# Ph/CS 219A
# Quantum Computation

## Lecture 8. Superdense Coding and Quantum Teleportation

Today we continue the discussion of quantum entanglement, with emphasis on how entanglement can be used as a resource for achieving particular tasks.

We have already discussed important examples. With quantum entanglement we can win a game, like the CHSH game, with higher success probability than would be possible without entanglement. That is what Bell inequality violation is all about.

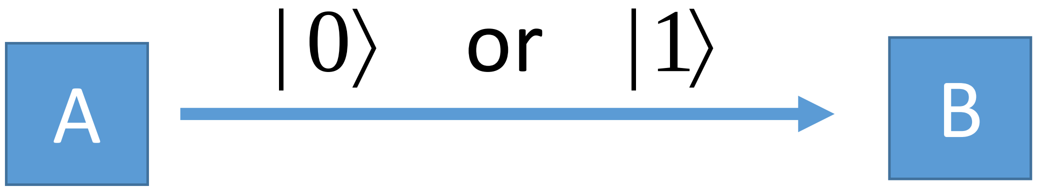
Now we'll discuss two other examples: superdense coding and quantum teleportation. Teleportation in particular is an important subroutine in a variety of useful quantum protocols. It is also pretty cool.

*See Chapter 4 of the Lecture Notes. Note that Problem Set 2 has been posted, due October 30.*

# Superdense Coding

Suppose Alice and Bob are connected by a noiseless quantum channel. Specifically, Alice can prepare a qubit in any quantum state she pleases, and send it to Bob through the channel. Bob receives exactly the state that Alice sent; he may then proceed to measure it or store it in a quantum memory.

They can use this *quantum* channel to send *classical* information from Alice to Bob. For example: Alice prepares one of two mutually orthogonal states, $|0\rangle$ or $|1\rangle$, and Bob measures in the basis $\{|0\rangle, |1\rangle\}$ upon receipt.




If Alice sends *n* qubits, can she convey more than *n* classical bits to Bob? *Holevo's Theorem* says this is impossible (the proof is in Chapter 10 of our Lecture Notes). This is not obvious. Alice might choose from an alphabet of more than two nonorthogonal states of the qubit, or she could send states that are entangled across many uses of the channel. But it turns out that such strategies do not improve the communication rate.


But what if Alice and Bob share quantum entanglement that has been previously distributed to them? Can they use the entanglement to send more bits per use of the channel?

# Superdense Coding

$$I \otimes I|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle$$

$$X \otimes I|\phi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\psi^+\rangle$$

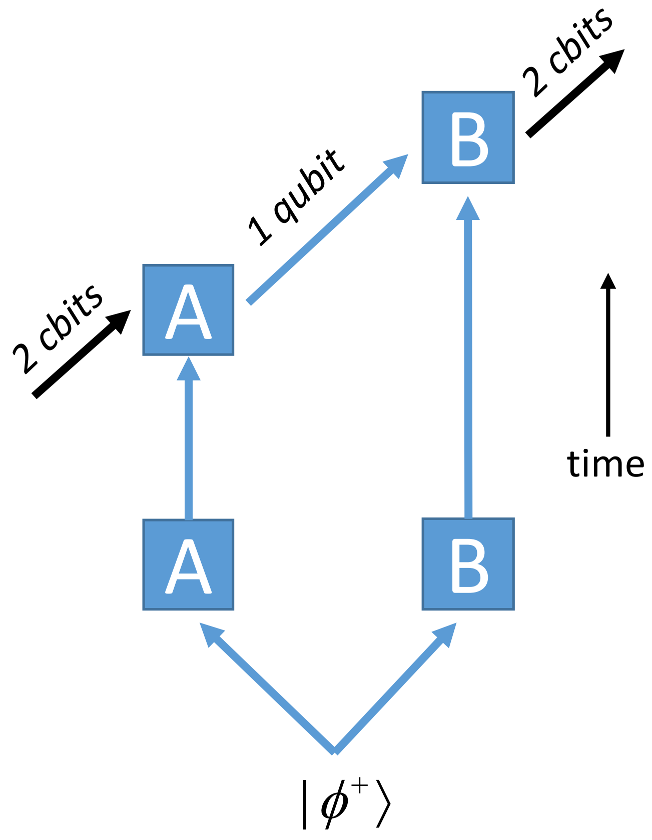
$$Y \otimes I|\phi^+\rangle = \frac{i}{\sqrt{2}}(|10\rangle - |01\rangle) \propto |\psi^-\rangle$$

$$Z \otimes I|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi^-\rangle$$

By applying a suitable unitary, Alice can transform the shared entangled state to one of four mutually orthogonal maximally entangled states, which can be perfectly distinguished by Bell measurement. Bob measures in the basis:

$$\{|\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^-\rangle\},$$

distinguishes $\{I, X, Y, Z\}$.




