Lecture 8 February 13^{th}, 2025

PART I Fundamental Concepts & Applications in Quantum Information

TODAY CHSH game and Exchanging Quantum Information

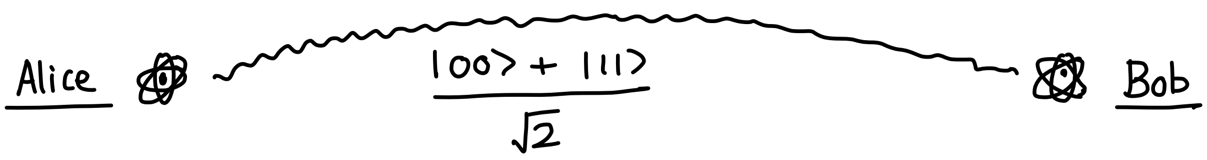
RECAP Bell's Theorem

No local hidden variable theory can be compatible with quantum mechanics

CHSH game

Alice & Bob prepare the Bell state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

They each take one of the qubits & go far away
say Alice goes to Mars & Bob goes to Jupiter

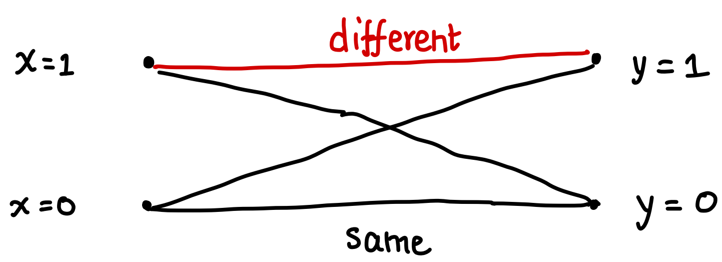


They are both issued a challenge by a referee as follows:

- Challenge to Alice is $x \in \{0,1\}$ and to Bob is $y \in \{0,1\}$ where x and y are independent random bits
- Referee puts the challenge in a box & Alice & Bob look at it at the same time
- They are both given 10 seconds to respond with a bit and Mars is at least 30 light minutes from Jupiter so no time for Alice to secretly communicate with Bob
- The boxes collect their responses and fly back to the referee
- They win the game if Alice's response bit $a \in \{0,1\}$ and Bob's response $b \in \{0,1\}$ satisfy the following

$$a \oplus b = x \wedge y$$

Another way of visualizing what happens in the game is via the following graph



Referee chooses a random edge
Alice & Bob's bit a & b should be different for the red edge and same otherwise to win the game

No deterministic or local hidden variable strategy can win with probability more than $3/4$

What does Quantum Mechanics predict?

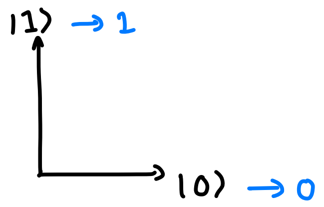
There exists a quantum strategy involving quantum entanglement where Alice & Bob win with probability ≈ 85%

This gives an experiment to rule out local hidden variable theories

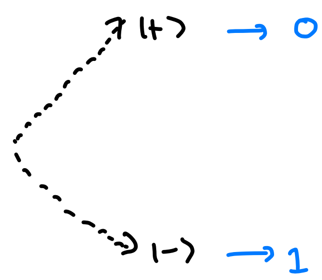
Quantum strategy   Alice ~~~ $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ ~~~ Bob

- Alice and Bob hold one qubit that jointly form an EPR pair
- Alice chooses either basis A_0 if $x=0$ or basis A_1 if $x=1$ to measure her qubit and interprets it as 0 or 1
- Bob chooses either basis B_0 if $y=0$ or basis B_1 if $y=1$ to measure his qubit and interprets it as 0 or 1

