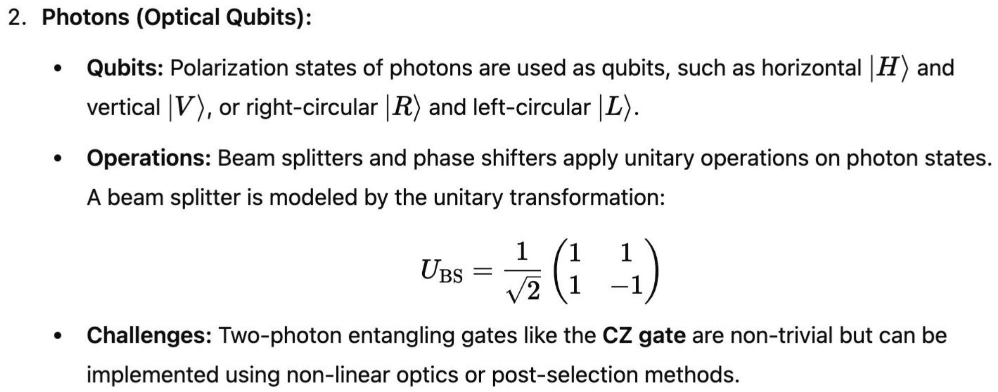
Implementation



1. **Ions (Trapped Ions):**
   - **Qubits:** Represented by the internal electronic states of the trapped ions, typically denoted as $|0\rangle$ and $|1\rangle$, where $|0\rangle$ could represent a ground state and $|1\rangle$ an excited state.
   - **Operations:** Quantum gates are performed using laser pulses. For example, a **Hadamard gate** H, which creates superposition, is applied as:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

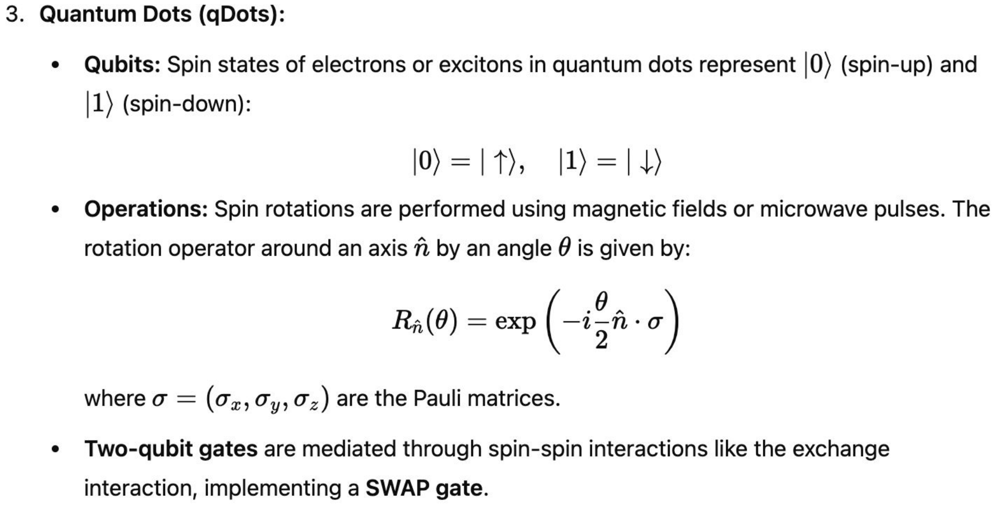
   - **Entangling Gates:** Operations like the **CNOT gate** between two ions are implemented via shared motional modes.



2. **Photons (Optical Qubits):**
   - **Qubits:** Polarization states of photons are used as qubits, such as horizontal $|H\rangle$ and vertical $|V\rangle$, or right-circular $|R\rangle$ and left-circular $|L\rangle$.
   - **Operations:** Beam splitters and phase shifters apply unitary operations on photon states. A beam splitter is modeled by the unitary transformation:

$$U_{\text{BS}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

   - **Challenges:** Two-photon entangling gates like the **CZ gate** are non-trivial but can be implemented using non-linear optics or post-selection methods.



3. **Quantum Dots (qDots):**
   - **Qubits:** Spin states of electrons or excitons in quantum dots represent $|0\rangle$ (spin-up) and $|1\rangle$ (spin-down):

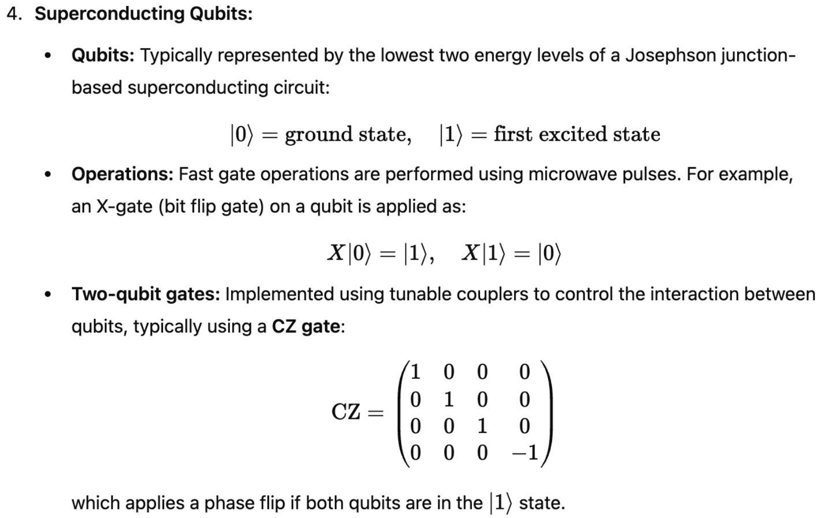
$$|0\rangle = |\uparrow\rangle, \quad |1\rangle = |\downarrow\rangle$$

   - **Operations:** Spin rotations are performed using magnetic fields or microwave pulses. The rotation operator around an axis $\hat{n}$ by an angle θ is given by:

$$R_{\hat{n}}(\theta) = \exp\left(-i\frac{\theta}{2}\hat{n}\cdot\sigma\right)$$

   where $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices.

   - **Two-qubit gates** are mediated through spin-spin interactions like the exchange interaction, implementing a **SWAP gate**.



4. **Superconducting Qubits:**
   - **Qubits:** Typically represented by the lowest two energy levels of a Josephson junction-based superconducting circuit:

$$|0\rangle = \text{ground state}, \quad |1\rangle = \text{first excited state}$$

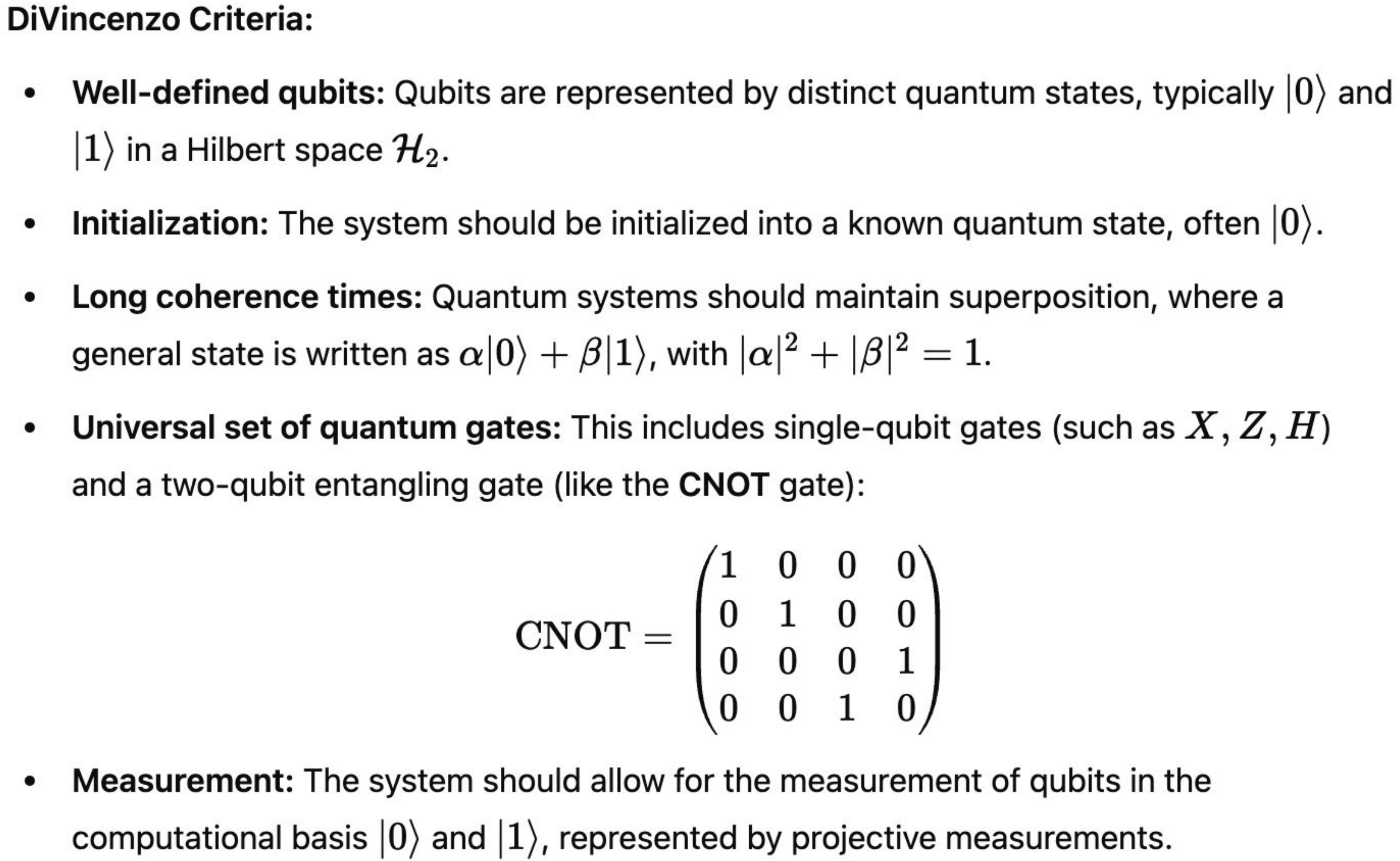
   - **Operations:** Fast gate operations are performed using microwave pulses. For example, an X-gate (bit flip gate) on a qubit is applied as:

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$$

   - **Two-qubit gates:** Implemented using tunable couplers to control the interaction between qubits, typically using a **CZ gate**:

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

   which applies a phase flip if both qubits are in the $|1\rangle$ state.



