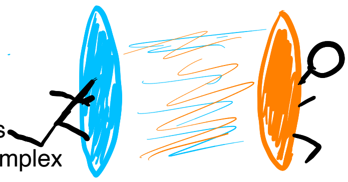
CMPT 476 Lecture 12

Teleportation



With classical bits, it becomes hard to send qubits
nce the amplitudes of the states could be infinitely complex

Previously we saw that shared entanglement allows one to send 2 classical bits by sending only 1 qubit. Today we look at the opposite:

Can we send quantum bits by sending only classical bits?

At first glance it appears impossible...

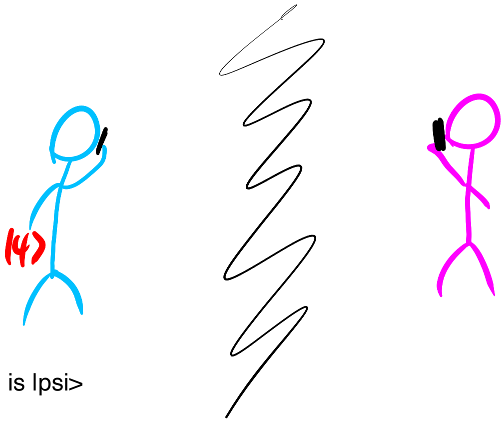
$$\alpha|0\rangle + \beta|1\rangle$$

Communicating the above state classically would require infinite precision since α and β are arbitrary complex numbers. However, the surprising protocol of quantum teleportation in fact allows Alice to "send" Bob an arbitrary qubit using only pre-shared entanglement and 2 classical bits.

Caution:
the content of this lecture may be underwhelming and ruin your enjoyment of science fiction films

(Quantum teleportation)

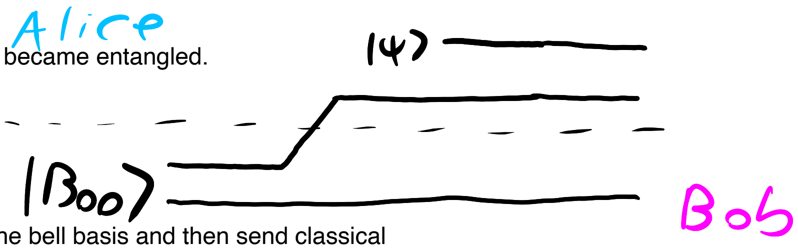
The set up is this: Alice has a qubit $|\psi\rangle$ that she wants to send to Bob, but their only means of communication is a cell phone.



h share B_{00}, but Alice's part of the qubit is lpsi>

She can't send it over the phone because it's stored in the spin of some particle. However, Alice and Bob do share an EPR pair $|B_{00}\rangle$ from last year's Christmas party. We can picture the scenario as a circuit like this:

d phi, and Bob had B_{00}, and they became entangled.



Alice will measure in the bell basis and then send classical bits to box to tell him how to change his state

The idea is to give Bob "instructions" to turn his qubit into $|\psi\rangle$. Figuring out those instructions becomes a little game of shuffling around vectors. First we have to ask what is their joint state?

Suppose $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then

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

Next, without any motivation, we're going to re-write Alice's two qubits over the Bell basis.

Recall from last lecture that

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

Conversly, we have

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

So writing $|\psi\rangle|\beta_{00}\rangle$ with Alice's qubits in the Bell basis gives

$$|\psi\rangle|\beta_{00}\rangle = \frac{1}{2}\Big(\alpha(|\beta_{00}\rangle + |\beta_{10}\rangle)|0\rangle + \beta(|\beta_{01}\rangle - |\beta_{11}\rangle)|0\rangle + \alpha(|\beta_{01}\rangle + |\beta_{11}\rangle)|1\rangle + \beta(|\beta_{00}\rangle - |\beta_{10}\rangle)|1\rangle\Big)$$

Factor out the Bell basis vectors

$$= \frac{1}{2}\Big(|\beta_{00}\rangle\overbrace{(\alpha|0\rangle + \beta|1\rangle)}^{\text{psi}} + |\beta_{01}\rangle\overset{\text{X psi}}{(\alpha|1\rangle + \beta|0\rangle)} + |\beta_{10}\rangle\underset{\text{Z psi}}{(\alpha|0\rangle - \beta|1\rangle)} + |\beta_{11}\rangle\underset{\text{XZ psi}}{(\alpha|1\rangle - \beta|0\rangle)}\Big)$$

When Alice measures, she finds out what state Bob has.
Bob can find out what Alice did and then apply the following operations.