*Resource inequality*: Alice sent one qubit, communicated two cbits. This would not have been possible without the shared entanglement.

$$[q \to q] + [qq] \geq 2[c \to c] \quad \text{(SD)}$$

*qubit* *ebit* *2 cbits*

This communication is *encrypted.* What if Eve (an eavesdropper) intercepts the qubit as it travels from Alice to Bob? This qubit is maximally mixed; it reveals nothing to Eve about Alice's message.

# Superdense Coding

$$I \otimes I\,|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle$$

$$X \otimes I\,|\phi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\psi^+\rangle$$

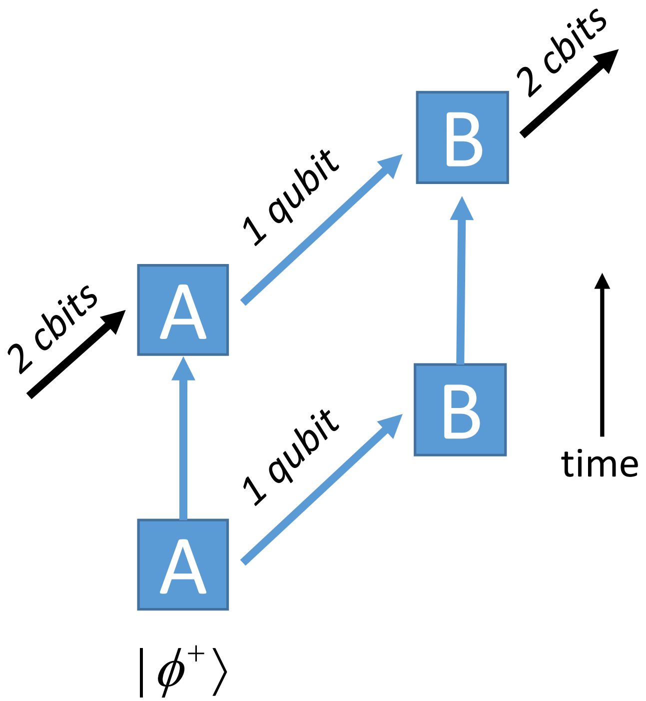
$$Y \otimes I\,|\phi^+\rangle = \frac{i}{\sqrt{2}}(|10\rangle - |01\rangle) \propto |\psi^-\rangle$$

$$Z \otimes I\,|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi^-\rangle$$

By applying a suitable unitary, Alice can transform the shared entangled state to one of four mutually orthogonal maximally entangled states, which can be perfectly distinguished by Bell measurement. Bob measures in the basis:

$\{|\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^-\rangle\}$,

distinguishes $\{I, X, Y, Z\}$.




Alice might have prepared the entangled state herself, and sent half to Bob yesterday, then sends the other half to Bob today. So in a sense:

$$2[q \to q] \geq 2[c \to c] \quad \Rightarrow \quad [q \to q] + [qq] \geq 2[c \to c] \quad \text{(SD)}$$