DiVincenzo Criteria:

- **Well-defined qubits:** Qubits are represented by distinct quantum states, typically $|0\rangle$ and $|1\rangle$ in a Hilbert space $\mathcal{H}_2$.
- **Initialization:** The system should be initialized into a known quantum state, often $|0\rangle$.
- **Long coherence times:** Quantum systems should maintain superposition, where a general state is written as $\alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$.
- **Universal set of quantum gates:** This includes single-qubit gates (such as X, Z, H) and a two-qubit entangling gate (like the **CNOT** gate):

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

- **Measurement:** The system should allow for the measurement of qubits in the computational basis $|0\rangle$ and $|1\rangle$, represented by projective measurements.

No Cloning Theorem

The **no-cloning theorem** states that it is **impossible** to create an exact copy of an arbitrary unknown quantum state.

Why not?

Quantum states can exist in a **superposition**, meaning they are a combination of 0 and 1.
Attempting to copy a quantum state involves measuring it, but **measurement collapses the state** into a definite value (0 or 1), destroying the superposition.

proof

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

Auxiliary Qubit

Let us have unknown q-state Psi. and starting in initial system's state as: $|\psi\rangle \otimes |0\rangle$

Suppose there exists a unitary operation *U* that can copy or perfectly clone this arbitrary quantum state.

Eqn. (i) $$U\left(|\psi\rangle \otimes |0\rangle\right) = \underbrace{|\psi\rangle \otimes |\psi\rangle}$$

cloning is to create two identical copies of the unknown state

$$= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

$$= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

For basis states:
$$\begin{cases} U(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \\ U(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle \end{cases}$$

For **Eqn (i)**
$$U\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\right)$$

$$= \alpha U(|0\rangle \otimes |0\rangle) + \beta U(|1\rangle \otimes |0\rangle) = \alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |1\rangle) \quad = \alpha|00\rangle + \beta|11\rangle$$

contradiction!

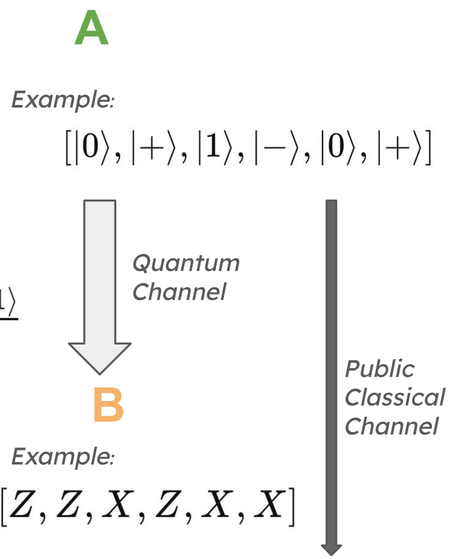
BB84

Quantum Key Distribution

Randomly selects sequence of qubits – some in the Z-basis and others in the X-basis

Z-basis: $|0\rangle$, $|1\rangle$

X-basis: $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$



A

Example:

$$[|0\rangle, |+\rangle, |1\rangle, |-\rangle, |0\rangle, |+\rangle]$$

Quantum Channel

B

Public Classical Channel

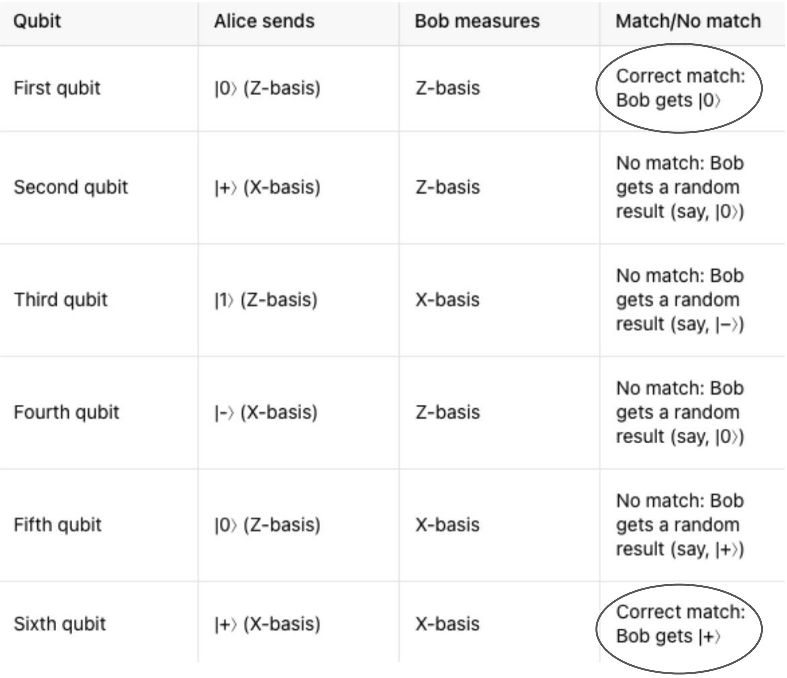
Example:

$$[Z, Z, X, Z, X, X]$$

Randomly chooses to measure each qubit in either the **Z-basis** or **X-basis**

After measurement, A publicly sends which bases was used to prepare each qubit

Compare their chosen bases (but **not the qubit values**), Explained in table: →



Qubit	Alice sends	Bob measures	Match/No match
First qubit	|0⟩ (Z-basis)	Z-basis	Correct match: Bob gets |0⟩
Second qubit	|+⟩ (X-basis)	Z-basis	No match: Bob gets a random result (say, |0⟩)
Third qubit	|1⟩ (Z-basis)	X-basis	No match: Bob gets a random result (say, |–⟩)
Fourth qubit	|-⟩ (X-basis)	Z-basis	No match: Bob gets a random result (say, |0⟩)
Fifth qubit	|0⟩ (Z-basis)	X-basis	No match: Bob gets a random result (say, |+⟩)
Sixth qubit	|+⟩ (X-basis)	X-basis	Correct match: Bob gets |+⟩

Discard the qubits where their bases do not match (qubits 2, 3, 4, and 5).

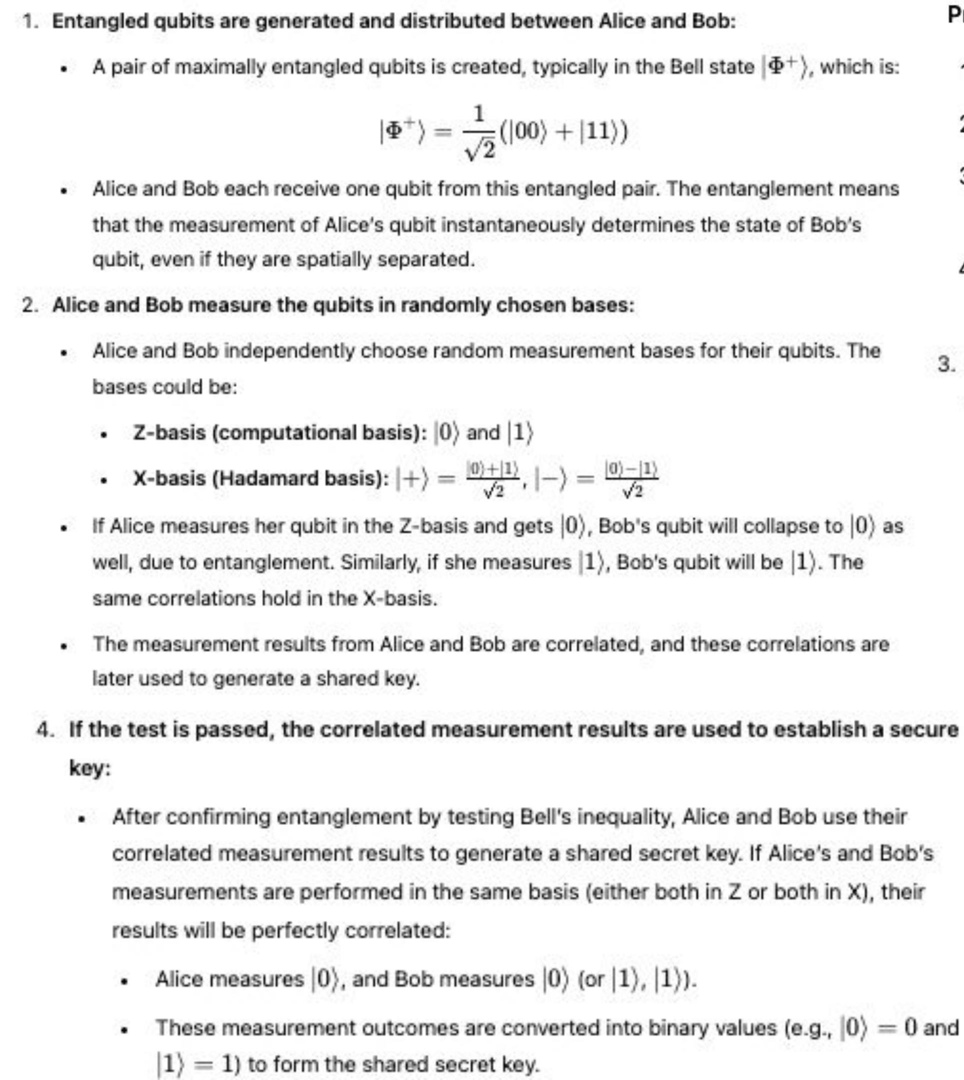
Qubits remaining after basis reconciliation form the **raw key**.

raw key: $[0, +]$

If Eavesdropper (E) tries to intercept the qubits:

E's **measurements** would disturb the system

$\Rightarrow$ Alice and Bob would notice errors when they compare a portion of their raw key.