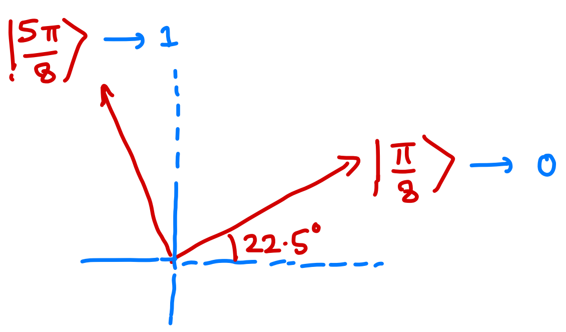
A_0 if $x=0$



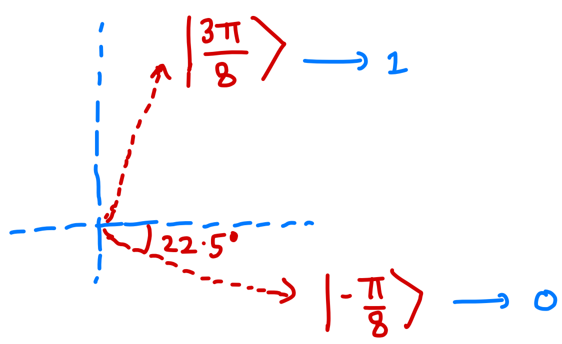
A_1 if $x=1$



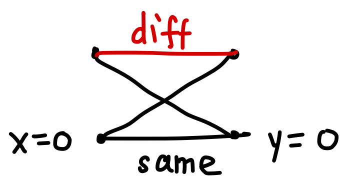
B_0 if $y=0$



B_1 if $y=1$



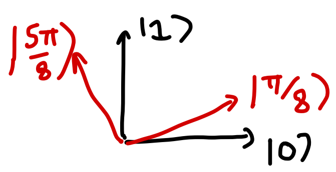
How well does this strategy do?



① Suppose $x=0$ and $y=0$

Alice measures in $\{|0\rangle, |1\rangle\}$ basis

& Bob measures in $\{|\frac{\pi}{8}\rangle, |\frac{5\pi}{8}\rangle\}$ basis



In order to win, Alice & Bob's answer must match

Since the order of measurement does not matter,
when Alice measures $|0\rangle$ with probability $\frac{1}{2}$ & joint state is $|0\rangle \otimes |0\rangle$

To win, Bob must measure his qubit & get the $|\frac{\pi}{8}\rangle$ outcome

Since his qubit is now in $|0\rangle$ state, he gets this outcome with probability

$$|\langle 0|\tfrac{\pi}{8}\rangle|^2 = \cos^2(\pi/8) = 0.853$$

when Alice measures $|1\rangle$ with probability $\frac{1}{2}$ & joint state is $|1\rangle \otimes |1\rangle$

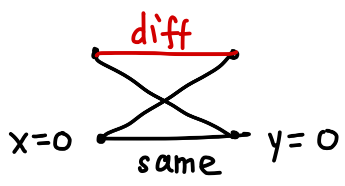
To win, Bob must measure his qubit & get the $|\frac{5\pi}{8}\rangle$ outcome

Since his qubit is now in $|1\rangle$ state, he gets this outcome with probability

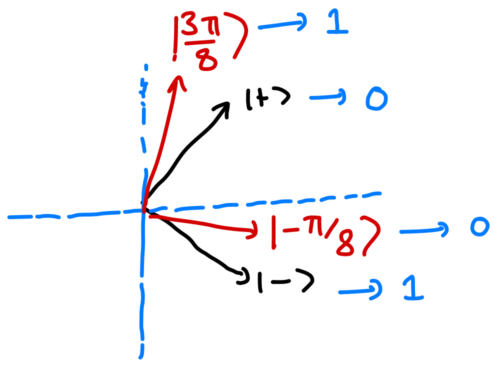
$$|\langle 1|\tfrac{5\pi}{8}\rangle|^2 = \cos^2(\pi/8) = 0.8535$$

