Week 3: Entanglement, Teleportation, EPR Paradox

COMS 4281 (Fall 2024)

Admin

1. Practice problem sheet available, quiz on Gradescope. Quizzes should be done individually.
2. Pset1 due October 6, 11:59pm.
3. Use EdStem to find pset collaborators. **However you must write your own solutions**.

Upcoming Events

- This Sunday: NYC HAQ at Columbia.
  - Talks from JP Morgan, NVIDIA, and Wells Fargo about their quantum research (11 - 1pm, Davis Auditorium).
  - **Need a couple student volunteers to help!**
- **Seminar**: Quantum Science with Tweezer Arrays.
  - When, where: Monday, Sept 23, 12:30pm, Pupin 8th floor.
  - Who: Manuel Endres (Caltech).

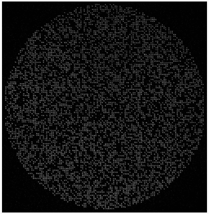
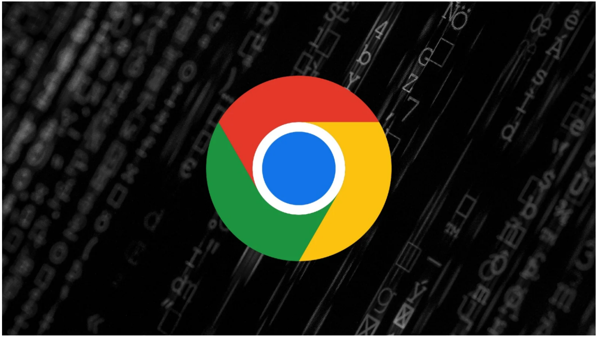


Figure 1: 6000 cesium atoms

In other news...

Chrome switching to NIST-approved ML-KEM quantum encryption

By **Bill Toulas** September 16, 2024 12:22 PM 2



Google is updating the post-quantum cryptography used in the Chrome browser to protect against TLS attacks using quantum computers and to mitigate store-now-decrypt-later attacks.

The upcoming change will swap Kyber used in hybrid key exchanges to a newer, and slightly modified version, renamed as Module Lattice Key Encapsulation Mechanism (ML-KEM).

Recap: Composite states

If the Hilbert space of one system is $\mathcal{H}_A$, and the Hilbert space of another system is $\mathcal{H}_B$, then the Hilbert space of them together is $\mathcal{H}_A \otimes \mathcal{H}_B$.

Recap: Composite states

If the Hilbert space of one system is $\mathcal{H}_A$, and the Hilbert space of another system is $\mathcal{H}_B$, then the Hilbert space of them together is $\mathcal{H}_A \otimes \mathcal{H}_B$.

A state of the joint system is a unit vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, which can be written as

$$|\psi\rangle = \sum_{\substack{1 \le i \le d_A \\ j \le j \le d_B}} \alpha_{ij} \, |i, j\rangle$$

where d_A, d_B are dimensions of $\mathcal{H}_A, \mathcal{H}_B$, respectively.

Recap: Composite states

Measuring $|\psi\rangle = \sum_{i,j} \alpha_{ij} |i,j\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ yields

$$|i,j\rangle \text{ with probability } |\alpha_{ij}|^2$$

and the joint state of the two systems is now $|i,j\rangle$

Recap: Composite states

Measuring $|\psi\rangle = \sum_{i,j} \alpha_{ij} |i,j\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ yields

$$|i,j\rangle \text{ with probability } |\alpha_{ij}|^2$$

and the joint state of the two systems is now $|i,j\rangle$

Examples: What happens when we measure these two-qubit states?

- $|-\rangle \otimes |-\rangle$.

Recap: Composite states

Measuring $|\psi\rangle = \sum_{i,j} \alpha_{ij} |i,j\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ yields

$$|i,j\rangle \text{ with probability } |\alpha_{ij}|^2$$

and the joint state of the two systems is now $|i,j\rangle$

Examples: What happens when we measure these two-qubit states?

- $|-\rangle \otimes |-\rangle$.
- $\frac{1}{\sqrt{6}} |0,0\rangle + \frac{1}{\sqrt{2}} |0,1\rangle + \frac{1}{\sqrt{3}} |1,1\rangle$.

