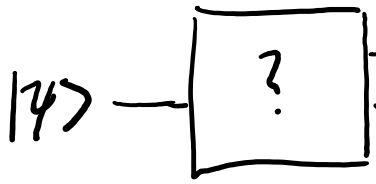
Lecture 8: No-Cloning, and Teleportation

(We've seen the CHSH game, which is a physically achievable demonstration of quantum advantage over classical info processing. Now in the course, we'll properly get into exactly this: cool stuff you can do with multiple qubits, like quantum money, key exchange, computing,...)

(We actually start, tho, with a negative result, a "no-go theorem", "No-Cloning", that will be a foil for our future positive results.)

No-Cloning Theorem (Wootters, Zurek; Nature, 1982)

There is no physical device that does this:



(2 unentangled copies of $|\psi\rangle$)

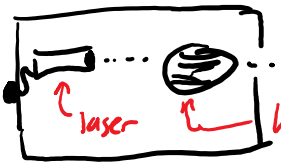
for all qubit states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

(Comments: · Proof is very easy
· Arguably not inherent to quantum. ∃ a "No-Cloning" theorem for coin flips.
· Extremely important to understand exact statement, b/c closely related things are possible.)

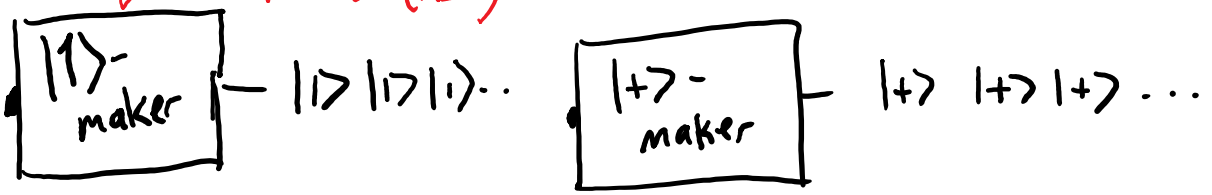
(A key point is that the machine must work for every "unknown" state $|\psi\rangle$. For example, building the following is no problem.)

(Every time you press button, a $|0\rangle$ comes out. Pressable many times.)

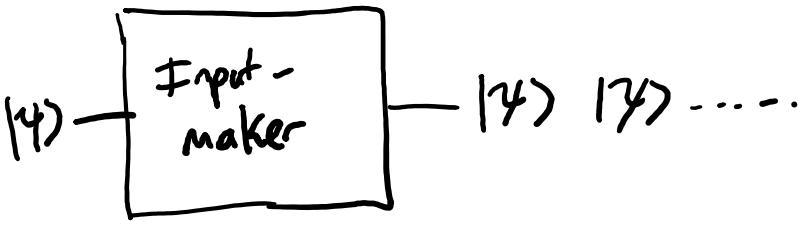
E.g.:



(Take a $|0\rangle$-maker, stick a NOT gate at end.)



Impossible:

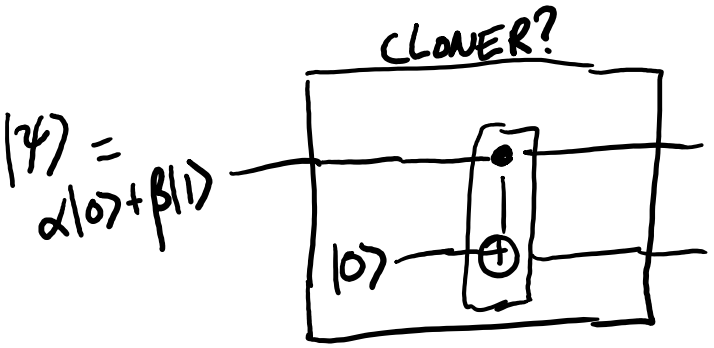


⇒ Unlearnability of an unknown state $|\psi\rangle$... (from one copy)

(If you could learn $|\psi\rangle$ exactly, in the sense of figuring out α, β, then you could do that, then attach the appropriate $|\psi\rangle$-building machine.)

What about CNOT?

(the most "copy"-like instruction in Q.C.)