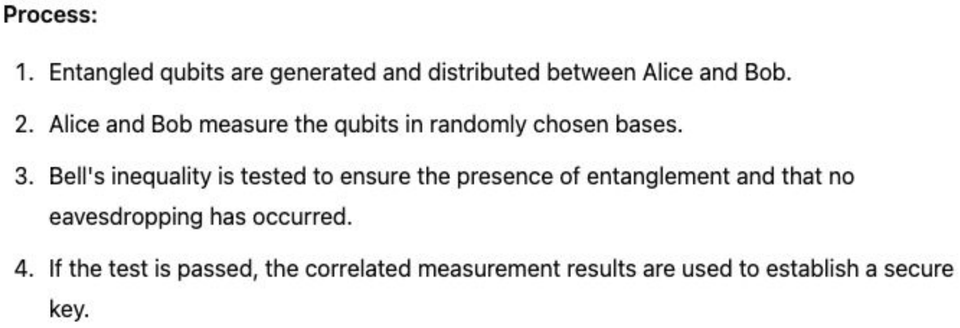


1. **Entangled qubits are generated and distributed between Alice and Bob:**
   - A pair of maximally entangled qubits is created, typically in the Bell state $|\Phi^+\rangle$, which is:

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

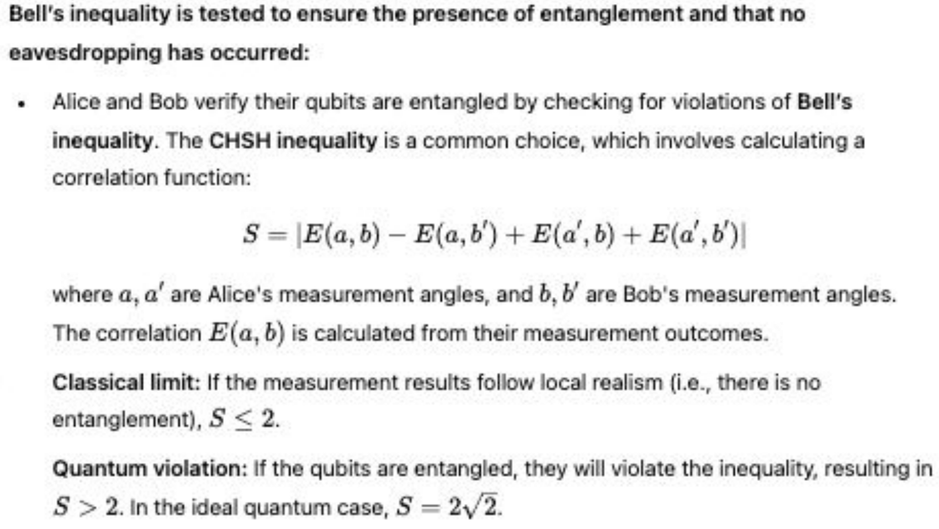
   - Alice and Bob each receive one qubit from this entangled pair. The entanglement means that the measurement of Alice's qubit instantaneously determines the state of Bob's qubit, even if they are spatially separated.
2. **Alice and Bob measure the qubits in randomly chosen bases:**
   - Alice and Bob independently choose random measurement bases for their qubits. The bases could be:
     - **Z-basis (computational basis):** $|0\rangle$ and $|1\rangle$
     - **X-basis (Hadamard basis):** $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
   - If Alice measures her qubit in the Z-basis and gets $|0\rangle$, Bob's qubit will collapse to $|0\rangle$ as well, due to entanglement. Similarly, if she measures $|1\rangle$, Bob's qubit will be $|1\rangle$. The same correlations hold in the X-basis.
   - The measurement results from Alice and Bob are correlated, and these correlations are later used to generate a shared key.

4. **If the test is passed, the correlated measurement results are used to establish a secure key:**
   - After confirming entanglement by testing Bell's inequality, Alice and Bob use their correlated measurement results to generate a shared secret key. If Alice's and Bob's measurements are performed in the same basis (either both in Z or both in X), their results will be perfectly correlated:
     - Alice measures $|0\rangle$, and Bob measures $|0\rangle$ (or $|1\rangle$, $|1\rangle$).
     - These measurement outcomes are converted into binary values (e.g., $|0\rangle = 0$ and $|1\rangle = 1$) to form the shared secret key.



Process:

1. Entangled qubits are generated and distributed between Alice and Bob.
2. Alice and Bob measure the qubits in randomly chosen bases.
3. Bell's inequality is tested to ensure the presence of entanglement and that no eavesdropping has occurred.
4. If the test is passed, the correlated measurement results are used to establish a secure key.



3. **Bell's inequality is tested to ensure the presence of entanglement and that no eavesdropping has occurred:**
   - Alice and Bob verify their qubits are entangled by checking for violations of **Bell's inequality**. The **CHSH inequality** is a common choice, which involves calculating a correlation function:

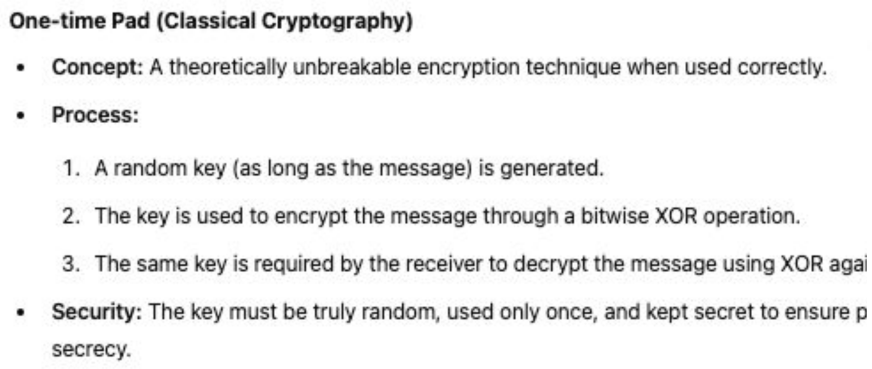
     $$S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')|$$

     where a, a' are Alice's measurement angles, and b, b' are Bob's measurement angles. The correlation $E(a,b)$ is calculated from their measurement outcomes.

     Classical limit: If the measurement results follow local realism (i.e., there is no entanglement), $S \leq 2$.

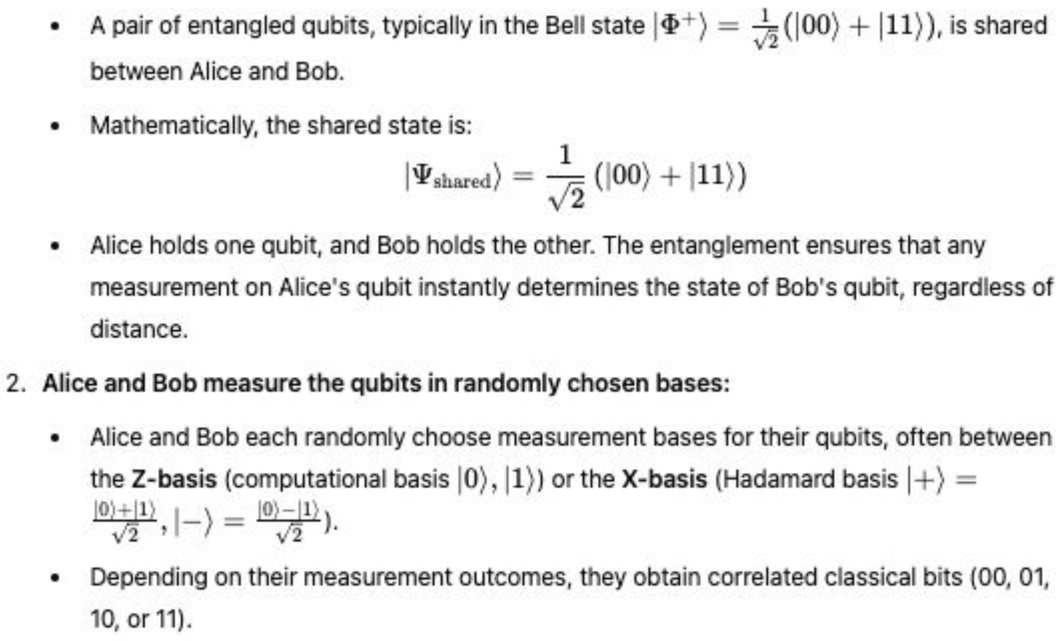
     Quantum violation: If the qubits are entangled, they will violate the inequality, resulting in $S > 2$. In the ideal quantum case, $S = 2\sqrt{2}$.

E91

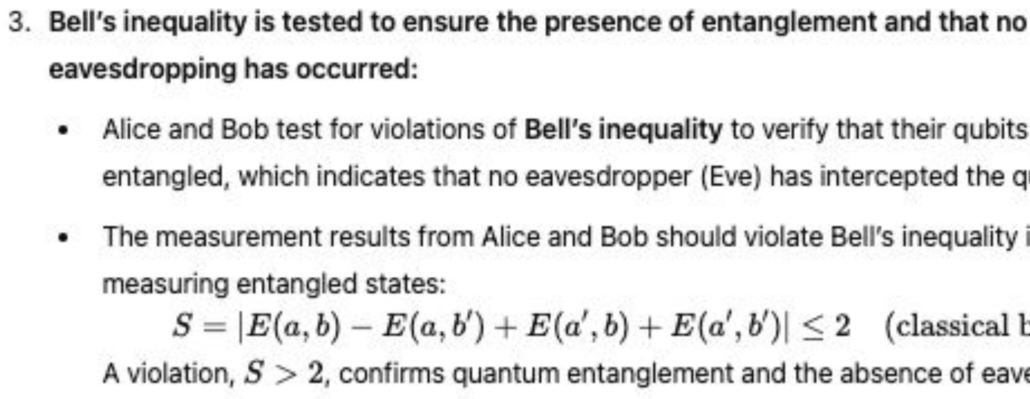


One-time Pad (Classical Cryptography)

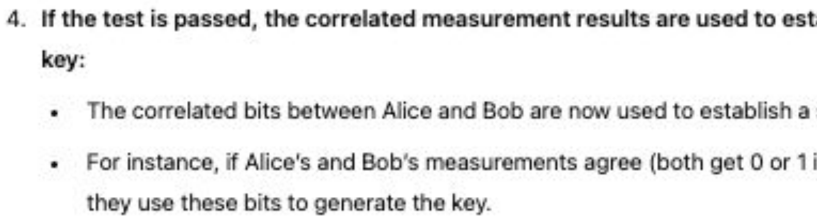
- **Concept:** A theoretically unbreakable encryption technique when used correctly.
- **Process:**
  1. A random key (as long as the message) is generated.
  2. The key is used to encrypt the message through a bitwise XOR operation.
  3. The same key is required by the receiver to decrypt the message using XOR agai
- **Security:** The key must be truly random, used only once, and kept secret to ensure p secrecy.



1. **Entangled qubits are generated and distributed between Alice and Bob:**
   - A pair of entangled qubits, typically in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, is shared between Alice and Bob.
   - Mathematically, the shared state is:
   $$|\Psi_{\text{shared}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
   - Alice holds one qubit, and Bob holds the other. The entanglement ensures that any measurement on Alice's qubit instantly determines the state of Bob's qubit, regardless of distance.
2. **Alice and Bob measure the qubits in randomly chosen bases:**
   - Alice and Bob each randomly choose measurement bases for their qubits, often between the **Z-basis** (computational basis $|0\rangle, |1\rangle$) or the **X-basis** (Hadamard basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$).
   - Depending on their measurement outcomes, they obtain correlated classical bits (00, 01, 10, or 11).