Partial Measurements

Partial measurements

What happens if we only measure the second half of the system (i.e. the qubit in Hilbert space $\mathcal{H}_B$)?

1. What should the distribution of outcomes be?

Partial measurements

What happens if we only measure the second half of the system (i.e. the qubit in Hilbert space $\mathcal{H}_B$)?

1. What should the distribution of outcomes be?
2. What should the state of the system be conditioned on a specific outcome?

Partial measurements

Example: Measuring second qubit of $|\psi\rangle = |-\rangle \otimes |-\rangle$.

- Distribution of outcomes:

- Post-measurement state given outcome $|b\rangle$:

Partial measurements

Example: Measuring second qubit of $|\psi\rangle = |-\rangle \otimes |-\rangle$.

- Distribution of outcomes:

$$|0\rangle, |1\rangle \text{ with equal probability}$$

- Post-measurement state given outcome $|b\rangle$:

$$|-\rangle \otimes |b\rangle$$

Partial measurements

Example: Measuring second qubit of $|\psi\rangle = |-\rangle \otimes |-\rangle$.

- Distribution of outcomes:

$$|0\rangle, |1\rangle \text{ with equal probability}$$

- Post-measurement state given outcome $|b\rangle$:

$$|-\rangle \otimes |b\rangle$$

Since the two qubits are **unentangled**, measuring second qubit does not affect first qubit!

Partial measurements

Example: Measuring second qubit of
$|\psi\rangle = \frac{1}{\sqrt{6}}|0,0\rangle + \frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{3}}|1,1\rangle$.

- Distribution of outcomes:

- Post-measurement state given outcome $|0\rangle$:

- Post-measurement state given outcome $|1\rangle$:

Partial measurements

Example: Measuring second qubit of
$|\psi\rangle = \frac{1}{\sqrt{6}}|0,0\rangle + \frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{3}}|1,1\rangle$.

- Distribution of outcomes:

$$|0\rangle \text{ with probability } \frac{1}{6}, \quad |1\rangle \text{ with probability } \frac{5}{6}$$

- Post-measurement state given outcome $|0\rangle$:

- Post-measurement state given outcome $|1\rangle$:

Partial measurements

Example: Measuring second qubit of
$|\psi\rangle = \frac{1}{\sqrt{6}}|0,0\rangle + \frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{3}}|1,1\rangle$.

- Distribution of outcomes:

$$|0\rangle \text{ with probability } \frac{1}{6}, \quad |1\rangle \text{ with probability } \frac{5}{6}$$

- Post-measurement state given outcome $|0\rangle$:

$$|0,0\rangle$$

- Post-measurement state given outcome $|1\rangle$:

Partial measurements

Example: Measuring second qubit of
$|\psi\rangle = \frac{1}{\sqrt{6}}|0,0\rangle + \frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{3}}|1,1\rangle$.

- Distribution of outcomes:

$$|0\rangle \text{ with probability } \frac{1}{6}, \quad |1\rangle \text{ with probability } \frac{5}{6}$$

- Post-measurement state given outcome $|0\rangle$:

$$|0,0\rangle$$

- Post-measurement state given outcome $|1\rangle$:

$$\left(\sqrt{\frac{3}{5}}|0\rangle + \sqrt{\frac{2}{5}}|1\rangle\right) \otimes |1\rangle$$

Partial measurements

Why does this make sense?

Outcome distribution: The outcome distribution of measuring a single qubit should be consistent with the scenario when we measure *both* qubits.

Why does this make sense?

Outcome distribution: The outcome distribution of measuring a single qubit should be consistent with the scenario when we measure *both* qubits.

In other words, the following two distributions are the same:

1. Measuring qubit $\#2$.
2. Measuring both qubits, and taking the marginal distribution of the second qubit.

Partial measurements

Why does this make sense?

Post-measurement states: The post-measurement state of the unmeasured qubit should be *consistent* with the measured qubit.

Partial measurements

Why does this make sense?

Post-measurement states: The post-measurement state of the unmeasured qubit should be *consistent* with the measured qubit.