Input:	Output:
$\|0\rangle$	$\|00\rangle$
$\|1\rangle$	$\|11\rangle$

(Are we done? "By linearity"?)

$\|+\rangle$	$\|++\rangle$?

$$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle \longmapsto \text{"}|0\rangle \text{ attached"} \longmapsto \frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$$

(Oops, that's the entangled EPR pair, not $|+\rangle\otimes|+\rangle$.)

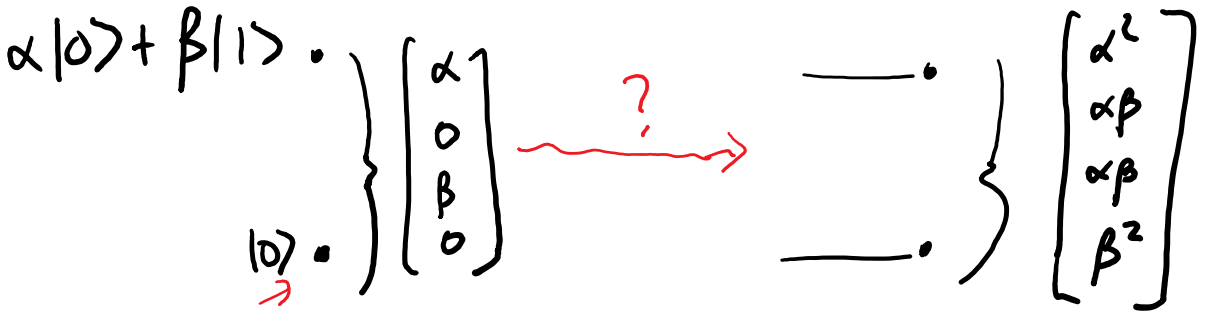
Generally: $\alpha|0\rangle+\beta|1\rangle \longmapsto \alpha|00\rangle+\beta|11\rangle = \begin{bmatrix}\alpha\\0\\0\\\beta\end{bmatrix}$

$\neq$

whereas $|\psi\rangle\otimes|\psi\rangle = (\alpha|0\rangle+\beta|1\rangle)\otimes(\alpha|0\rangle+\beta|1\rangle) = \begin{bmatrix}\alpha^2\\\alpha\beta\\\alpha\beta\\\beta^2\end{bmatrix}$

Proof of Theorem

Intuitively (but incompletely):



(Need to get a 2nd particle into picture, WLOG: $|0\rangle$)

$$\begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix} \longmapsto \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{bmatrix}$$

is not a linear map. (let alone unitary)


(?)

(Thoughts on why this is incomplete?)

- Not linear as a map $\mathbb{C}^4 \to \mathbb{C}^4$ but perhaps when domain restricted to $\begin{bmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{bmatrix}$ s.t. $|\alpha|^2+|\beta|^2=1$?

Eg., $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \longmapsto \begin{bmatrix} \alpha^3+\alpha\beta^2 \\ \alpha^2\beta+\beta^3 \end{bmatrix}$ looks like a cubic map...

but when restricted to qubit states...

it's $\begin{bmatrix} \alpha(\alpha^2+\beta^2) \\ \beta(\alpha^2+\beta^2) \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$. Identity map!

(So, we'll see the intuition is right, and the cloning map really isn't linear. Still, must be careful.)