If Alice were to measure her qubits in the Bell basis, this would be the result:

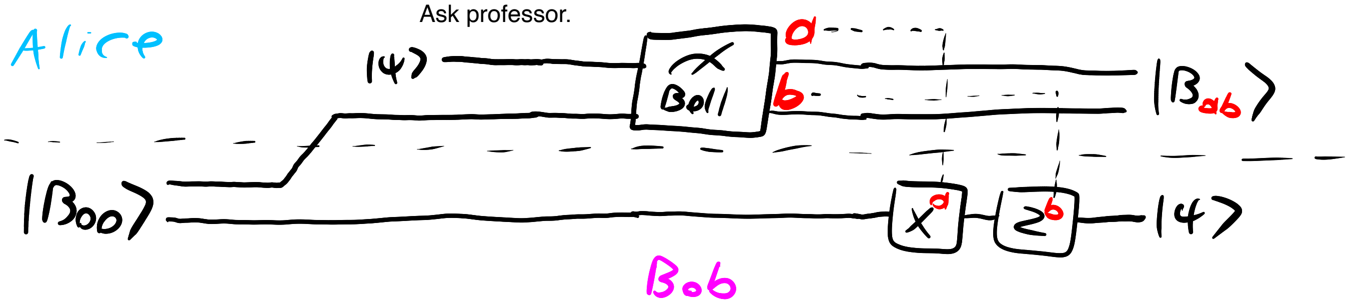
Alice's result	β_{00}	β_{01}	β_{10}	β_{11}
Bob's state	$\alpha|0\rangle + \beta|1\rangle$	$\alpha|1\rangle + \beta|0\rangle$	$\alpha|0\rangle - \beta|1\rangle$	$\alpha|1\rangle - \beta|0\rangle$
	$=$	$=$	$=$	$=$
	$|\psi\rangle$	$X|\psi\rangle$	$Z|\psi\rangle$	$XZ|\psi\rangle$

In every case Bob's state is, up to a local transformation, equal to the teleported state! While Bob doesn't know which of the 4 states he has, Alice can communicate the measurement result using 2 bits over the phone, which will tell Bob the correction he needs to make,

e.g. if Alice sends B_{11}, Bob applies ZX to give $ZX(XZ|\psi\rangle) = ZXXZ|\psi\rangle = |\psi\rangle$

The complete protocol is shown below

This measurement removed the shared entanglement. How? Ask professor.