In either case, they win with probability $\cos^2(\frac{\pi}{8}) \approx 0.8535$

② Let's take a different case



① Suppose $x=1$ and $y=1$
Alice measures in $\{|\pm\rangle\}$ basis
& Bob measures in $\{|-\frac{\pi}{8}\rangle, |\frac{3\pi}{8}\rangle\}$ basis



In order to win, Alice & Bob's answer must differ

when Alice measures $|+\rangle$ with probability $\frac{1}{2}$ & joint state is $|+\rangle \otimes |+\rangle$

To win, Bob must measure his qubit & get the $|\frac{3\pi}{8}\rangle$ outcome

Since his qubit is now in $|+\rangle$ state, he gets this outcome with probability

$$|\langle +|\tfrac{3\pi}{8}\rangle|^2 = \cos^2(\pi/8) = 0.853$$

when Alice measures $|-\rangle$ with probability $\frac{1}{2}$ & joint state is $|-\rangle \otimes |-\rangle$

To win, Bob must measure his qubit & get the $\left|\frac{-\pi}{8}\right\rangle$ outcome

Since his qubit is now in $|-\rangle$ state, he gets this outcome with probability

$$|\langle -|-\pi/8\rangle|^2 = \cos^2(\pi/8) = 0.853$$

Checking the other two cases, you can see that they always win with probability $\cos^2\left(\frac{\pi}{8}\right) \approx 0.8535$

This shows that there is quantum advantage in the CHSH game

It turns out that $\cos^2\left(\frac{\pi}{8}\right)$ is the best win probability for quantum strategies

This is called Tsirelson's theorem and we won't prove it in this course

Quantum advantage in the CHSH game comes from shared entanglement

Local measurements on entangled states give rise to correlations that are stronger than any classical correlations

These correlations are often called non-local

Experimental Confirmation of Bell's Theorem

Since 1970s many experiments conducted and all demonstrate winning probabilities of more than 80% which cannot be explained with Local Hidden Variable theories.

Conclusion: ① Quantum Mechanics is fundamentally a non-classical theory & Nature seems to be quantum mechanical

② Nature is inherently probabilistic

In 2015, a "loophole free" Bell test was conducted for the first time

This avoids (1) Locality loophole

(2) Detection loophole

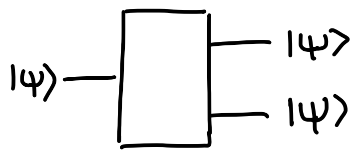
2022 Nobel Prize in Physics

Applications: Randomness generation, Verifying quantum computers, Quantum cryptography

How to exchange quantum information?

No Cloning Theorem

There is no physical device that does this



} unentangled copies

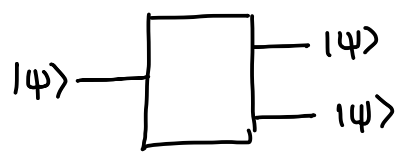
for all qubit states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

This is not inherently quantum as there is a similar theorem you can prove if you have probabilistic bits

There are some similar looking things you can do

e.g. you can make as many copies of $|0\rangle$, $|1\rangle$, $|+\rangle$, or any fixed state

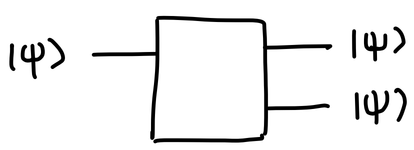
e.g.



is possible if $|\psi\rangle \in \{|0\rangle, |1\rangle\}$

How would you do this ?

e.g.



is possible if $|\psi\rangle$ is limited to perfectly distinguishable states e.g. $\{|+\rangle, |-\rangle\}$