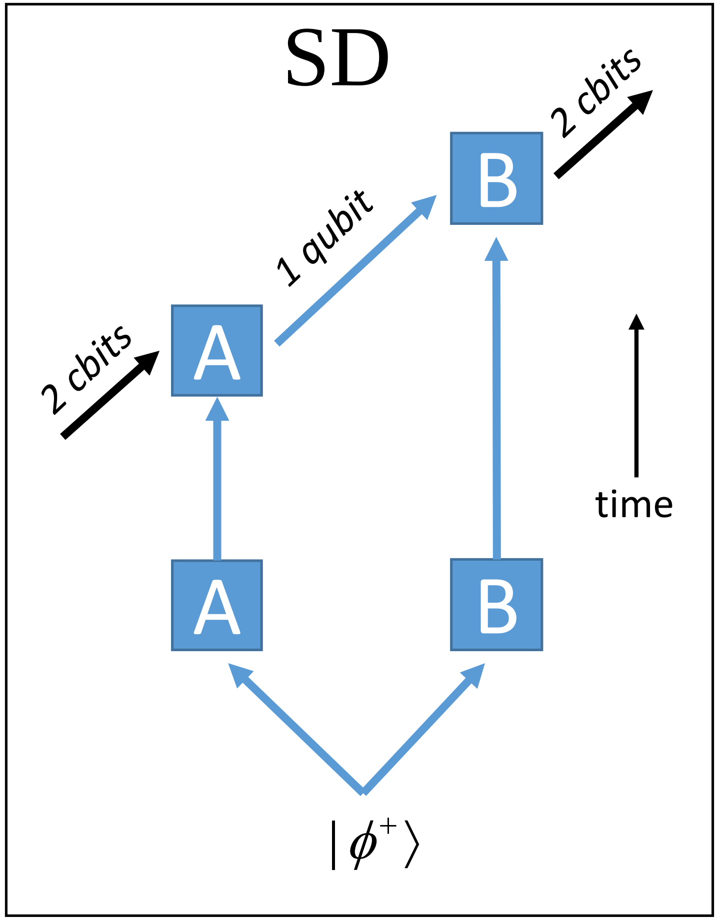
*qubit* *ebit* *2 cbits*

But:

(1) Alice sent the first qubit before she decided today what message to send to Bob.

(2) The first qubit could have been sent from Bob to Alice, or prepared by Charlie and distributed to Alice and Bob.

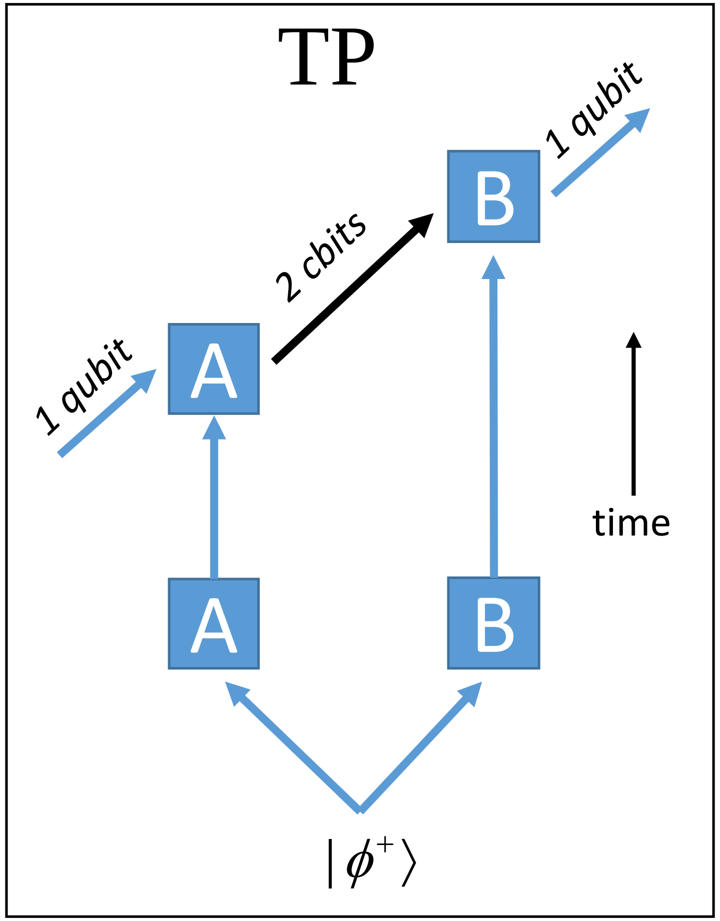
(3) Neither qubit by itself carries any information about the message.




# Quantum Teleportation

Quantum teleportation is in a sense the *dual* of superdense coding. Now Alice performs Bell measurement, sends two cbits to communicate her measurement outcome to Bob, and Bob applies one of $\{I, X, Y, Z\}$.

This way, a qubit is conveyed from Alice's lab to Bob's, though neither Alice nor Bob knows the qubit's state. This would not have been possible without the shared entanglement.




$$2[c \to c] + [qq] \geq [q \to q] \quad \text{(TP)}$$

2 cbits ebit qubit

Alice was able to send her (unknown) qubit to Bob with perfect fidelity, even though no quantum channel was available at the time. If Alice had measured the qubit and sent her measurement outcome to Bob, that would not have worked; the measurement disturbs the state.