Think of it as a quantum analogue of "Bayesian updating": when we learn the outcome of measuring the second qubit, the distribution of measuring the first qubit changes.

Partial measurements

Formal recipe for analyzing partial measurements on second qubit: first, re-arrange terms:

$$|\psi\rangle = \sum_{i,j} \alpha_{ij} |i, j\rangle = \sum_{j} \left(\sum_{i} \alpha_{ij} |i\rangle \right) \otimes |j\rangle$$

Partial measurements

Let $\beta_j = \sqrt{\sum_i |\alpha_{ij}|^2}$, then we can re-write the sum as

$$|\psi\rangle = \sum_j \beta_j \left(\sum_i \frac{\alpha_{ij}}{\beta_j} |i\rangle \right) \otimes |j\rangle \ .$$

Partial measurements

Let $\beta_j = \sqrt{\sum_i |\alpha_{ij}|^2}$, then we can re-write the sum as

$$|\psi\rangle = \sum_j \beta_j \left(\sum_i \frac{\alpha_{ij}}{\beta_j} |i\rangle \right) \otimes |j\rangle \ .$$

Note that $\sum_i \frac{\alpha_{ij}}{\beta_j} |i\rangle$ is a normalized quantum state on $\mathcal{H}_A$.

Partial measurements

Now, if we measure system $\mathcal{H}_B$, we'll see outcome $|j\rangle$ with probability

$$\beta_j^2 = \sum_i |\alpha_{ij}|^2$$

And the state of the first system after seeing $|j\rangle$ is

$$\frac{1}{\beta_j} \sum_i \alpha_{ij} |i\rangle \ .$$

Quantum Teleportation

Quantum teleportation

Imagine Alice and Bob are friends, and Alice has a state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ that she wants to share with Bob.

Quantum teleportation

Imagine Alice and Bob are friends, and Alice has a state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ that she wants to share with Bob. However Bob is really far away, and they can only communicate classically (so Alice can't just hand Bob her qubit). Can Alice transfer her exact qubit to Bob somehow?

Quantum teleportation

Imagine Alice and Bob are friends, and Alice has a state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ that she wants to share with Bob. However Bob is really far away, and they can only communicate classically (so Alice can't just hand Bob her qubit). Can Alice transfer her exact qubit to Bob somehow?

She could try to call Bob over the phone and send a classical description of $|\psi\rangle$, but that could require an infinite number of bits if $|\psi\rangle$ has amplitudes that use transcendental numbers.

Quantum teleportation

If Alice and Bob preshare quantum entanglement, then Alice can **teleport** $|\psi\rangle$ to Bob.

Quantum teleportation

If Alice and Bob preshare quantum entanglement, then Alice can **teleport** $|\psi\rangle$ to Bob.

Suppose one year ago, Alice and Bob were in the same quantum lab, and they generated the entangled state

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \,.$$

Alice takes the first qubit, Bob takes the second qubit and they go their separate ways.

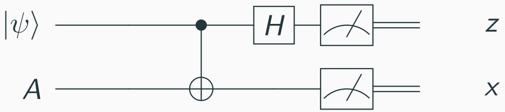
Quantum teleportation

Fast forward to today, when Alice gets a gift qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$.

Quantum teleportation

Fast forward to today, when Alice gets a gift qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

She performs the following circuit on her two qubits:



where A denotes Alice's half of the EPR pair, and the measurement outcomes are denoted $z, x \in \{0, 1\}$ respectively.

Quantum teleportation

Alice calls up Bob over the phone: "I just teleported $|\psi\rangle$ over to you using the EPR pair we split a year ago."

Quantum teleportation

Alice calls up Bob over the phone: "I just teleported $|\psi\rangle$ over to you using the EPR pair we split a year ago."

Bob: "Nice! What corrections do I need to do?"

Quantum teleportation

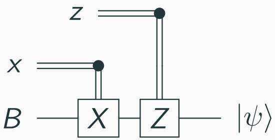
Alice calls up Bob over the phone: “I just teleported $|\psi\rangle$ over to you using the EPR pair we split a year ago.”

