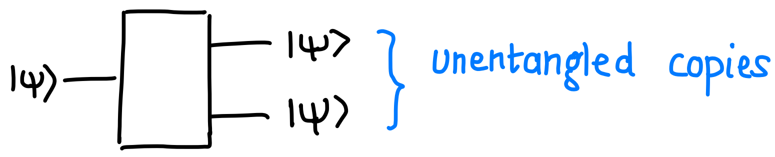
Lecture 8 September 14th, 2023

PART I Fundamental Concepts & Applications in Quantum Information

TODAY Exchanging Quantum Information

No Cloning Theorem There is no physical device that does this



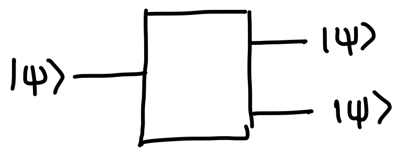
for all qubit states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

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

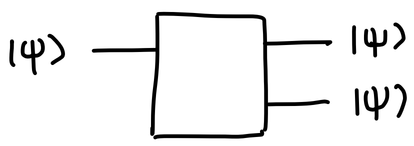
e.g.



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

How would you do this ?

e.g.

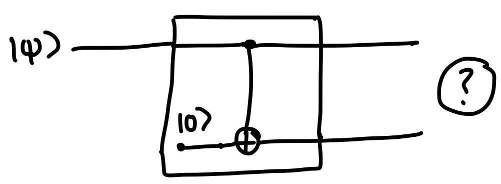


is possible if $|\psi\rangle$ is limited to perfectly distinguishable states e.g. $\{|+\rangle, |-\rangle\}$

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



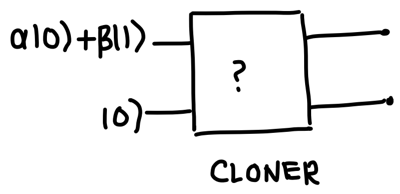
CLONER?

Does this work ?

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

Proof of No-cloning Theorem

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

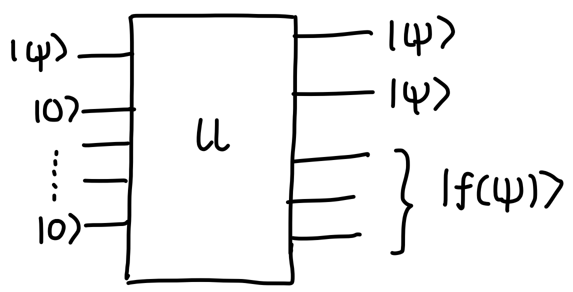


$\alpha^2\lvert 00\rangle + \alpha\beta\lvert 01\rangle + \beta\alpha\lvert 10\rangle + \beta^2\lvert 11\rangle$

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

But one can do measurements & use extra qubits as well

$\boxed{\text{The Proof}}$ (without measurements) Suppose $\exists$ a cloner



$$U(\lvert\psi\rangle \otimes \underbrace{\lvert 0\rangle \cdots \otimes \lvert 0\rangle}_{n-1}) = \lvert\psi\rangle \otimes \lvert\psi\rangle \otimes \lvert f(\psi)\rangle$$

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

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

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

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

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

But these two states are not equal

e.g. if we measure the first two qubits

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

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

Classical comparison   Can we clone a biased coin ?

If we can only toss it once ⟶ No!

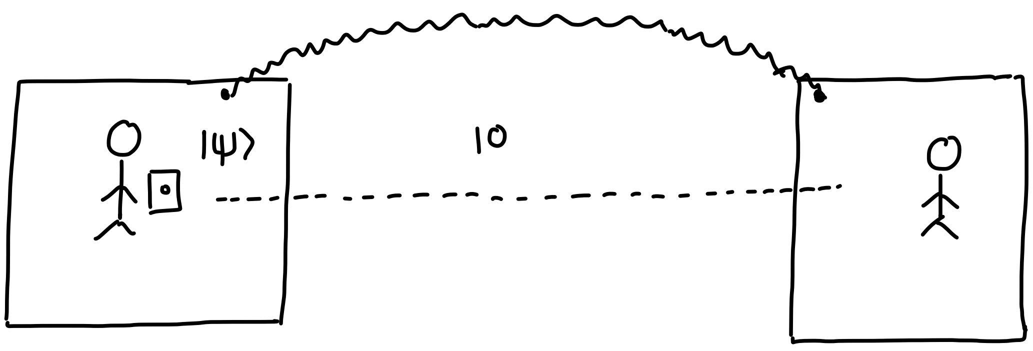
If we can toss it many times, we can estimate the bias