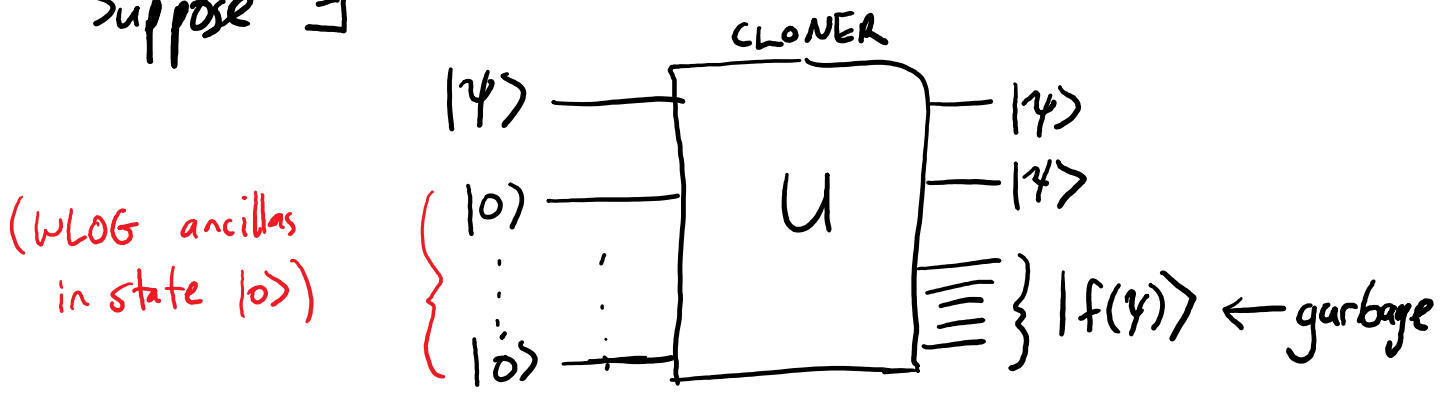
- Perhaps the cloner uses extra "ancilla" qubits (WLOG, initialized to $|0\rangle$) and outputs some "garbage" in addition to $|\psi\rangle \otimes |\psi\rangle$ (unentangled)

- Perhaps cloner uses internal measurements.

(We'll skip ruling this out, but one can. Not too hard. Maybe on future homework, once we see the Principle of Deferred Measurement.)

Real Proof (omitting possibility of internal measurements)

Suppose $\exists$



so $U(|\psi\rangle \otimes |00\cdots0\rangle) = |\psi\rangle \otimes |\psi\rangle \otimes |f(\psi)\rangle$

($n-1$ zeros; $|f(\psi)\rangle$ is 2^{n-2}-dimensional)

$\forall$ qubit states $|\psi\rangle$.

$\therefore$ $U(|0\rangle \otimes |00\cdots0\rangle) = |00\rangle \otimes |f(0)\rangle$ ⓐ

$U(|1\rangle \otimes |00\cdots0\rangle) = |11\rangle \otimes |f(1)\rangle$ ⓑ

$U(|+\rangle \otimes |00\cdots0\rangle) = |++\rangle \otimes |f(+)\rangle$ ⓒ

$\frac{1}{\sqrt{2}}$ⓐ + $\frac{1}{\sqrt{2}}$ⓑ $\Rightarrow$ $U(|+\rangle \otimes |00\cdots0\rangle) =$

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

ⓒ

$(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle) \otimes |f(+)\rangle$.

So we've deduced:

$$\frac{1}{\sqrt{2}}|00\rangle \otimes |f(0)\rangle + \frac{1}{\sqrt{2}}|11\rangle \otimes |f(1)\rangle \quad (*)$$

$$=$$

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

But this is false! Why? Consider measuring first two qubits:

(*) See 00 or 11, $\frac{1}{2}$ prob each

($\neq$) See 00, 01, 10, 11, $\frac{1}{4}$ prob each.

∎

Remark: Proof shows $\nexists$ cloner that even works simultaneously for

$$\{|0\rangle, |1\rangle, |+\rangle\}.$$

Classical comparison: cloning biased coins?

(Imagine you want a machine that takes such a coin as input, outputs 2 coins, with same bias.)

(Think about how you'd do it....

① "Study" the coin. Weigh it, measure it, etc.
That's a difference w/ quantum states: can't just "look" at them. Can only formally "measure" them — which is very much like "flipping" a coin.

② So flip it? Well, you'd probably want to flip it 1000 times, estimate bias — say 81% — then start building 81%-biased coins.
Again, a difference with quantum states: they can essentially only measured <u>once</u>.)

Quantum state ~~similar to~~ one-time-flippable coin

(And pretty clear can't learn much from ↑. In fact, can prove a "No-Cloning" Theorem for such coins. Proof is same.)