3. **Bell's inequality is tested to ensure the presence of entanglement and that no eavesdropping has occurred:**
   - Alice and Bob test for violations of **Bell's inequality** to verify that their qubits entangled, which indicates that no eavesdropper (Eve) has intercepted the q
   - The measurement results from Alice and Bob should violate Bell's inequality i measuring entangled states:
   $$S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')| \leq 2 \quad (\text{classical b}$$
   A violation, $S > 2$, confirms quantum entanglement and the absence of eave



4. **If the test is passed, the correlated measurement results are used to est key:**
   - The correlated bits between Alice and Bob are now used to establish a
   - For instance, if Alice's and Bob's measurements agree (both get 0 or 1 i they use these bits to generate the key.

One-time Pad

Bipartite Communication Protocols

2 party-communication/ information transfer:

Quantum Teleportation

Transmit unknown state from one location to another without physically transferring the particle.

1. Entangling Qubits

$$|\Phi^+\rangle_{A_2B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

2 Qubits – 1 sent to Bob, 1 sent to Alice – prepared in a maximally entangled state (Bell State)

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

Alice has an additional qubit that she wants to teleport

$$|\psi\rangle_{A_1} \otimes |\Phi^+\rangle_{A_2B} = (\alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{A_2B} + |11\rangle_{A_2B})$$

$$|\text{Initial State}\rangle = \frac{1}{\sqrt{2}}[\alpha|000\rangle_{A_1A_2B} + \alpha|011\rangle_{A_1A_2B} + \beta|100\rangle_{A_1A_2B} + \beta|111\rangle_{A_1A_2B}]$$

$$|\text{Total State}\rangle = \frac{1}{2}\,[|\Phi^+\rangle_{A_1A_2}(\alpha|0\rangle + \beta|1\rangle)_B + |\Phi^-\rangle_{A_1A_2}(\alpha|0\rangle - \beta|1\rangle)_B + |\Psi^+\rangle_{A_1A_2}(\beta|0\rangle$$
$$+ |\Psi^+\rangle_{A_1A_2}(\beta|0\rangle + \alpha|1\rangle)_B + |\Psi^-\rangle_{A_1A_2}(\beta|0\rangle - \alpha|1\rangle)_B]$$

The **four Bell states** are:

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

Alice performs a Bell-state measurement on her two qubits:
- qubit she wants to teleport,
- her qubit in the entangled state

This Projects measurement into one of the Bell States:

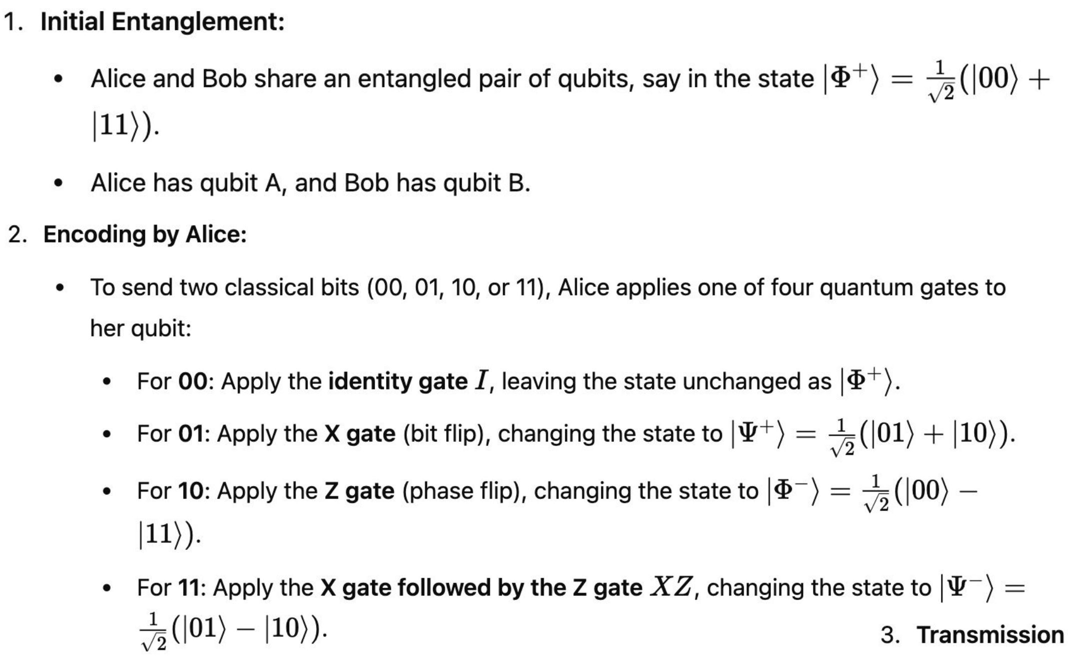
result

- **If Alice measures** $|\Phi^+\rangle$: Bob's qubit is in the state $\alpha|0\rangle + \beta|1\rangle$, which is the original state Alice wanted to teleport.
- **If Alice measures** $|\Phi^-\rangle$: Bob's qubit is in the state $\alpha|0\rangle - \beta|1\rangle$, meaning he needs to apply a **Z gate (phase flip)** to recover the original state.
- **If Alice measures** $|\Psi^+\rangle$: Bob's qubit is in the state $\beta|0\rangle + \alpha|1\rangle$, meaning he needs to apply a **X gate (bit flip)** to recover the original state.
- **If Alice measures** $|\Psi^-\rangle$: Bob's qubit is in the state $\beta|0\rangle - \alpha|1\rangle$, meaning he needs to apply a **X gate followed by a Z gate** (bit flip + phase flip) to recover the original state.

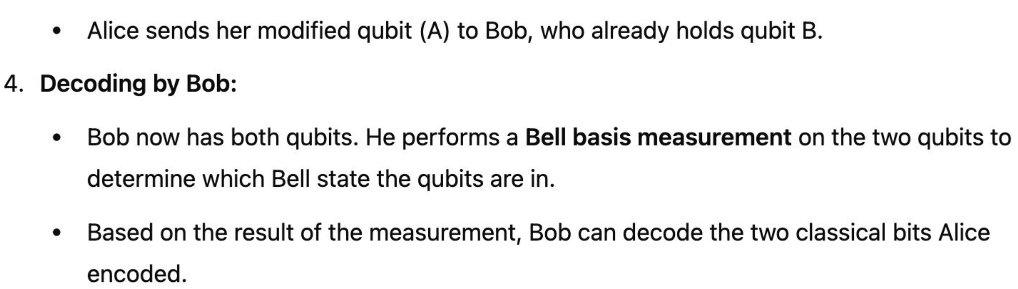
Superdense coding:

Superdense coding is a quantum communication protocol that allows the transmission of **two classical bits** of information using only **one qubit**. It leverages the power of quantum entanglement to achieve this compression of classical information.

Alice and Bob share a pair of **entangled qubits (**in a Bell state**).** Alice can manipulate her qubit to encode two classical bits of information, and then send that single qubit to Bob. Once Bob receives Alice's qubit, he can measure both qubits in the **Bell basis** and recover the two classical bits.



1. **Initial Entanglement:**
   - Alice and Bob share an entangled pair of qubits, say in the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
   - Alice has qubit A, and Bob has qubit B.
2. **Encoding by Alice:**
   - To send two classical bits (00, 01, 10, or 11), Alice applies one of four quantum gates to her qubit:
     - For **00**: Apply the **identity gate** I, leaving the state unchanged as $|\Phi^+\rangle$.
     - For **01**: Apply the **X gate** (bit flip), changing the state to $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.
     - For **10**: Apply the **Z gate** (phase flip), changing the state to $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.
     - For **11**: Apply the **X gate followed by the Z gate** XZ, changing the state to $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

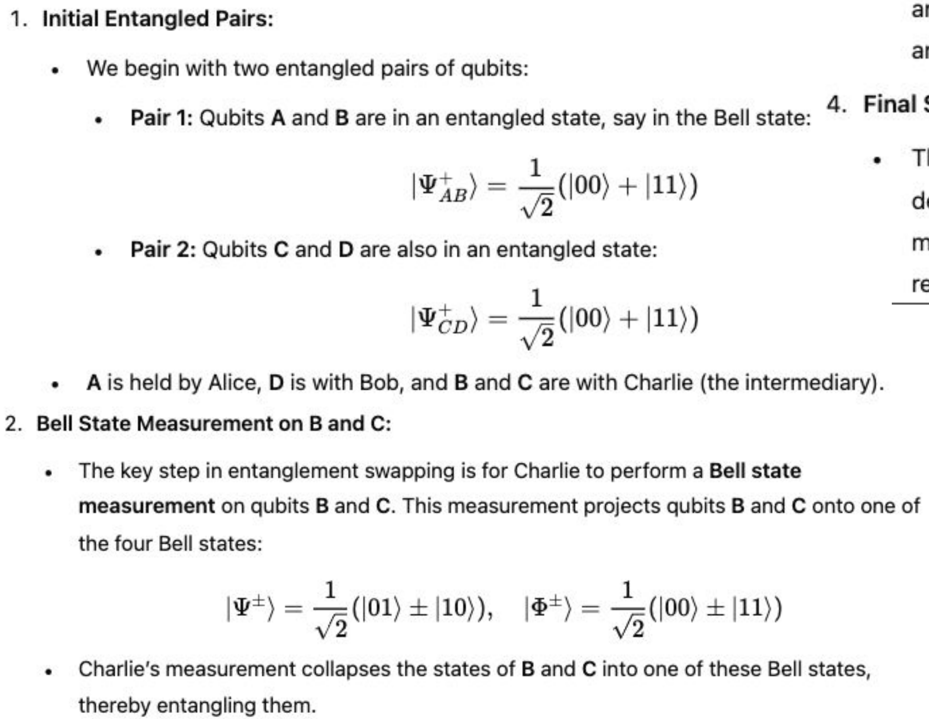


3. **Transmission to Bob:**
   - Alice sends her modified qubit (A) to Bob, who already holds qubit B.
4. **Decoding by Bob:**
   - Bob now has both qubits. He performs a **Bell basis measurement** on the two qubits to determine which Bell state the qubits are in.
   - Based on the result of the measurement, Bob can decode the two classical bits Alice encoded.

Entanglement Swapping

a quantum phenomenon where two particles that have never interacted or shar entanglement directly become entangled through an intermediary process.

Consider four qubits: **A**, **B**, **C**, and **D**. Initially, qubits **A** and **B** are entangled, and qubits **C** and **D** are entangled, but **A** and **D** are not entangled, nor are **B** and **C**. Entanglement swapping allows us to entangle **A** and **D** without them ever interacting directly.