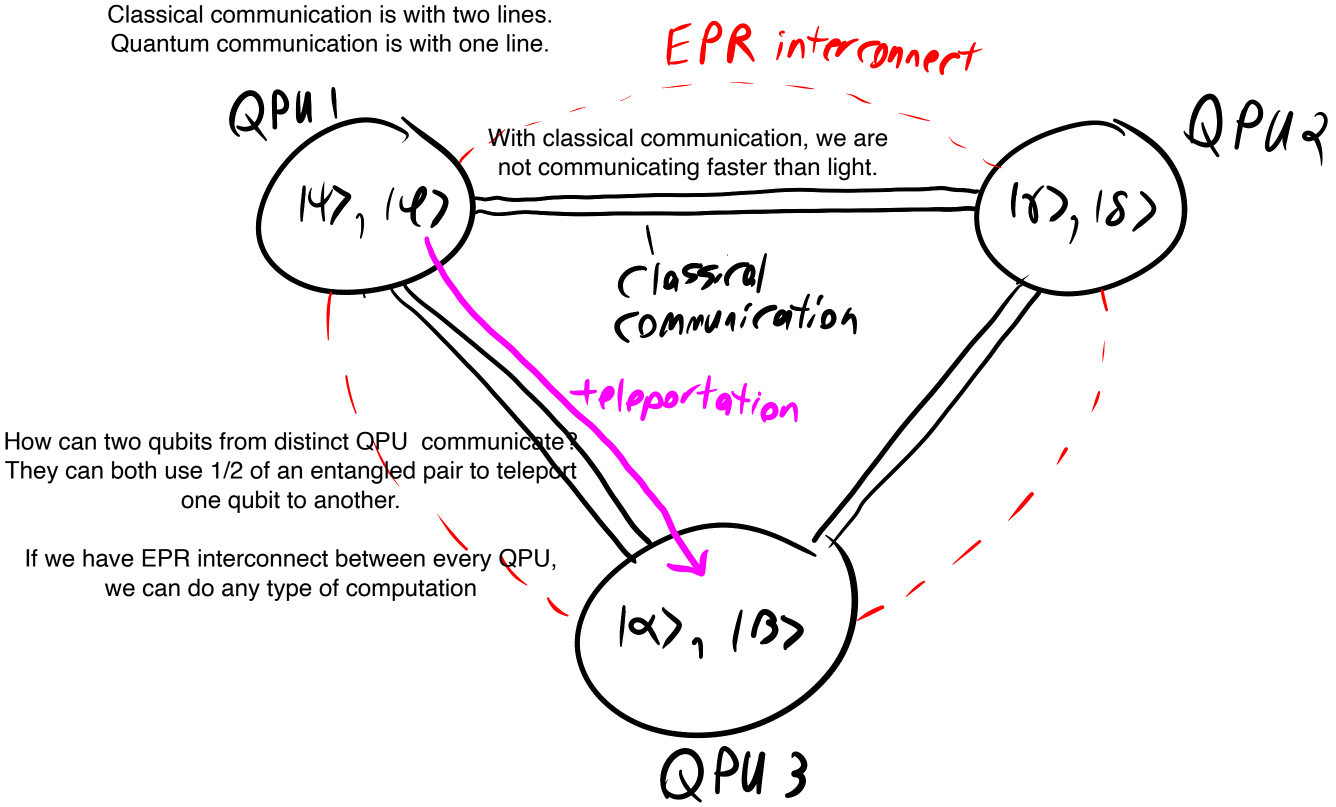


So what does this mean?

One thing that should be clear is that teleportation doesn't work like in the movies. While it may look like abstract mathematical manipulation, it has been experimentally verified many times over great distances. The key idea is that entanglement is a resource which can be used to facilitate the transfer and manipulation of quantum information over long distances. This is particulary important in recent proposals to scale quantum computation via distributed quantum computing and the quantum internet.

(Distributed quantum computing)

We need many qubits to perform quantum algorithms. Many more than would fit on a single chip in fact. To deal with this and other issues, recent proposals for scaling QC are based around establishing interconnects between processors — either at local scales or truly distributed "internet" scales — which allow the teleportation of qubits from one processor to another.



Question:

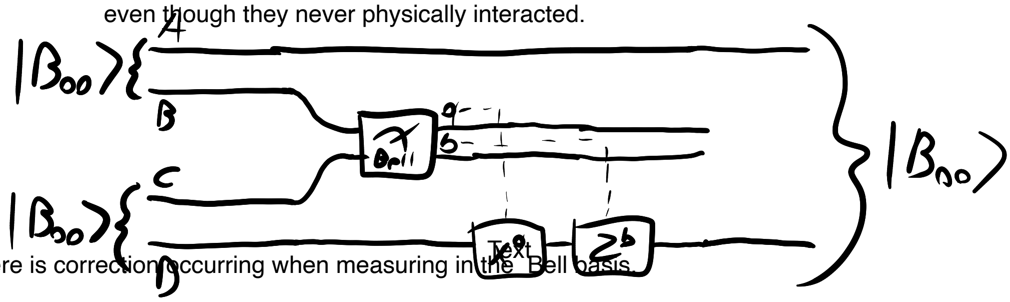
Do we need interconnects between each processor to move qubits freely between any pair?

No, due to entanglement swapping

(Entanglement swapping)

Suppose we have 4 qubits, A, B, C, D with A & B entangled and C & D entangled. Teleporting $B \longrightarrow D$ entangles A & D without A & D ever interacting directly

We can send B and C and measure both in the bell basis.
Qubit B was initially entangled with qubit A.
After doing this protocol, Qubits A and D are now entangled
even though they never physically interacted.