(By the way, you can learn a coin's bias to some precision, if you can flip it many times.)

unknown p-bias coin (1-time flippable)

↳ many copies ⟿ "learning alg" ⟿ can est. p to ε accuracy

Similarly: unknown qubit $|\psi\rangle$

↓

given many copies $|\psi\rangle \otimes |\psi\rangle \otimes \cdots \otimes |\psi\rangle$ ⟿ "learning" ⟿ can est. $|\psi\rangle$'s amplitudes

"quantum tomography"

(They called "learning", "tomography", for some reason)

(This is a major part of my (O'Donnell's) research.)

(We'll talk about this exact problem some dozen lectures from now....)

Quantum Teleportation

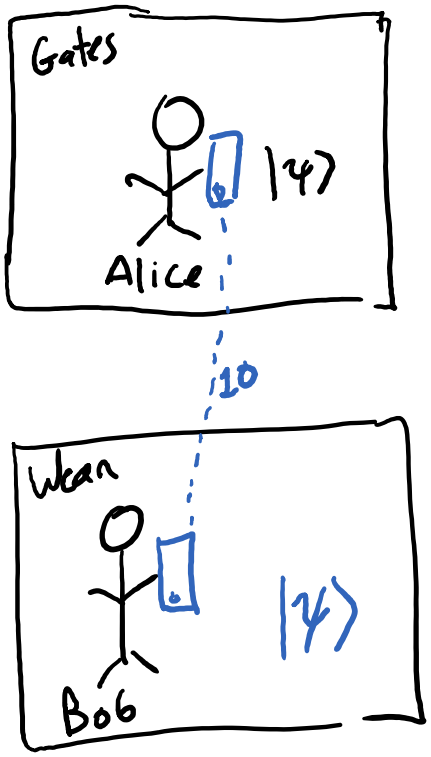
(A "magic trick" discovered in 1993 by some Q.C. pioneers (Bennett, Brassard...) and others. BTW: cool that this is some "recent" stuff; you were probably also born in '90s.)

(Looks a bit like Cloning - but of course, isn't.)

(The name is pretty fancy-sounding, but one thing to emphasize is that no physical matter will be moved a great distance - what will move is information, a quantum state.)

(Also, will involve classical transmission of info., so best to imagine teleportation is only over a modest distance; say from the Gates building to the Wean building on campus....)

Quantum Teleportation (another Alice/Bob magic trick)



(Alice is messing about in her office and runs across...)

$|\psi\rangle$: a qubit in an unknown state

(She knows her friend Bob, over in Wean, loves mystery particles. She'd like to give $|\psi\rangle$ to Bob.

Option 1: Walk the particle over there.

Naaah. Alice too lazy for that.

Option 2: Alice does... something quantum-y.. (TBD). Then she texts Bob a message consisting of 2 classical bits.

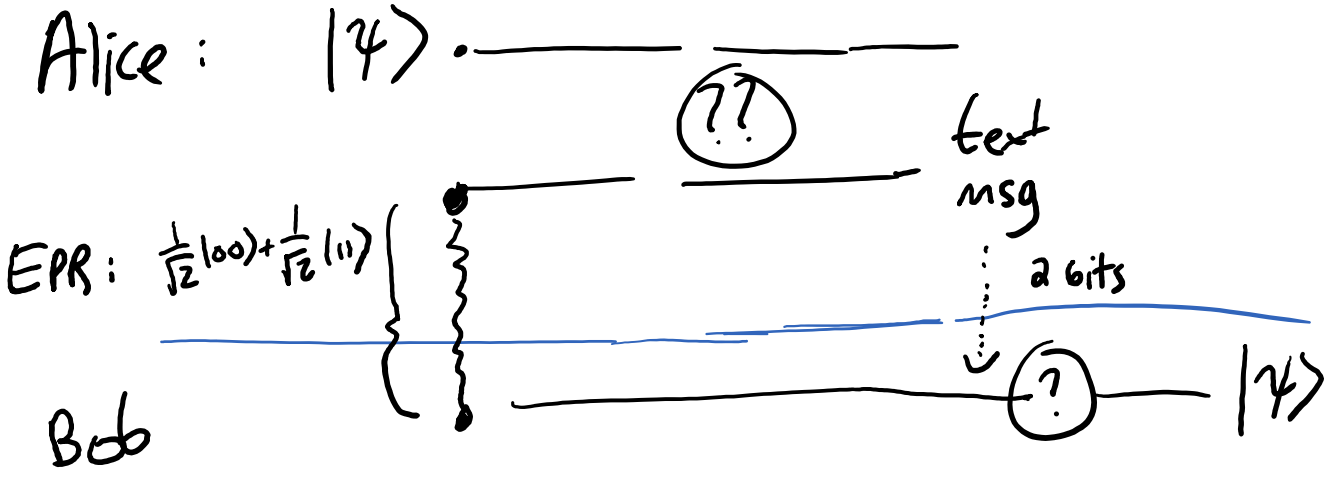
Now – boom: Bob holds qubit in state $|\psi\rangle$! Of course, Alice better <u>not</u> have $|\psi\rangle$, else No-Cloning violated.)