1. **Initial Entangled Pairs:**
   - We begin with two entangled pairs of qubits:
     - **Pair 1:** Qubits **A** and **B** are in an entangled state, say in the Bell state:

$$|\Psi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

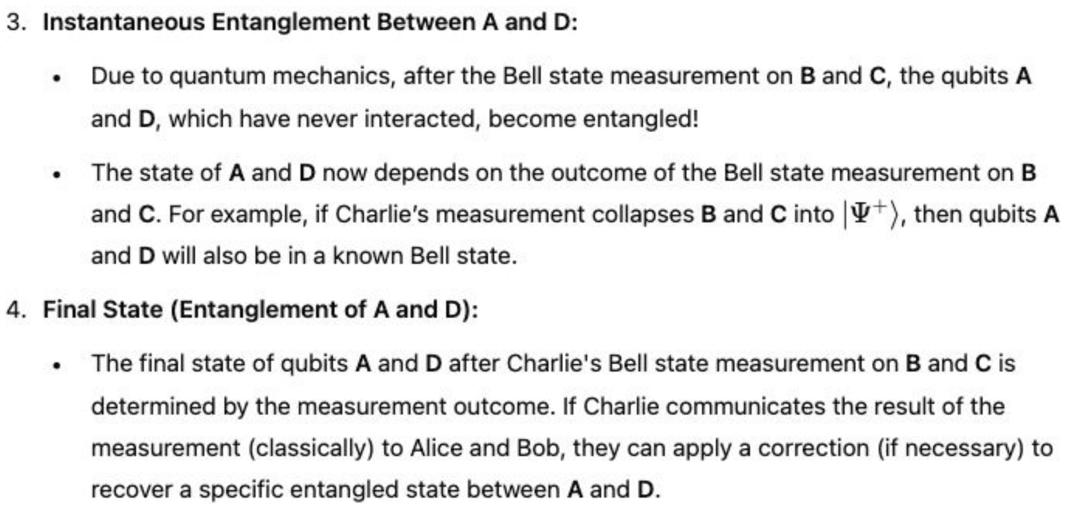
     - **Pair 2:** Qubits **C** and **D** are also in an entangled state:

$$|\Psi^+_{CD}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   - **A** is held by Alice, **D** is with Bob, and **B** and **C** are with Charlie (the intermediary).
2. **Bell State Measurement on B and C:**
   - The key step in entanglement swapping is for Charlie to perform a **Bell state measurement** on qubits **B** and **C**. This measurement projects qubits **B** and **C** onto one of the four Bell states:

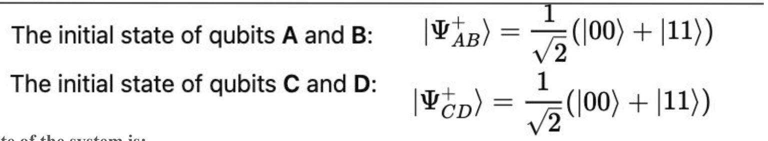
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad |\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

   - Charlie's measurement collapses the states of **B** and **C** into one of these Bell states, thereby entangling them.



3. **Instantaneous Entanglement Between A and D:**
   - Due to quantum mechanics, after the Bell state measurement on **B** and **C**, the qubits **A** and **D**, which have never interacted, become entangled!
   - The state of **A** and **D** now depends on the outcome of the Bell state measurement on **B** and **C**. For example, if Charlie's measurement collapses **B** and **C** into $|\Psi^+\rangle$, then qubits **A** and **D** will also be in a known Bell state.
4. **Final State (Entanglement of A and D):**
   - The final state of qubits **A** and **D** after Charlie's Bell state measurement on **B** and **C** is determined by the measurement outcome. If Charlie communicates the result of the measurement (classically) to Alice and Bob, they can apply a correction (if necessary) to recover a specific entangled state between **A** and **D**.

Example:



The initial state of qubits **A** and **B**: $|\Psi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

The initial state of qubits **C** and **D**: $|\Psi^+_{CD}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

The total state of the system is:

$$|\Psi^+_{AB}\rangle \otimes |\Psi^+_{CD}\rangle = \frac{1}{2}(|00\rangle_{AB}|00\rangle_{CD} + |11\rangle_{AB}|11\rangle_{CD})$$

When Charlie performs a Bell state measurement on **B** and **C**, he collapses the joint state of qubits **B** and **C** into one of the four Bell states. For instance, if the measurement results in Psi_BC, then the state of **A** and **D** will also collapse into a Bell state, such as PSi_AD. The outcome depends on the result of the Bell measurement, which Charlie communicates to Alice and Bob.

Quantum Fourier Transform

$$e^{2\pi i \frac{xy}{2^n}}$$

maps a quantum state $|x\rangle$ to a superposition of states, with each state weighted by a complex coefficient *used to extract periodicity from quantum states,*

On *n*-qubit q-state $|x\rangle$

$$QFT(|x\rangle) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{2^n}} |y\rangle$$

x is an integer represented in binary form (example):

$$for \;\; x = 6 \begin{cases} 6 \div 2 = 3, \text{ remainder } 0 \\ 3 \div 2 = 1, \text{ remainder } 1 \\ 1 \div 2 = 0, \text{ remainder } 1 \end{cases}$$

$$\Rightarrow \quad x = 110_2$$

General binary representation:

$$6 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$

$$x = x_{n-1} \cdot 2^{n-1} + x_{n-2} \cdot 2^{n-2} + \cdots + x_1 \cdot 2^1 + x_0 \cdot 2^0$$

example:

QFT on a 2-qubit state $|01\rangle$ $n = 2, x = 1$

$$QFT(|01\rangle) = \frac{1}{2} \sum_{y=0}^{3} e^{2\pi i \frac{1y}{4}} |y\rangle$$

- For $y = 0$: $e^{2\pi i \frac{1 \cdot 0}{4}} = 1$
- For $y = 1$: $e^{2\pi i \frac{1 \cdot 1}{4}} = e^{\pi i/2} = i$
- For $y = 2$: $e^{2\pi i \frac{1 \cdot 2}{4}} = e^{\pi i} = -1$
- For $y = 3$: $e^{2\pi i \frac{1 \cdot 3}{4}} = e^{3\pi i/2} = -i$

Final QFT state is:

$$QFT(|01\rangle) = \frac{1}{2} (|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$$

QFT continued…

- **Hadamard Gates**: Apply on each qubit to create superpositions.
- **Controlled Phase Shifts**: Implemented between qubits to introduce the necessary phases (interference.)
- **SWAP Gate**: Reverses the qubit order at the end

$$cR_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}$$

$$|1\rangle \otimes |q_t\rangle \rightarrow |1\rangle \otimes e^{2\pi i/2^k}|q_t\rangle$$

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

$$\begin{cases} H|\psi\rangle = H(\alpha|0\rangle + \beta|1\rangle) \\ \qquad = \alpha\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \beta\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ H|\psi\rangle = \frac{1}{\sqrt{2}}\left[(\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle\right] \end{cases}$$

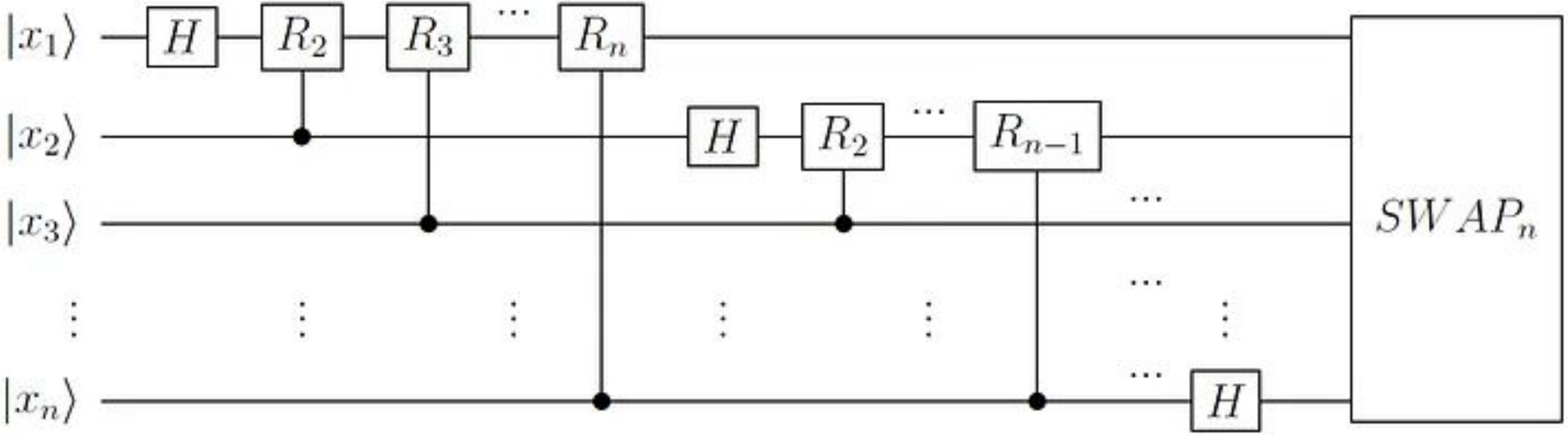
$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$SWAP|00\rangle = |00\rangle$$

$$SWAP|01\rangle = |10\rangle$$

$$SWAP|10\rangle = |01\rangle$$

$$SWAP|11\rangle = |11\rangle$$



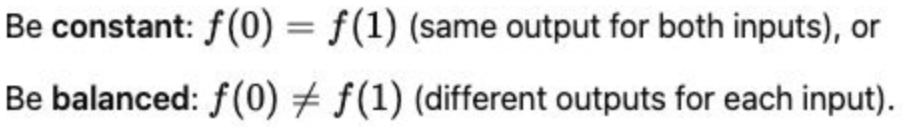
Deutsch Algorithm

$f:\{0,1\}\rightarrow\{0,1\}$

Problem

a **black-box function** *f* that: takes one bit as input (0 or 1),
returns single 1 bit output (0 or 1)

The function can either be:



Be **constant**: $f(0)=f(1)$ (same output for both inputs), or

Be **balanced**: $f(0)\neq f(1)$ (different outputs for each input).