Bob: “Nice! What corrections do I need to do?”

Alice tells Bob the bits z, x.

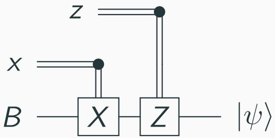
Quantum teleportation

Bob then applies the following gates to his EPR qubit B, depending on the values of x, z.



Quantum teleportation

Bob then applies the following gates to his EPR qubit B, depending on the values of x, z.

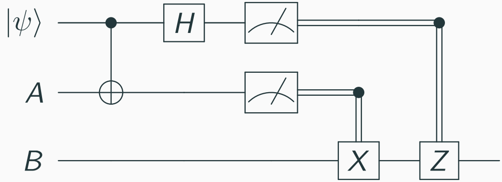


Recall that

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ .$$

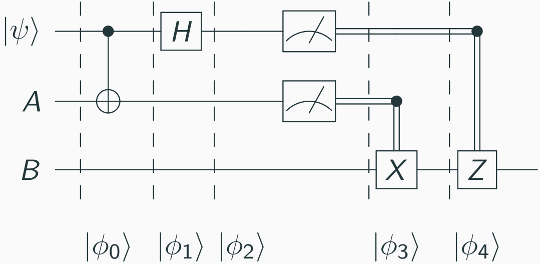
Quantum teleportation

Viewing the entire process as a circuit, this looks like

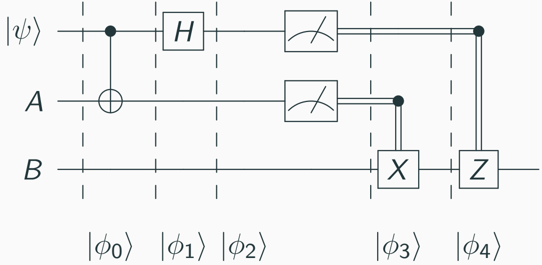


Quantum teleportation

We analyze it step by step:



We analyze it step by step:



Let's do this together on the board!

Does this violate the No-Cloning Theorem?

Does this violate the No-Cloning Theorem?

No! Alice has measured her qubits, so no longer possesses $|\psi\rangle$.

Quantum teleportation

Does this violate the No-Cloning Theorem?

No! Alice has measured her qubits, so no longer possesses $|\psi\rangle$.

Can this be used to send information faster than speed of light?

Quantum teleportation

Does this violate the No-Cloning Theorem?

No! Alice has measured her qubits, so no longer possesses $|\psi\rangle$.

Can this be used to send information faster than speed of light?

No! In order for Bob to recover $|\psi\rangle$, Alice needs to classically transmit the "correction bits" z, x to Bob, which is limited by the speed of light.

Quantum teleportation

Does this violate the No-Cloning Theorem?

No! Alice has measured her qubits, so no longer possesses $|\psi\rangle$.

Can this be used to send information faster than speed of light?

No! In order for Bob to recover $|\psi\rangle$, Alice needs to classically transmit the "correction bits" z, x to Bob, which is limited by the speed of light.

Both the preshared entanglement, and the classical communication are necessary for quantum teleportation to work.

Public Service Announcement

Entanglement does not allow for faster-than-light communication!

Nonstandard Measurements

Nonstandard measurements

So far, measurement of a quantum state $|\psi\rangle = \sum_x \alpha_x |x\rangle$ meant obtaining the classical state $|x\rangle$ with probability $|\alpha_x|^2$.

Nonstandard measurements

So far, measurement of a quantum state $|\psi\rangle = \sum_x \alpha_x |x\rangle$ meant obtaining the classical state $|x\rangle$ with probability $|\alpha_x|^2$.

This is what we call a **standard basis measurement** or a **computational basis measurement**: the outcomes are the standard basis (a.k.a. computational basis) vectors

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Nonstandard measurements

But often we'd like to measure a quantum state in a different basis, where the outcomes are quantum states that are *not* computational basis states.

Nonstandard measurements

But often we'd like to measure a quantum state in a different basis, where the outcomes are quantum states that are *not* computational basis states.