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

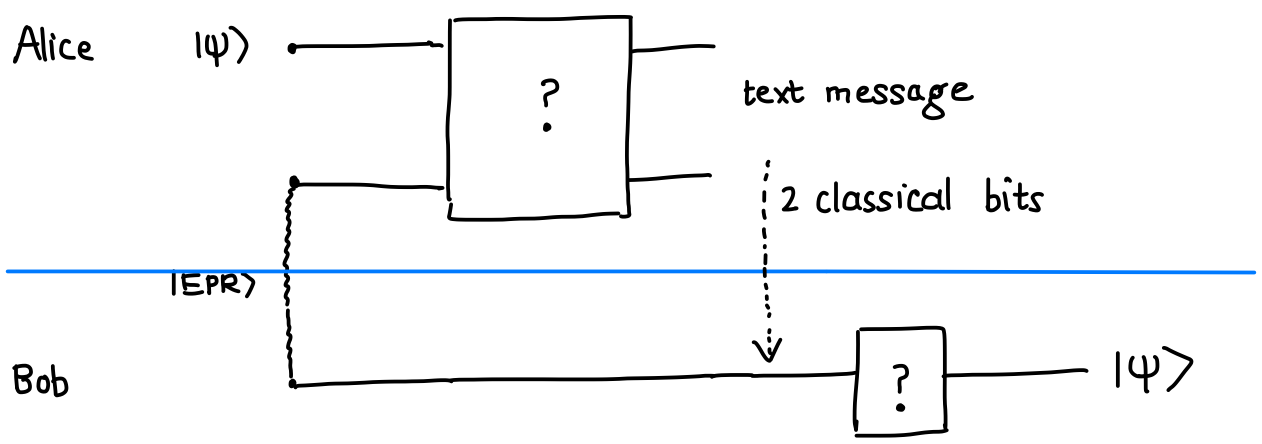
But if you have access to many copies of the quantum state, you can learn it !
This is called quantum tomography

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



Moral "1 ebit + 2 classical bits $\geq$ 1 qubit"

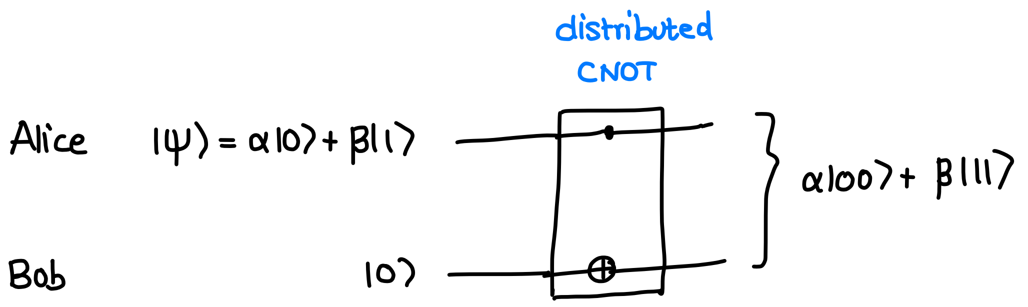
Even if Alice knew the description of $|\psi\rangle$ you would think she needs to send many bits to describe the amplitudes, but here she only sends two bits & Bob gets a perfect copy of $|\psi\rangle$

How does this work ?

Suppose that Alice and Bob could do a distributed CNOT gate where Alice has the control qubit & Bob has the target

We will describe how they can do this in a bit but let's proceed assuming this

Why CNOT ? It's the thing that's most similar to copying



At the end Bob is supposed to have $|\psi\rangle$ and Alice's copy is supposed to be destroyed

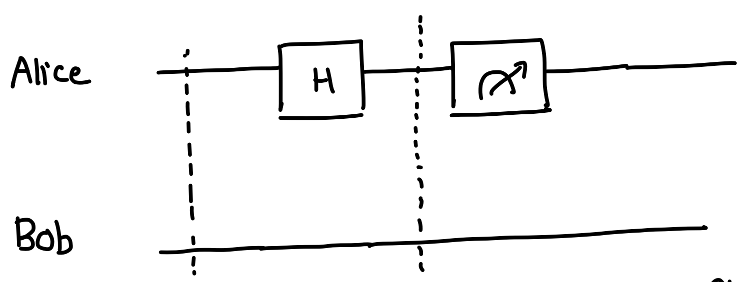
What can she do ? Measure her qubit ?