4 cases:

$$f(0)=f(1)=0$$
$$f(0)=f(1)=1$$

constant

$$f(0)=1 \quad \& \quad f(1)=0$$
$$f(0)=0 \quad \& \quad f(1)=1$$

balanced

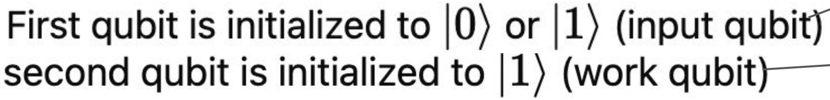
Classically: *must evaluate the function twice to determine if it is balanced or constant – both* $f(0)$ & $f(1)$

VERSUS

Quantumly: *can evaluate the function ONCE to determine if it is balanced or constant*

Algorithm

1



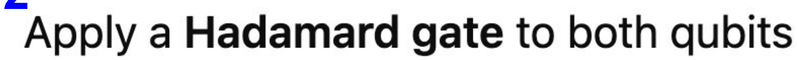
First qubit is initialized to $|0\rangle$ or $|1\rangle$ (input qubit) $|x\rangle$

second qubit is initialized to $|1\rangle$ (work qubit) $|y\rangle$

Together, state is:

$$|x\rangle\otimes|y=1\rangle$$

2



Apply a **Hadamard gate** to both qubits

Each qubit is now in a *superposition of 0 and 1*

⇒ **Together**, after applying the Hadamard gates to both qubits,
the state Psi becomes a superposition of 4 possible states: $|\psi\rangle \quad |00\rangle, |01\rangle, |10\rangle, |11\rangle$

Recall:

$$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$
$$H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

Explained in next slide

continued…

$x \in \{0,1\}$ **2 cases– *x* is 0 or 1**

$y = 1$

The quantum State when applying hadamard gate is: $H \otimes H|xy\rangle$

If $x = 0$:

$$H \otimes H\,(|0\rangle \otimes |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi\rangle = \frac{1}{2}\,(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

If $x = 1$:

$$H \otimes H\,(|1\rangle \otimes |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi\rangle = \frac{1}{2}\,(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

3 Apply **oracle (i.e. function f(x))**

– in quantum computing, this is a Gate (matrix), notation: U_f

This oracle gate applies the function to the first qubit *x*, but **modifies the second qubit** based on the result of the function. This is expressed mathematically as:

$$U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

$\oplus$ is the XOR (modulo-2 addition).

…continued…

$$U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

If $f(0) = 0, f(1) = 0$ (Constant Function):

$\Rightarrow$ The second qubit remains **unchanged** for all states:

$$U_f(|00\rangle) = |00\rangle$$

$$U_f(|01\rangle) = |01\rangle$$

$$U_f(|10\rangle) = |10\rangle$$

$$U_f(|11\rangle) = |11\rangle$$

$$|\psi_{\text{after oracle}}\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

(for both $x = 0$ and $x = 1$)

If $f(0) = 0, f(1) = 1$ (Balanced Function):

$\Rightarrow$ The second qubit The second qubit is flipped **only when x=1:**

$$U_f(|00\rangle) = |00\rangle$$

$$U_f(|01\rangle) = |01\rangle$$

$U_f(|10\rangle) = |11\rangle$ (second qubit flipped)

$U_f(|11\rangle) = |10\rangle$ (second qubit flipped)

$$|\psi_{\text{after oracle}}\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle)$$

(for both $x = 0$ and $x = 1$)

Notice sign flips!

Deutsch-Jozsa's Algorithm !

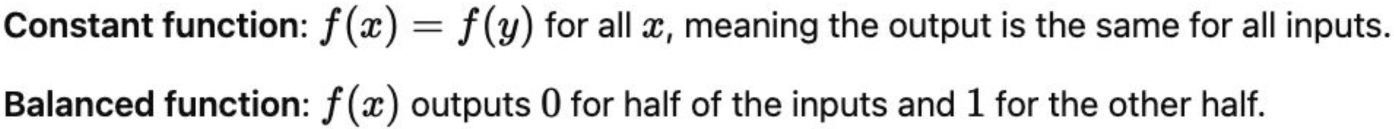
*Goal of the **Deutsch-Jozsa Algorithm** is to determine whether a given function (that takes an n-bit input) is **constant** or **balanced**.* $f\colon \{0,1\}^n \rightarrow \{0,1\}$

Classically $2^{n-1}+1$

' Inputs to determine,

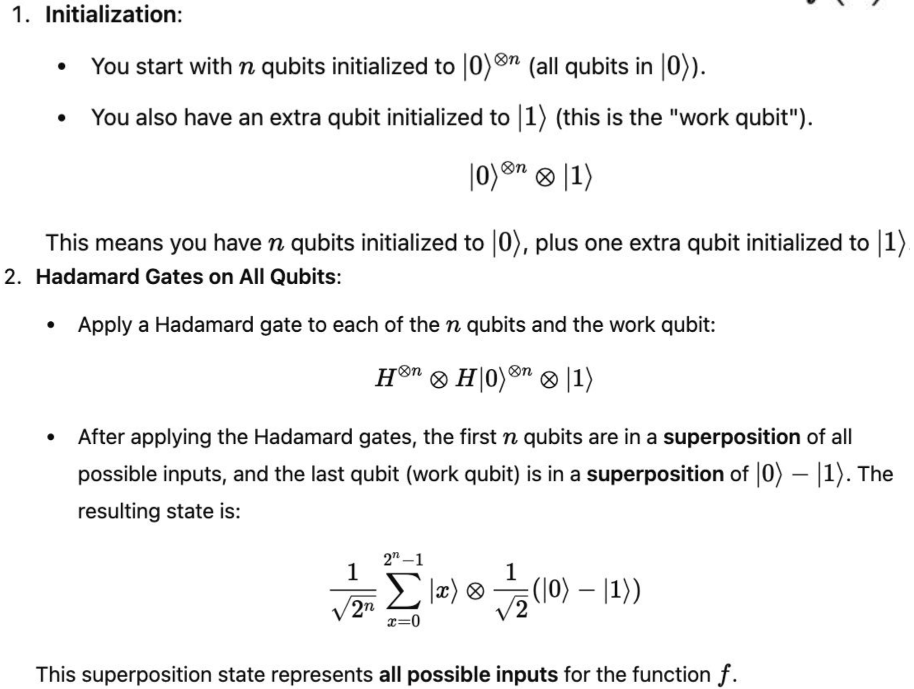
Quantumly,

ONE function evaluation



Constant function: $f(x) = f(y)$ for all x, meaning the output is the same for all inputs.

Balanced function: $f(x)$ outputs 0 for half of the inputs and 1 for the other half.



1. **Initialization:**
   - You start with n qubits initialized to $|0\rangle^{\otimes n}$ (all qubits in $|0\rangle$).
   - You also have an extra qubit initialized to $|1\rangle$ (this is the "work qubit").

$$|0\rangle^{\otimes n} \otimes |1\rangle$$

This means you have n qubits initialized to $|0\rangle$, plus one extra qubit initialized to $|1\rangle$

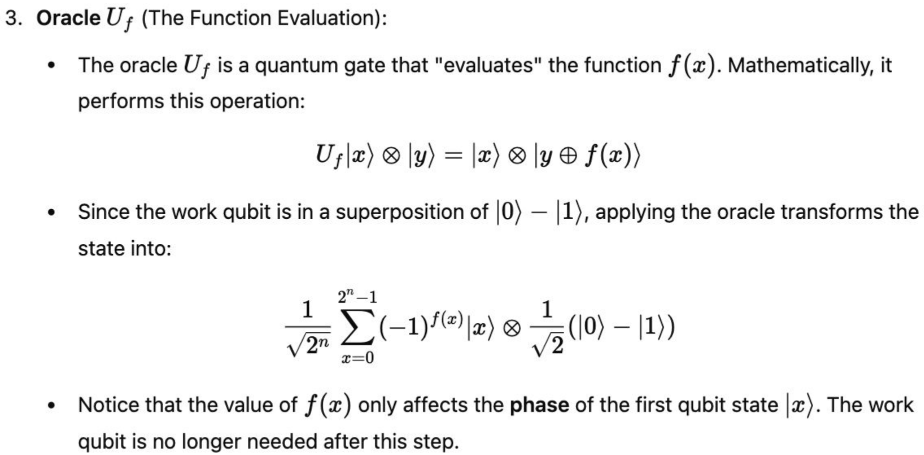
2. **Hadamard Gates on All Qubits:**
   - Apply a Hadamard gate to each of the n qubits and the work qubit:

$$H^{\otimes n} \otimes H|0\rangle^{\otimes n} \otimes |1\rangle$$

   - After applying the Hadamard gates, the first n qubits are in a **superposition** of all possible inputs, and the last qubit (work qubit) is in a **superposition** of $|0\rangle - |1\rangle$. The resulting state is:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

This superposition state represents **all possible inputs** for the function f.



3. **Oracle** U_f (The Function Evaluation):
   - The oracle U_f is a quantum gate that "evaluates" the function $f(x)$. Mathematically, it performs this operation:

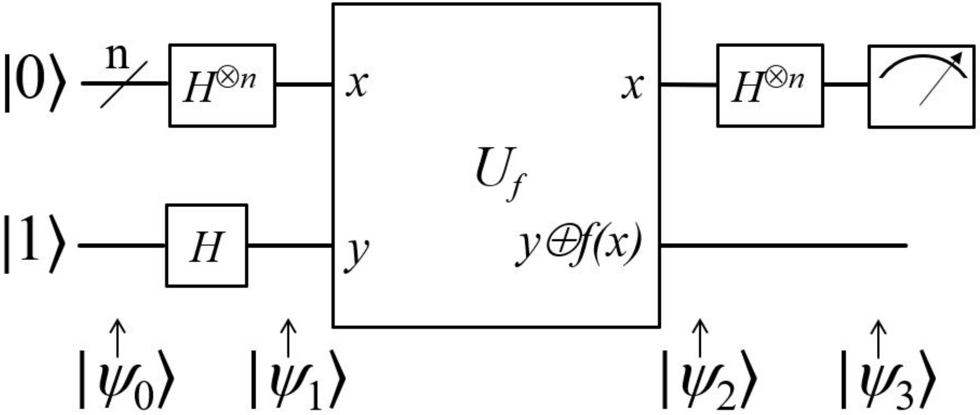
$$U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

   - Since the work qubit is in a superposition of $|0\rangle - |1\rangle$, applying the oracle transforms the state into:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

   - Notice that the value of $f(x)$ only affects the **phase** of the first qubit state $|x\rangle$. The work qubit is no longer needed after this step.

continued….



4. **Hadamard Gates on First n Qubits**:
   - Now, apply another set of Hadamard gates to the first n qubits

$$H^{\otimes n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle$$

   - This transforms the state into:

$$\frac{1}{2^n}\sum_{z=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{x\cdot z+f(x)}\right]|z\rangle$$

Here, $x \cdot z$ is the **bitwise dot product** (modulo-2) between the binary representations of x and z.