Another basis for $\mathbb{C}^2$ is $\{|+\rangle, |-\rangle\}$ (called the **diagonal** or **Hadamard basis**). This is an orthonormal basis, and that means we can also measure with respect to this basis.

Nonstandard measurements

But often we'd like to measure a quantum state in a different basis, where the outcomes are quantum states that are *not* computational basis states.

Another basis for $\mathbb{C}^2$ is $\{|+\rangle, |-\rangle\}$ (called the **diagonal** or **Hadamard basis**). This is an orthonormal basis, and that means we can also measure with respect to this basis.

Measuring in diagonal basis

Let $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ denote a qubit state. What happens if we measure in the diagonal basis?

Measuring in diagonal basis

Let $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ denote a qubit state. What happens if we measure in the diagonal basis?

Rewrite $|\psi\rangle$ as a linear combination of the $\{|+\rangle\,, |-\rangle\}$ basis:

$$|\psi\rangle = \alpha\frac{\sqrt{2}}{2}\Big(\,|+\rangle + |-\rangle\,\Big) + \beta\frac{\sqrt{2}}{2}\Big(\,|+\rangle - |-\rangle\,\Big)$$

Measuring in diagonal basis

Let $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ denote a qubit state. What happens if we measure in the diagonal basis?

Rewrite $|\psi\rangle$ as a linear combination of the $\{|+\rangle\,,|-\rangle\}$ basis:

$$|\psi\rangle = \alpha\frac{\sqrt{2}}{2}\Big(\,|+\rangle + |-\rangle\,\Big) + \beta\frac{\sqrt{2}}{2}\Big(\,|+\rangle - |-\rangle\,\Big)$$

$$= \frac{\sqrt{2}}{2}\Big(\alpha + \beta\Big)\,|+\rangle + \frac{\sqrt{2}}{2}\Big(\alpha - \beta\Big)\,|-\rangle$$

Measuring in diagonal basis

The probability of getting $|+\rangle$ outcome is thus

$$\left(\frac{\sqrt{2}}{2}\right)^2 \cdot \left|\alpha + \beta\right|^2$$

and similarly the probability of $|-\rangle$ outcome is

$$\left(\frac{\sqrt{2}}{2}\right)^2 \cdot \left|\alpha - \beta\right|^2$$

Another perspective

There's also a geometric way to think about it:

$$\Pr\left[\text{measuring } |\psi\rangle \text{ in diagonal basis yields } |+\rangle\right] = \text{overlap of } |\psi\rangle \text{ and } |+\rangle$$

Another perspective

There's also a geometric way to think about it:

$$\Pr\left[\text{measuring } |\psi\rangle \text{ in diagonal basis yields } |+\rangle\right] = \left|\left\langle + \,\middle|\, \psi \right\rangle\right|^2$$

Another perspective

There's also a geometric way to think about it:

$$\Pr\left[\text{measuring } |\psi\rangle \text{ in diagonal basis yields } |+\rangle\right] = \left|\left\langle + \,\middle|\, \psi \right\rangle\right|^2$$

Similarly,

$$\Pr\left[\text{measuring } |\psi\rangle \text{ in diagonal basis yields } |-\rangle\right] = \left|\left\langle - \,\middle|\, \psi \right\rangle\right|^2$$

General formula for measuring in a basis

Let $|\psi\rangle \in \mathbb{C}^d$ be a quantum state. Let $B = \{|b_1\rangle, \ldots, |b_d\rangle\}$ be an **orthonormal basis** for $\mathbb{C}^d$.

Then measuring $|\psi\rangle$ with respect to basis B yields outcome $|b_j\rangle$ with probability

$$\left|\left\langle b_j \middle| \psi \right\rangle\right|^2$$

and the post-measurement state is $|b_j\rangle$.

Implementing measurements in different bases

How do you actually measure in a different basis? For example in Qiskit you only get the ability to measure in the standard basis.

Implementing measurements in different bases

How do you actually measure in a different basis? For example in Qiskit you only get the ability to measure in the standard basis.

Measuring $|\psi\rangle$ in a basis B is **equivalent** to

1. Apply a unitary V that maps B to standard basis (i.e. $|b_j\rangle \rightarrow |j\rangle$).
2. Measure in standard basis.