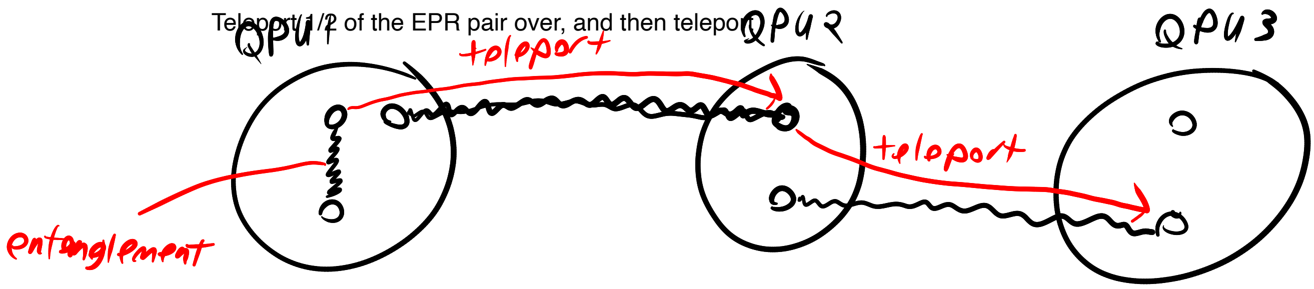
We know that there is correction occurring when measuring in the Bell basis.

Since you can write the Bell basis in different ways, the position of the X and Z gates may change.

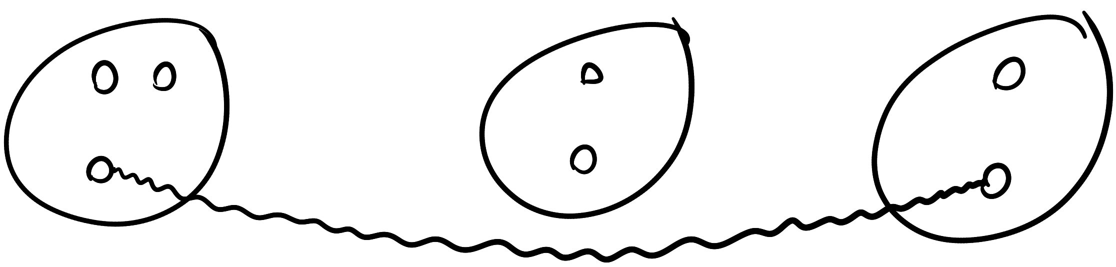
We can use this protocol to generate entangled pairs between any pair of path-connected processors, e.g.

We can now do distributed computing using a set of interconnects.

Teleport 1/2 of the EPR pair over, and then teleport

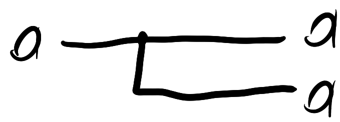


Ask professor about path connected.



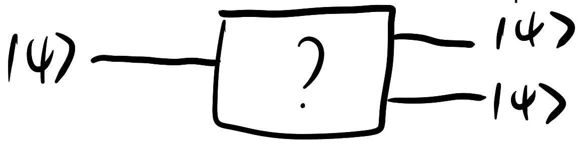
(State cloning)

One thing that we may notice about the teleportation protocol is that it is in a sense highly destructive: Alice loses her initial state $|\psi\rangle$ (and both Alice and Bob burn up an EPR pair...). A reasonable and practically important question is can we clone the state $|\psi\rangle$ first so that Alice retains a copy? Classically this is the FANOUT gate



The question is: Does there exist a quantum analogue of the FANOUT gate

Since unitary gates are reversible, we need to take a psi and a ancilla and see if we can create two copies of psi.



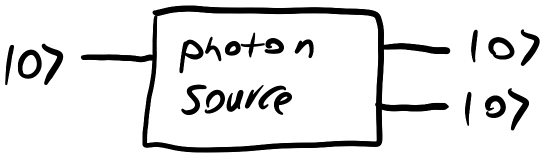
(No-cloning theorem (Wooters & Zurek, 1982))

(Informally)

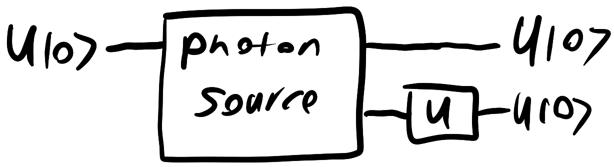
It is physically impossible to clone an <u>arbitrary</u> quantum state

no single purpose gate which can create a copy of any arbitrary state.