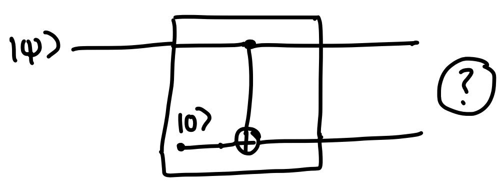
Corollary of No-cloning Theorem

Unlearnability of a qubit (from one copy)

You can't learn the amplitudes $\alpha|0\rangle + \beta|1\rangle$

Attempts at making a cloner

Let us consider the following



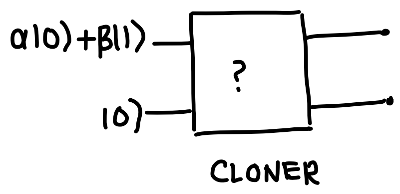
CLONER?

Does this work ?

Input	Output
$\|0\rangle$	$\|00\rangle$
$\|1\rangle$	$\|11\rangle$
$\|+\rangle$	$\|{+}{+}\rangle$? but we get the EPR pair $\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
$\alpha\|0\rangle+\beta\|1\rangle$	Want $\alpha^2\|00\rangle + \alpha\beta\|01\rangle + \beta\alpha\|10\rangle + \beta^2\|11\rangle$ but get $\alpha\|00\rangle + \beta\|11\rangle$

Proof of No-cloning Theorem

$\boxed{\text{Intuitive}}$ (But not a complete proof)



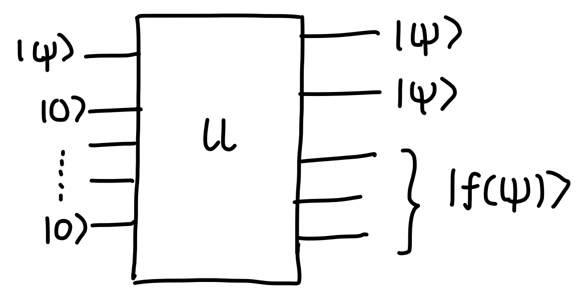
$\alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$

$$\begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix} \longrightarrow \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \beta\alpha \\ \beta^2 \end{bmatrix}$$ This is not a linear map

But one can do measurements & use extra qubits as well

$\boxed{\text{The Proof}}$ Suppose $\exists$ a cloner

(without measurements)



$$U(|\psi\rangle \otimes \overbrace{|0\rangle \cdots \otimes |0\rangle}^{n-1}) = |\psi\rangle \otimes |\psi\rangle \otimes |f(\psi)\rangle$$

Let's apply U to $|0\rangle$, $|1\rangle$ and $|+\rangle$

$$U(|0\rangle \otimes |0\rangle^{\otimes n-1}) = |00\rangle \otimes |f(0)\rangle = ⓐ$$
$$U(|1\rangle \otimes |0\rangle^{\otimes n-1}) = |11\rangle \otimes |f(1)\rangle = ⓑ$$
$$U(|+\rangle \otimes |0\rangle^{\otimes n-1}) = |{+}{+}\rangle \otimes |f(+)\rangle = ⓒ$$

Since U is a linear map, $\frac{1}{\sqrt{2}}ⓐ + \frac{1}{\sqrt{2}}ⓑ = ⓒ$

$$\frac{1}{\sqrt{2}} a + \frac{1}{\sqrt{2}} b = \frac{1}{\sqrt{2}} |00\rangle \otimes |f(0)\rangle + \frac{1}{\sqrt{2}} |11\rangle \otimes |f(1)\rangle$$

$$c = \left(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right) \otimes |f(+)\rangle$$

But these two states are not equal

e.g. if we measure the first two qubits

$\frac{1}{\sqrt{2}} a + \frac{1}{\sqrt{2}} b$: see "00" or "11" w/prob $\frac{1}{2}$ each

c : see all 4 outcomes w/prob $\frac{1}{4}$ each

<u>Classical comparison</u> Can we clone a biased coin ?

If we can only toss it once $\longrightarrow$ No!