5. **Measurement**:
   - Now, you measure the first n qubits. Two outcomes are possible:
     - If $f(x)$ is **constant**, the measurement will yield $|0\rangle^{\otimes n}$ with **certainty** (all zeroes).
     - If $f(x)$ is **balanced**, the result will be **anything but** $|0\rangle^{\otimes n}$ with high probability.

continued…

4 Apply Hadamard again:

Constant Function:

$$H \otimes I \left(\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \right)$$

$$= \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle - \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle \right)$$

5 first qubit collapses to $|0\rangle$ when measured

Balanced Function:

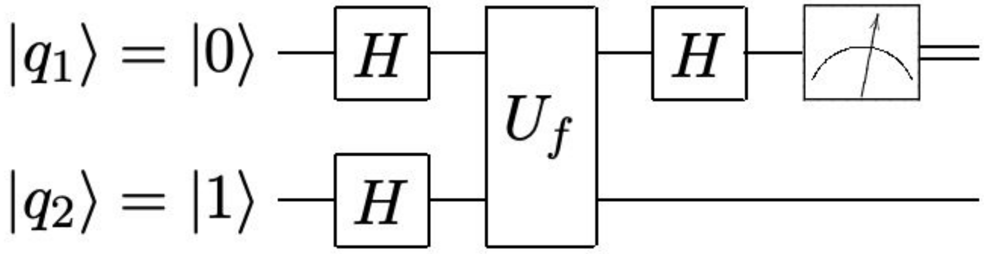
$$H \otimes I \left(\frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) \right)$$

$$= \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle - \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \right)$$

5 first qubit collapses to $|1\rangle$ when measured

$$H \otimes H \, U_f \, H \otimes H \, |xy\rangle$$

circuit



Deutsch's Algorithm is a *specific case* of the general problem: **Deutsch-Jozsa's Algorithm !**

Shor's Factorization Algorithm

Problem: given a large composite number N, find its prime factors.

1. reducing the factorization problem to an order-finding problem

(Classical)

2. Choose a random number a s.t $1 < a < N$ ——(number to be factored)

3. Check if $\gcd(a, N) \neq 1$ using ***Euclid's Algorithm***

We are interested in **periodic behavior** of powers of a under **modulo** N arithmetic when $\gcd(a, N) = 1$

Order *of a number, (*order = ***r****),*
is the smallest integer s.t: $a^r \equiv 1 \pmod N$

Example of Order and Periodicity

$N = 15$, $a = 2$

$$2^1 \mod 15 = 2$$
$$2^2 \mod 15 = 4$$
$$2^3 \mod 15 = 8$$
$$2^4 \mod 15 = 16 \mod 15 = 1$$

So, *r* = 4

because after raising 2 to the power of 4, we get 1. This means the sequence of powers of 2 mod 15 starts repeating every 4 steps:

$$2, 4, 8, 1, 2, 4, 8, 1, \ldots$$

Compute the greatest common divisor (GCD) *of 2 numbers – GCD is is the largest number that divides both of them without leaving a remainder*

$$\gcd(a, N) = \gcd(N, a \mod N)$$

If:

$\gcd(a, N) \neq 1$ then a and N have a common factor

$\gcd(a, N) = 1$ then a and N are coprime

coprime (no common factors other than 1)

EX: ***a = 8 & N = 42*** $\gcd(8, 42) = \gcd(42, 8 \mod 42).$

1. $42/8 = 5$ r2 $\Rightarrow \gcd(8, 42) = \gcd(8, 2)$
2. $8/2 = 4$ r0 $\Rightarrow \gcd(8, 2) = 2$

So, no need to proceed further since you've found gcd: $\gcd(8, 42) = 2$

continued… Shor’s algorithm finds this **order *r*** using quantum methods (specifically, the Quantum Fourier Transform) much more efficiently than classical algorithms can.

1. Create a superposition:

    *this allows the q-computer to simultaneously compute multiple values of a**x mod N*

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

2. Apply a q-circuit that computes:

    ***a**x mod N** for each x in the superposition.*

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|a^x \mod N\rangle$$

each *x* is "paired" with its corresponding ***a**x mod N*** value, but it is not known what those values are yet

3. Apply Quantum Fourier Transform (QFT):

    *Extract the **periodicity** (or order r) of the function **a**x mod N***

    *Classically, this would be like performing a **Fourier analysis** to find the frequency (or periodicity) of a signal,*

4. Measure first register:

    The result is a value *k* that is **related to the order *r*** of *a* mod *N*

Grover’s Search Algorithm

to search for a specific item in an unsorted database

list of N items and want to find a specific target.

→ classically, check $N/2$ times on avg., worst case N times

Classic algorithms time it takes to solve:

$$O(N)$$

Grover’s Algorithm:

$$O(\sqrt{N})$$

1. Initialization: Superposition of All States

n qubits $\quad N = 2^n$

Apply Hadamard to each qubit → q-state is now:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

2. Oracle Query: Marking the Target State

An **oracle** (black-box function) is used to mark the correct state (the target) by flipping its phase (multiply by -1)

Oracle is implemented as a unitary operation O, which acts as:

$$O|x\rangle = \begin{cases} -|x\rangle & \text{if } x \text{ is the target,} \\ |x\rangle & \text{if } x \text{ is not the target} \end{cases}$$

3. Grover Diffusion Operator: Amplifying the Target State

This operator amplifies the probability amplitude of the target state, making it more likely to be measured

This operation reflects the amplitudes about the average amplitude of all states

$$\boxed{D = 2|\psi\rangle\langle\psi| - I}$$

Psi = equal superposition state

4. Repeat: Oracle + Diffusion

After each iteration, probability of finding target increases, until it reaches ~1

Bernstein Vazirani's Algorithm

Goal is to find the hidden bit string *s* with the fewest possible queries to the black-box function

black-box function $f(x)$

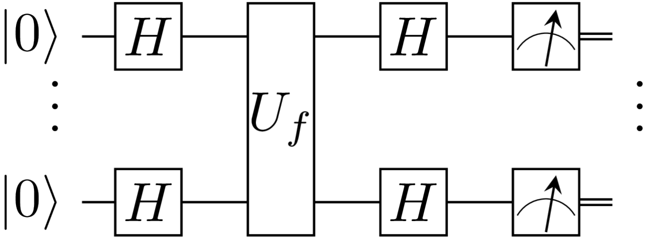
$$f(x) = x \cdot s \mod 2$$

input bit string

unknown **secret bit string** (or hidden integer)

Classically,
in the worst case, a classical algorithm would need to query the black-box function *n* times (for each bit of *s*) to find the hidden string

Quantumly,
just **one query** to the black-box function using quantum computing



1. Apply a Hadamard Transform to the *n*-qubit state $|0\rangle^{\otimes n}$
2. Apply oracle U_f which transforms $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$
3. Another Hadamard transform is applied to each qubit

makes it so that for qubits where *s_i = 1,* its state is converted from $|-\rangle$ to $|1\rangle$ and for qubits where *s_i = 0*, its state is converted from $|+\rangle$ to $|0\rangle$

Full Algorithm:

$$|0\rangle^n \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)+x\cdot y}|y\rangle = |s\rangle$$

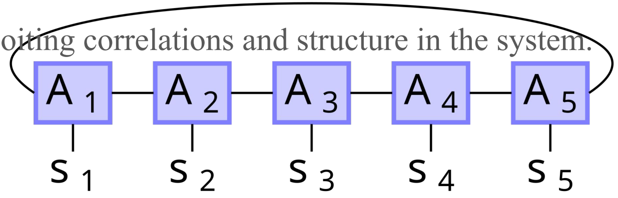
Fidelity:

- quantifies the **closeness** between two quantum states – i.e. how similar two quantum states are to each other
- **1** means the states are identical, while **0** means they are completely different (orthogonal).
- It is a critical tool in evaluating the accuracy of quantum operations and algorithms.

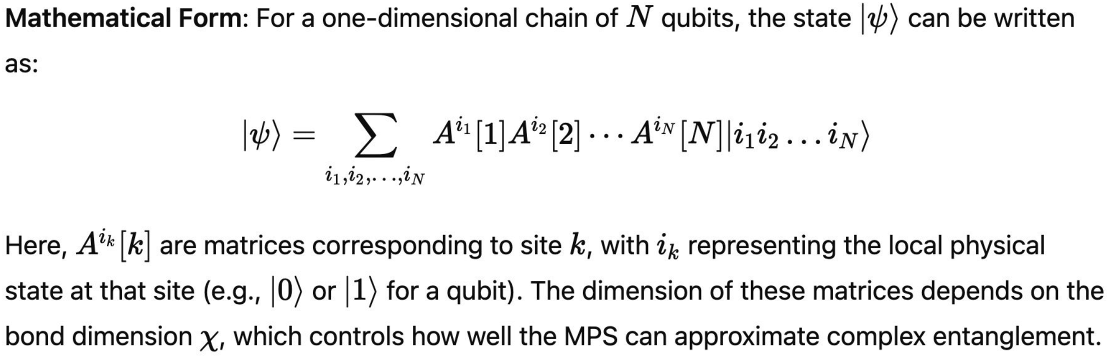
$$F\underbrace{(\rho,\sigma)}_{\text{Density matrices of the 2 quantum states}} = \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\right)^{2} \xrightarrow{\text{If both states are pure then…}} F(|\psi\rangle,|\phi\rangle) = |\langle\psi|\phi\rangle|^{2}$$

Miscellaneous

MPS (Matrix Product States) provides a way to efficiently represent certain quantum states by exploiting correlations and structure in the system.



In an MPS, the quantum state is represented as a chain of tensors (matrices), each corresponding to one site (or qubit), with connections (or bonds) between neighboring sites.



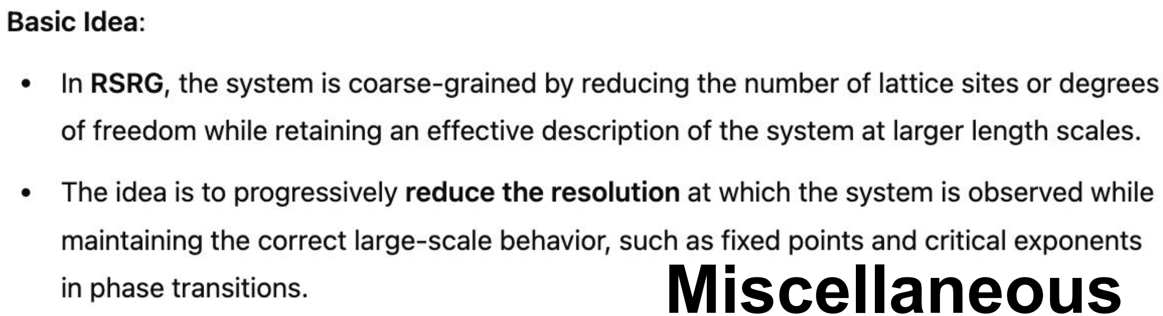
Mathematical Form: For a one-dimensional chain of N qubits, the state $|\psi\rangle$ can be written as:

$$|\psi\rangle = \sum_{i_1,i_2,\ldots,i_N} A^{i_1}[1]A^{i_2}[2]\cdots A^{i_N}[N]|i_1 i_2 \ldots i_N\rangle$$

Here, $A^{i_k}[k]$ are matrices corresponding to site k, with i_k representing the local physical state at that site (e.g., $|0\rangle$ or $|1\rangle$ for a qubit). The dimension of these matrices depends on the bond dimension χ, which controls how well the MPS can approximate complex entanglement.