Quantum Teleportation — How?

(Of course, those magicians...)

Alice & Bob assumed to have pre-shared an EPR pair.

(They're friends — of course they'll make sure they always have halves of such pairs stored in their respective office fridges!)



"1 ebit + 2 bits ≥ 1 qubit"

↑ entangled

(Compare Hmwk 3, #3: "1 ebit + 1 qubit ≥ 2 bits" "superdense coding")

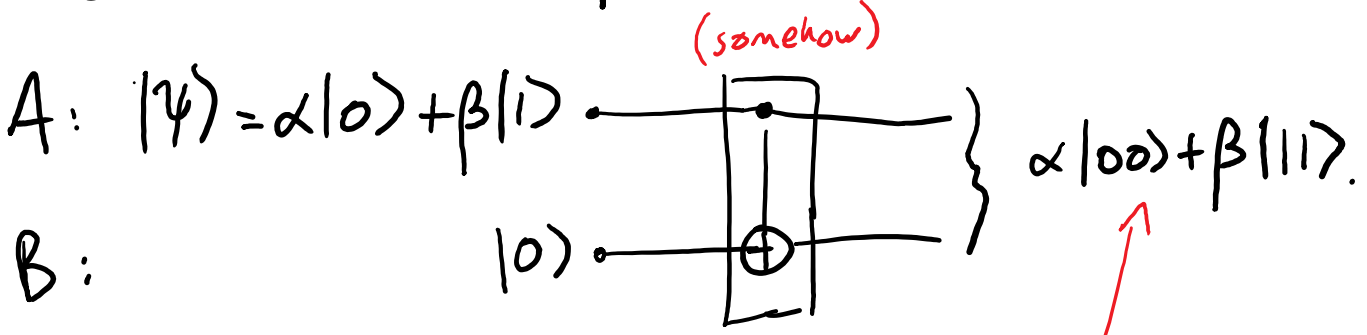
NB: 2 classical bits is far less info than is in |ψ⟩'s 2 complex amplitudes.

(So even if Alice knew |ψ⟩ exactly, conveying it by text to Bob would need... well, infinitely many classical bits.)

(One can just write down the solution, but it looks a little unmotivated that way. I will give U. Vazirani's explanation, which I like a lot.)

We'll (somehow) show A & B can effect a CNOT gate betw. their offices. (Later.)

Why does that help?



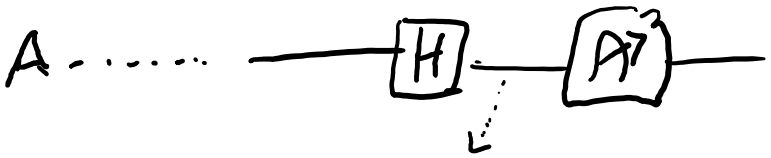
(OK. Trying to end up with just $|\psi\rangle$ in Bob's hands. Must get rid of Alice's particle, So... measure?)

A measures? Bob will end with $|0\rangle$ or $|1\rangle$. ☹

(What the heck else can Alice do?... Measure in $|\pm\rangle$ basis.)

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

(Now Alice measures....)



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

(Now Alice measures....)