$\boxed{\text{Try 1}}$ Alice measures in the standard basis $\longrightarrow$ w/prob. $|\alpha|^2$ Bob has $|0\rangle$ Not what

$|\beta|^2$ Bob has $|1\rangle$ we wanted

$\boxed{\text{Try 2}}$ Alice measures in the $|\pm\rangle$ basis

Let's simulate this with "Alice applies a Hadamard gate & measures in the std. basis"



$\alpha|00\rangle + \beta|11\rangle$ $\quad$ $\alpha|{+}0\rangle + \beta|{-}1\rangle = \frac{\alpha}{\sqrt{2}}|00\rangle + \frac{\alpha}{\sqrt{2}}|10\rangle + \frac{\beta}{\sqrt{2}}|01\rangle - \frac{\beta}{\sqrt{2}}|11\rangle$

After Alice measures

$\mathbb{P}[\text{ outcome } 0] = \left|\frac{\alpha}{\sqrt{2}}\right|^2 + \left|\frac{\beta}{\sqrt{2}}\right|^2 = 1/2$

Bob's qubit becomes $\alpha|0\rangle + \beta|1\rangle$ which is $|\psi\rangle$:)

$\mathbb{P}[\text{outcome } 1] = \frac{1}{2}$

Bob's qubit becomes $\alpha|0\rangle - \beta|1\rangle$ $\longrightarrow$ Almost $|\psi\rangle$ but not quite

Alice texts Bob her measurement outcomes

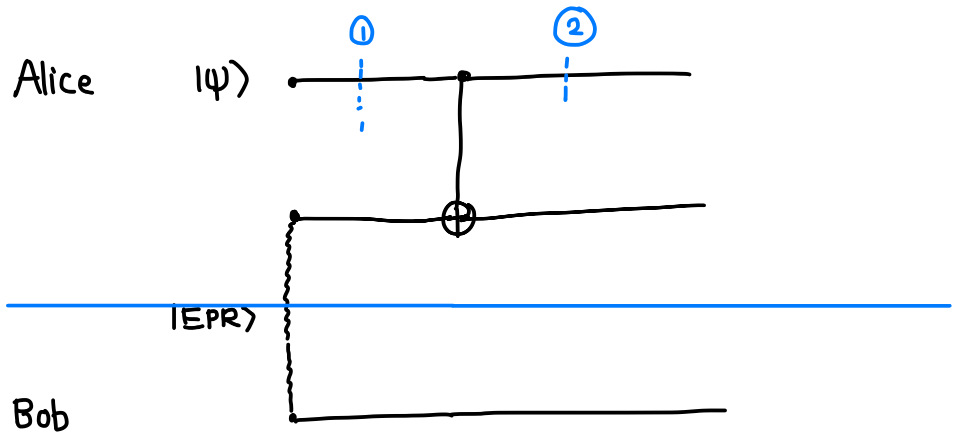
If 0 : Bob does nothing

If 1 : Bob applies the Z gate $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$

& Bob has $|\psi\rangle$:)

Note : Alice's qubit is destroyed after she measures

How do they perform a distributed CNOT without getting together ?



Let's say Alice first does a local CNOT

At time 1 the state of all three particles is

$$(\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

Target

Control

At time 2, the state is $\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle$

Now what ? At the end Alice's wants to do a distributed CNOT with first qubit as control and Bob's qubit as target
She measures the second qubit

$$\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

$\mathbb{P}[\text{outcome "0"}] = \left|\frac{\alpha}{\sqrt{2}}\right|^2 + \left|\frac{\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}$

State of particles 1 & 3 is $\alpha|00\rangle + \beta|11\rangle$ $\longrightarrow$ Distributed CNOT !!!

$\mathbb{P}[\text{outcome "1"}] = \frac{1}{2}$

State of particles 1 & 3 is $\alpha|01\rangle + \beta|10\rangle$:-/ Not quite what we want

But Alice can text Bob what she measured :

if "0" : Bob does nothing

if "1" : Bob applies NOT gate to his qubit

Then, the state is $\alpha|00\rangle + \beta|11\rangle$ $\leftarrow$ They have performed a distributed CNOT!

$\boxed{\text{NEXT TIME}}$ Information Content of qubits & Basics of Quantum Computing