The arbitrary requirement is important here, since we can easily clone particular states.



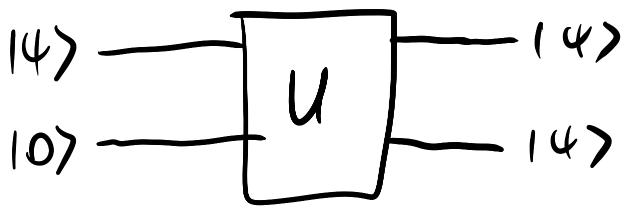
or



(Ancillas)

Note that the photon source operation above is non-unitary since it increases the number of qubits. Yet, it is physically implementable. We typically assume access to something like a photon source which will allow us to add a new qubit in the $|0\rangle$ state to a computation, called an ancilla. Another way we can view this is to say that the qubit previously existed, but since it was not yet used and its state was not entangled with the rest of the qubits, we simply ignored it.

With ancillas, we can start to hone in on what a general cloner might look like mathematically. In particular, is there a unitary transformation U s.t.



(An almost cloner)

Recall the CNOT gate $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ which sends

$$|0\rangle|0\rangle \longmapsto |0\rangle|0\rangle$$
$$|1\rangle|0\rangle \longmapsto |1\rangle|1\rangle$$

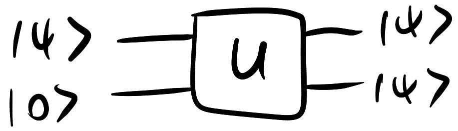
So it looks a lot like a cloner. Let's see what happens when the first qubit is in the state

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

By linearity,

$$CNOT|\psi\rangle|0\rangle = CNOT(\alpha|00\rangle + \beta|10\rangle) = \alpha|00\rangle + \beta|11\rangle$$
$$\neq |\psi\rangle|\psi\rangle$$

The fact that there is no cloner

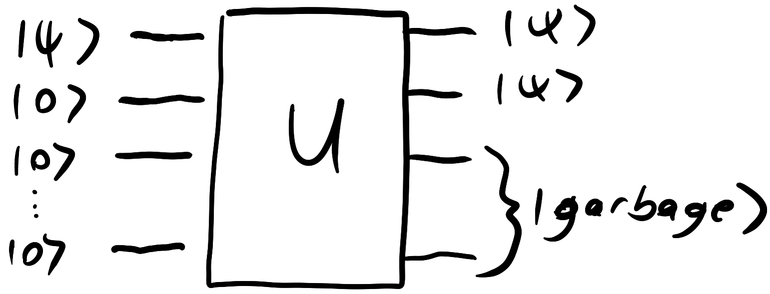


is trivial, because if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then

Issues:
Probability does not sum to 1

$$|\psi\rangle|0\rangle \longmapsto |\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

is **not even linear**! However, it could be linear in some **larger state space**, for instance a computation which uses some additional ancillas and leaves them in some **(unentangled) garbage state**, i.e.



This is what is sometimes called a **general quantum operation.**

(No-cloning theorem)
There is no general quantum operation U as above.

Proof

Let $|\psi\rangle$ and $|\varphi\rangle$ be states such that

$$0 < |\langle\psi|\varphi\rangle| < 1$$

How are we obtaining these values? If we conjoin the phi and (whatever the other symbol is), we end up with the dot product of the larger state, which is is bigger than 1.

Hence, $0 < |\underbrace{\langle\psi|\langle 00\cdots 0|\cdot|\varphi\rangle|00\cdots 0\rangle}| < 1$

$$= \langle\psi|\varphi\rangle\langle 00\cdots 0|00\cdots 0\rangle$$
$$= \langle\psi|\varphi\rangle$$

Now, since U preserves inner products we have

$$\langle\psi|\langle 00\cdots 0|\cdot|\varphi\rangle|00\cdots 0\rangle = \langle\psi|\langle\psi|\langle garbage|\cdot|\varphi\rangle|\varphi\rangle|garbage'\rangle$$
$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2\langle garbage|garbage'\rangle$$
$$1 = \langle\psi|\varphi\rangle\langle garbage|garbage'\rangle$$

But $|\langle\psi|\varphi\rangle| < 1$ and $|\langle garbage|garbage'\rangle| \leq 1$, a contradiction

$\square$