$Pr[0] = \left|\frac{\alpha}{\sqrt{2}}\right|^2 + \left|\frac{\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}$, Bob's state collapses to...

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

$Pr[1] = \left|\frac{\alpha}{\sqrt{2}}\right|^2 + \left|\frac{-\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}$, Bob's state collapses to...

$\alpha|0\rangle - \beta|1\rangle$:/

(Hmm. Now what?)

Alice texts Bob her outcome.

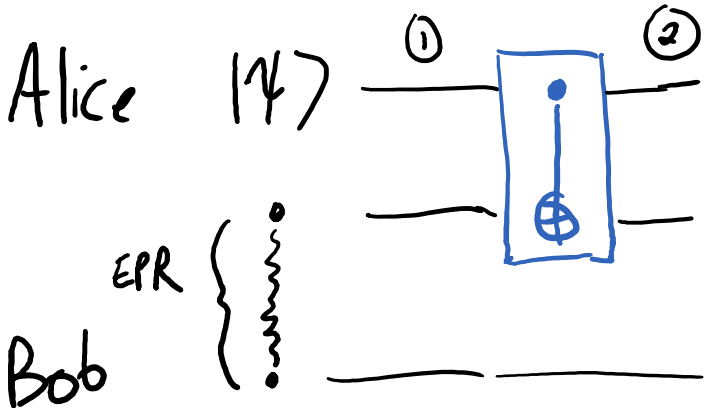
If "0": Bob does nothing.

If "1": Bob applies "Z" $= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

($|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto -|1\rangle$.)

☺ Now Bob has $|\psi\rangle$.

(Great! Well, how do they do this distributed CNOT? Used up 1 classical bit of communication. Still have one left - and more importantly, still haven't used EPR pair!)



(I mean, Alice holds $|\psi\rangle$ & half an EPR pair. What else to try, but CNOT-ing them?)

Time ①: $(\alpha|0\rangle+\beta|1\rangle)\otimes\left(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle\right)$

CNOT first two ↓ $= \frac{\alpha}{\sqrt{2}}|000\rangle+\frac{\alpha}{\sqrt{2}}|011\rangle+\frac{\beta}{\sqrt{2}}|100\rangle+\frac{\beta}{\sqrt{2}}|111\rangle$

Time ②: $\frac{\alpha}{\sqrt{2}}|000\rangle+\frac{\alpha}{\sqrt{2}}|011\rangle+\frac{\beta}{\sqrt{2}}|110\rangle+\frac{\beta}{\sqrt{2}}|101\rangle$

(Again, Alice trying to divest qubits, so she should measure something. Probably the target qubit, the and one.)

$$\frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle$$

Alice measures 2nd qubit:

$\Pr[0] = \left|\frac{\alpha}{\sqrt{2}}\right|^2 + \left|\frac{\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}$, collapse to... $\alpha|00\rangle + \beta|11\rangle$ ☺

(Desired magic CNOT outcome!)

$\Pr[1] = \left|\frac{\alpha}{\sqrt{2}}\right|^2 + \left|\frac{\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}$, collapse to... $\alpha|01\rangle + \beta|10\rangle$ ☺

("almost" the desired state. Bob just needs to NOT.)

Alice texts Bob her outcome.