Implementing measurements in different bases

How do you actually measure in a different basis? For example in Qiskit you only get the ability to measure in the standard basis.

Measuring $|\psi\rangle$ in a basis B is **equivalent** to

1. Apply a unitary V that maps B to standard basis (i.e. $|b_j\rangle \to |j\rangle$).
2. Measure in standard basis.

Probability of getting $|j\rangle$ in this new process is the same as getting $|b_j\rangle$ when measuring in basis B.

Partial measurements plus nonstandard measurements

Let's combine the two concepts! Let $|\psi\rangle = \sum_{i,j} \alpha_{ij} |i\rangle \otimes |j\rangle$ denote a two-qubit state. Say we measure the first qubit with respect to basis $\{|b_0\rangle, |b_1\rangle\}$.

Partial measurements plus nonstandard measurements

Let's combine the two concepts! Let $|\psi\rangle = \sum_{i,j} \alpha_{ij} |i\rangle \otimes |j\rangle$ denote a two-qubit state. Say we measure the first qubit with respect to basis $\{|b_0\rangle, |b_1\rangle\}$.

Measurement rule: Probability of obtaining outcome $|b_0\rangle$ is the **length squared** of the vector

$$|a\rangle = (\langle b_0| \otimes I) |\psi\rangle = \sum_{i,j} \alpha_{ij} \langle b_0 \mid i\rangle \ |j\rangle .$$

Note this is a vector in $\mathbb{C}^2$, not $\mathbb{C}^2 \otimes \mathbb{C}^2$. It's a **partial inner product**.

Partial measurements plus nonstandard measurements

The probability is thus:

$$\Big\| \, |a\rangle \, \Big\|^2 = \sum_j \Big| \sum_i \alpha_{ij} \langle b_0 \mid i\rangle \Big|^2$$

Partial measurements plus nonstandard measurements

The probability is thus:

$$\Big\| \, |a\rangle \, \Big\|^2 = \sum_j \Big| \sum_i \alpha_{ij} \langle b_0 \mid i \rangle \Big|^2$$

The **post-measurement** state of both qubits is

$$|b_0\rangle \otimes \frac{|a\rangle}{\| \, |a\rangle \, \|}.$$

Partial measurements plus nonstandard measurements

Let's work through an example:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,.$$

Measure the **first** qubit in the **diagonal basis**.

Partial measurements plus nonstandard measurements

Let's work through an example:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,.$$

Measure the **first** qubit in the **diagonal basis**.

- What is the probability the outcome is $|+\rangle$? Or $|-\rangle$?
- What is the post-measurement state in either case?

Next time

Heisenberg's uncertainty principle, EPR paradox, Bell's Theorem.

Heisenberg Uncertainty Principle

Heisenberg Uncertainty Principle

Popular science version: can't exactly know both the position and momentum of a particle simultaneously.

Heisenberg Uncertainty Principle

In quantum information theory terms: it is not possible for a qubit $|\psi\rangle \in \mathbb{C}^2$ to be simultaneously determined in both the **standard** basis and the **diagonal basis**.

Heisenberg Uncertainty Principle

In quantum information theory terms: it is not possible for a qubit $|\psi\rangle \in \mathbb{C}^2$ to be simultaneously determined in both the **standard** basis and the **diagonal basis**.

In other words, if measuring $|\psi\rangle$ in standard basis yields a deterministic outcome, then it **cannot** have a deterministic outcome if measured according to diagonal basis.

Heisenberg Uncertainty Principle

Important point: it's not about what happens if you **sequentially** measure the state $|\psi\rangle$ (what happens then?).

Heisenberg Uncertainty Principle

Important point: it's not about what happens if you **sequentially** measure the state $|\psi\rangle$ (what happens then?).

It's reasoning about **counterfactual scenarios**: measuring $|\psi\rangle$ in the standard basis, **or** measuring $|\psi\rangle$ in the diagonal basis.

Heisenberg Uncertainty Principle

We say that the standard basis and diagonal basis are **incompatible** or **complementary**.

In quantum physics, the position and momentum of a particle correspond to incompatible measurements!