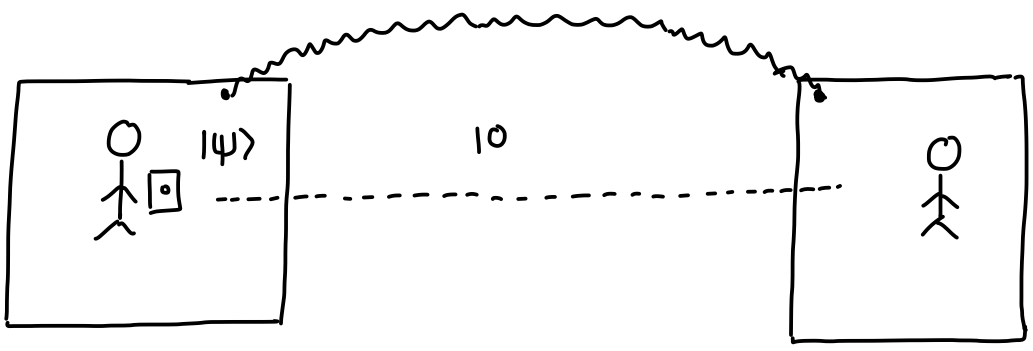
If we can toss it many times, we can estimate the bias

The situation in the quantum case is similar to having a one-time flippable coin and you cannot look at the coin either

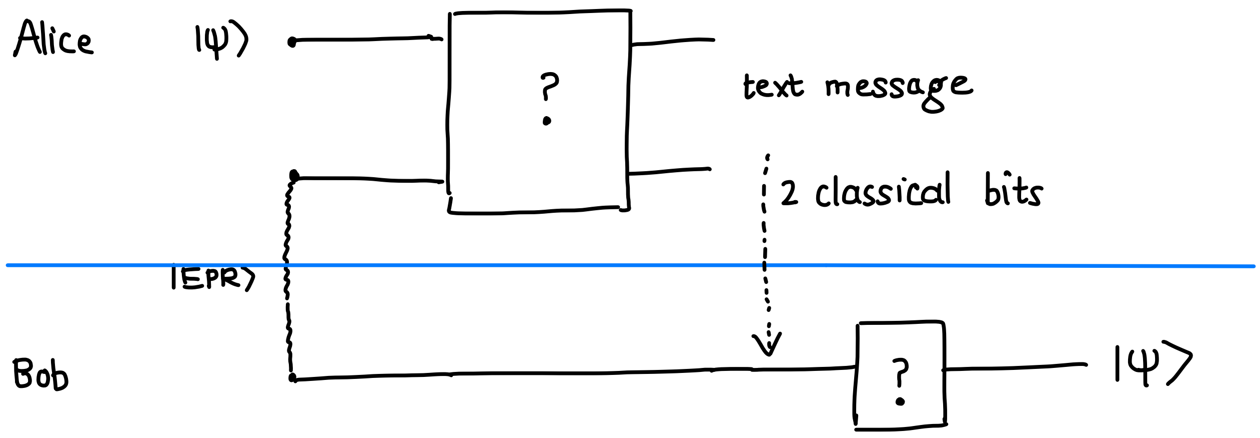
But if you have access to many copies of the quantum state, you can learn it ! This is called quantum tomography

Quantum Teleportation

Suppose Alice has a qubit $|\psi\rangle$ in an unknown state and she wants to send it to Bob
- They can only exchange classical messages
- They share an EPR pair



Alice sends Bob two bits
Bob has the state $|\psi\rangle$ afterwards
Alice's copy is destroyed



$\boxed{\text{Moral}}$ "1 ebit + 2 classical bits $\geq$ 1 qubit"

Even if Alice knew the description of $|\psi\rangle$ you would think she needs to send many bits to describe the amplitudes, but here she only sends two bits & Bob gets a perfect copy of $|\psi\rangle$

NEXT TIME How does this work ?
How to exchange quantum information ?