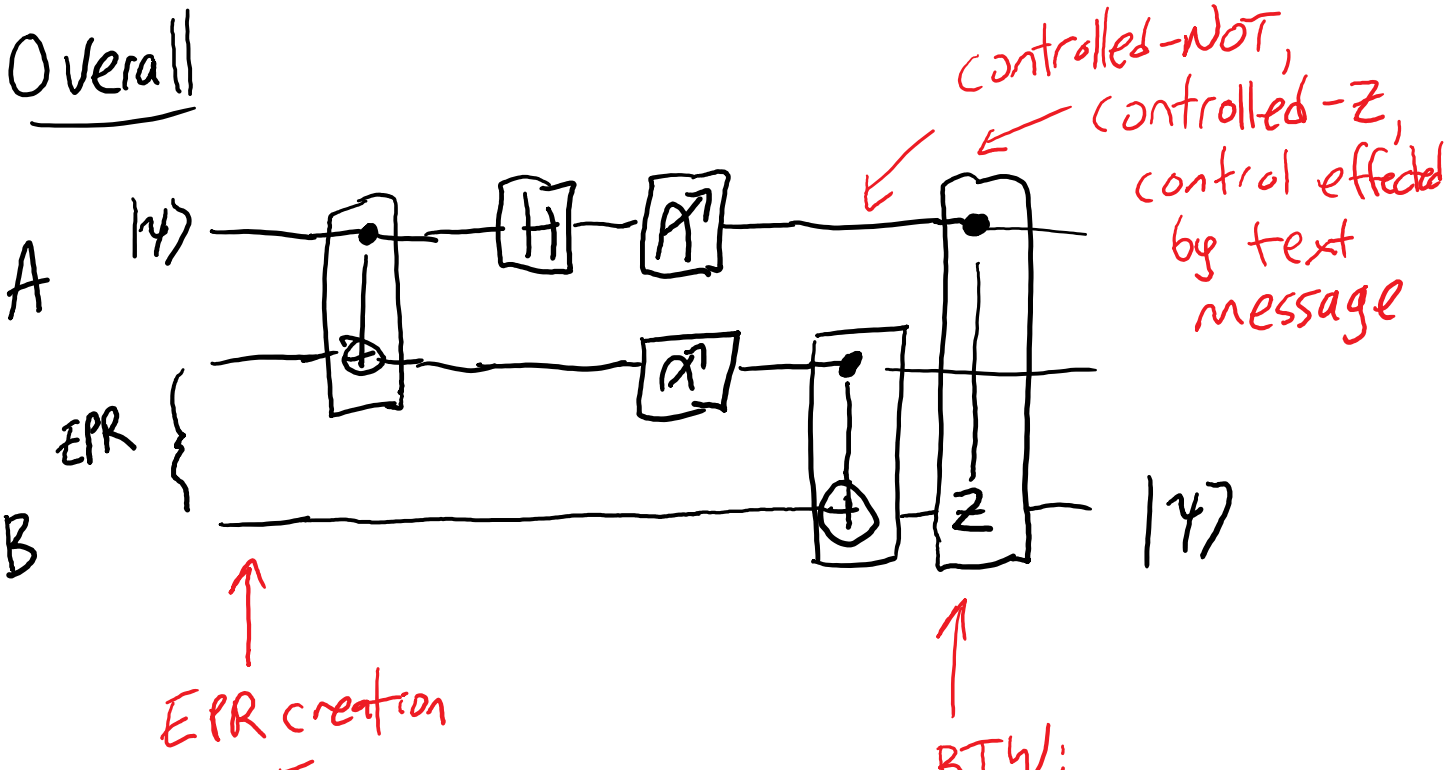
If "0", Bob does nothing.

If "1", Bob NOTs his qubit.

→ now A & B share $\alpha|00\rangle + \beta|11\rangle$; i.e., have accomplished the "distributed-CNOT"!

Can now finish as before.

Overall



(So whole picture is H, NOT, CNOT, measurement)

(Remarks: This quantum teleportation experiment has been done many times; most impressively, between Tibet & a space satellite, Jian-Wei Pan, '17.)

Also: used in several attempts to design Q.C.'s. Very useful to be able to do these "physically distributed 2-qubit gates"!)

Entanglement Swapping

(I kind of misled you in a response to a student question in Lecture 5. Was asked if it's possible for two particles to get entangled if they're never physically collocated. In fact, they can be...)

(Charlie, in Doherty building, also friends with Alice, they share EPR pair. Bob & Charlie not friends, never meet,)

Alice can prep 2 more entangled particles in her office.

(Ellie the electron → •~~• ← Phil the Photon)

Perhaps Bell state.

Teleport one to Bob, one to Charlie.

Now (check!) Bob & Charlie hold an entangled pair!

(This also used in practice to generate distant entanglement

Also, shows that EPR pairs suffice for generating all entanglement. If n remote parties want to get an entangled n-qubit state, enough for each party to share half an EPR pair with Alice. She can prep the n-qubit entangled state herself, and teleport each particle to the appropriate party.)