Real-Space Renormalization Group (RSRG)

to study systems with many degrees of freedom, typically on a lattice, such as spin systems or condensed matter systems. The method is designed to simplify these complex systems by systematically reducing the number of degrees of freedom while preserving the essential physics, such as critical behavior near phase transitions.



Basic Idea:

- In **RSRG**, the system is coarse-grained by reducing the number of lattice sites or degrees of freedom while retaining an effective description of the system at larger length scales.
- The idea is to progressively **reduce the resolution** at which the system is observed while maintaining the correct large-scale behavior, such as fixed points and critical exponents in phase transitions.

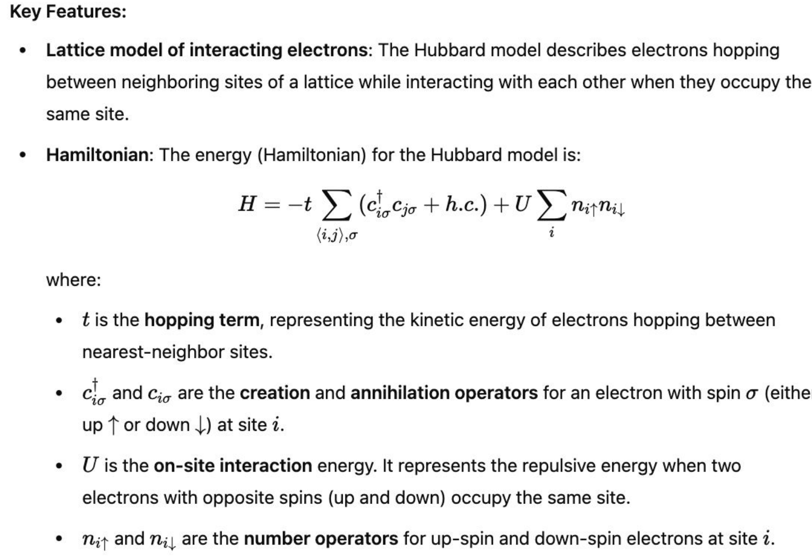
Density Matrix Renormalization Group (DMRG), which is a highly efficient method for finding ground states of one-dimensional quantum systems–for solving quantum many-body problems.
DMRG can be understood in modern terms as a variational optimization method over **Matrix Product States (MPS)**

- one-dimensional chain of particles or spins, is divided into two parts: the **block** and its **environment**.
- block may represent a small section of the entire system (perhaps a few sites or particles). As the algorithm proceeds, the block is **grown iteratively** by adding one site at a time.
- Without truncation, the **state space** of the quantum system grows **exponentially** as more sites are added to the block– ex: N sites– then growth is like d**N
- DMRG **truncates** the number of states it keeps track of by only retaining the most significant states. This is done by looking at

Miscellaneous 2

Ising model: is a mathematical model of ferromagnetism statistical mechanics.

Hubbard model: study **electron correlations** in systems with interacti electrons. It is one of the simplest models to describe phenomena such as **metal-insulator transitions** and **high-temperature superconductivity**



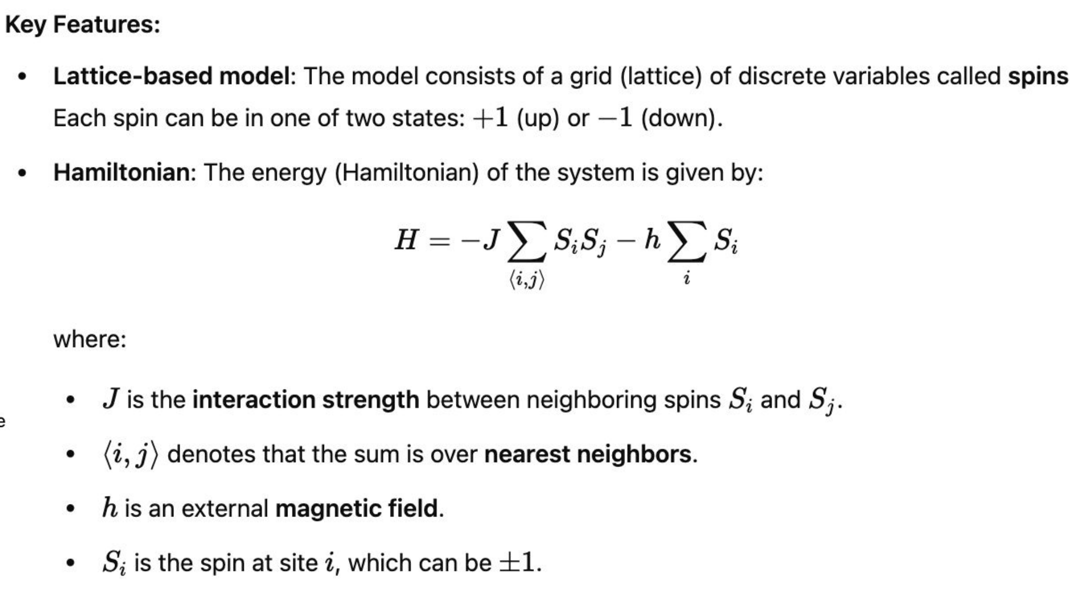
Key Features:

- **Lattice model of interacting electrons**: The Hubbard model describes electrons hopping between neighboring sites of a lattice while interacting with each other when they occupy the same site.
- **Hamiltonian**: The energy (Hamiltonian) for the Hubbard model is:

$$H = -t \sum_{\langle i,j \rangle,\sigma} (c^\dagger_{i\sigma} c_{j\sigma} + h.c.) + U \sum_i n_{i\uparrow} n_{i\downarrow}$$

where:

- t is the **hopping term**, representing the kinetic energy of electrons hopping between nearest-neighbor sites.
- $c^\dagger_{i\sigma}$ and $c_{i\sigma}$ are the **creation** and **annihilation operators** for an electron with spin σ (either up ↑ or down ↓) at site i.
- U is the **on-site interaction** energy. It represents the repulsive energy when two electrons with opposite spins (up and down) occupy the same site.
- $n_{i\uparrow}$ and $n_{i\downarrow}$ are the **number operators** for up-spin and down-spin electrons at site i.



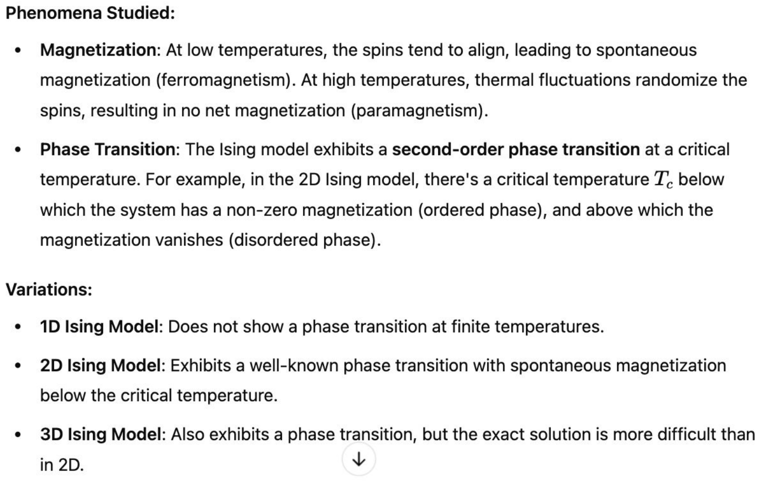
Key Features:

- **Lattice-based model**: The model consists of a grid (lattice) of discrete variables called **spins** Each spin can be in one of two states: $+1$ (up) or -1 (down).
- **Hamiltonian**: The energy (Hamiltonian) of the system is given by:

$$H = -J \sum_{\langle i,j \rangle} S_i S_j - h \sum_i S_i$$

where:

- J is the **interaction strength** between neighboring spins S_i and S_j.
- $\langle i, j \rangle$ denotes that the sum is over **nearest neighbors**.
- h is an external **magnetic field**.
- S_i is the spin at site i, which can be ± 1.



Phenomena Studied:

- **Magnetization**: At low temperatures, the spins tend to align, leading to spontaneous magnetization (ferromagnetism). At high temperatures, thermal fluctuations randomize the spins, resulting in no net magnetization (paramagnetism).
- **Phase Transition**: The Ising model exhibits a **second-order phase transition** at a critical temperature. For example, in the 2D Ising model, there's a critical temperature T_c below which the system has a non-zero magnetization (ordered phase), and above which the magnetization vanishes (disordered phase).

Variations:

- **1D Ising Model**: Does not show a phase transition at finite temperatures.
- **2D Ising Model**: Exhibits a well-known phase transition with spontaneous magnetization below the critical temperature.
- **3D Ising Model**: Also exhibits a phase transition, but the exact solution is more difficult than in 2D.

Quantum Error Correction

nahhh

Citations

Waleed, Syed & Ullah, Inam & Khan, Wali Ullah & Khan, Ullah & Ateeq, · & Rehman, Ateeq & Rahman, Taj & Li, Shanbin. (2021). Resource allocation of 5G network by exploiting particle swarm optimization. Iran Journal of Computer Science. 4. 10.1007/s42044-021-00091-5.

https://www.fostshop.com/?ggcid=932830

Bonyadi, M. R.; Michalewicz, Z. (2017). "Particle swarm optimization for single objective continuous space problems: a review". *Evolutionary Computation*. **25** (1): 1–54. doi:10.1162/EVCO_r_00180. PMID 26953883. S2CID 8783143.

Kennedy, J.; Eberhart, R. (1995). "Particle Swarm Optimization". *Proceedings of IEEE International Conference on Neural Networks*. Vol. IV. pp. 1942–1948. doi:10.1109/ICNN.1995.488968.

Shi, Y.; Eberhart, R.C. (1998). "A modified particle swarm optimizer". *Proceedings of IEEE International Conference on Evolutionary Computation*. pp. 69–73. doi:10.1109/ICEC.1998.699146.

Poli, R. (2008). "Analysis of the publications on the applications of particle swarm optimisation" (PDF). *Journal of Artificial Evolution and Applications*. **2008**: 1–10. doi:10.1155/2008/685175.

Clerc, M.; Kennedy, J. (2002). "The particle swarm - explosion, stability, and convergence in a multidimensional complex space". *IEEE Transactions on Evolutionary Computation*. **6** (1): 58–73. CiteSeerX 10.1.1.460.6608. doi:10.1109/4235.985692.