# Quantum Teleportation

A computation shows that it works:

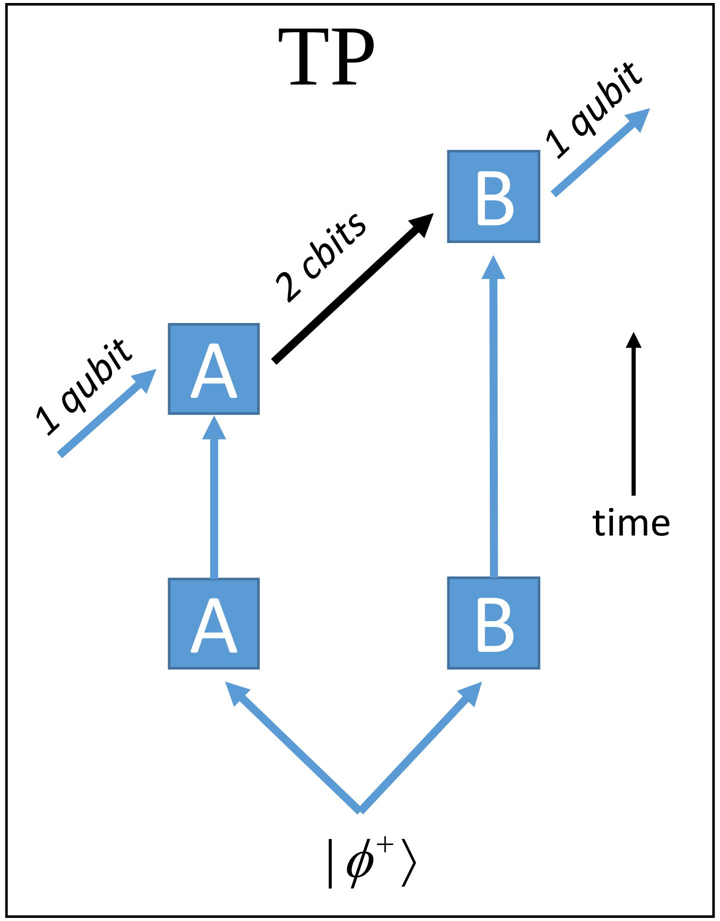
$$|\psi\rangle_C \otimes |\phi^+\rangle_{AB} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$$

$$= \frac{1}{2}\Big(a(|\phi^+\rangle + |\phi^-\rangle)|0\rangle + a(|\psi^+\rangle + |\psi^-\rangle)|1\rangle + b(|\psi^+\rangle - |\psi^-\rangle)|0\rangle + b(|\phi^+\rangle - |\phi^-\rangle)|1\rangle\Big)$$

$$= \frac{1}{2}\Big(|\phi^+\rangle(a|0\rangle + b|1\rangle) + |\psi^+\rangle(a|1\rangle + b|0\rangle) + |\psi^-\rangle(a|1\rangle - b|0\rangle) + |\phi^-\rangle(a|0\rangle - b|1\rangle)\Big)$$

$$= \frac{1}{2}\Big(|\phi^+\rangle_{CA} \otimes |\psi\rangle_B + |\psi^+\rangle_{CA} \otimes X|\psi\rangle_B + |\psi^-\rangle_{CA} \otimes (-iY)|\psi\rangle_B + |\phi^-\rangle_{CA} \otimes Z|\psi\rangle_B\Big)$$

Alice measures in basis $\{|\phi^+\rangle, |\psi^+\rangle, |\psi-\rangle, |\phi^-\rangle\}$, Bob applies $\{I, X, Y, Z\}$.




Before receiving the message from Alice, Bob holds a maximally mixed qubit.
After receiving the message, he knows he holds $\sigma|\psi\rangle$ where $\sigma \in \{\mathrm{I, X, Y, Z}\}$.

$$2[c \to c] + [qq] \geq [q \to q] \quad \text{(TP)}$$

Alice, Bob learn nothing about $|\psi\rangle$ . (That's good --- no disturbance.)
Was the state cloned? No, Alice's copy is destroyed before Bob's can appear.
Do the cbits carry the quantum information? No, they are uniformly random.
Does the entanglement do it? Recall, $|\phi^+\rangle$ could have been prepared yesterday.

How to verify? Charlie can prepare and deliver to Alice, then measure in basis $\{|\psi\rangle, |\psi^\perp\rangle\}$ in Bob's lab later.

# Quantum Teleportation

Teleportation in *N* dimensions. $|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\otimes|i\rangle \quad \Rightarrow$

$$U\otimes I\,|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_{i,j=0}^{N-1}|j\rangle U_{ji}\otimes|i\rangle = \frac{1}{\sqrt{N}}\sum_{i,j=0}^{N-1}|j\rangle\otimes|i\rangle U_{ij}^{T} = I\otimes U^{T}\,|\Phi\rangle$$

$$\Rightarrow U\otimes V\,|\Phi\rangle = I\otimes VU^{T}\,|\Phi\rangle = UV^{T}\otimes I\,|\Phi\rangle$$

Any maximally entangled state can be obtained from any other by applying *either* a unitary on Alice's side or a unitary on Bob's side.
A general maximally entangled state can be expressed: $|\Phi(U)\rangle = U\otimes I\,|\Phi\rangle$

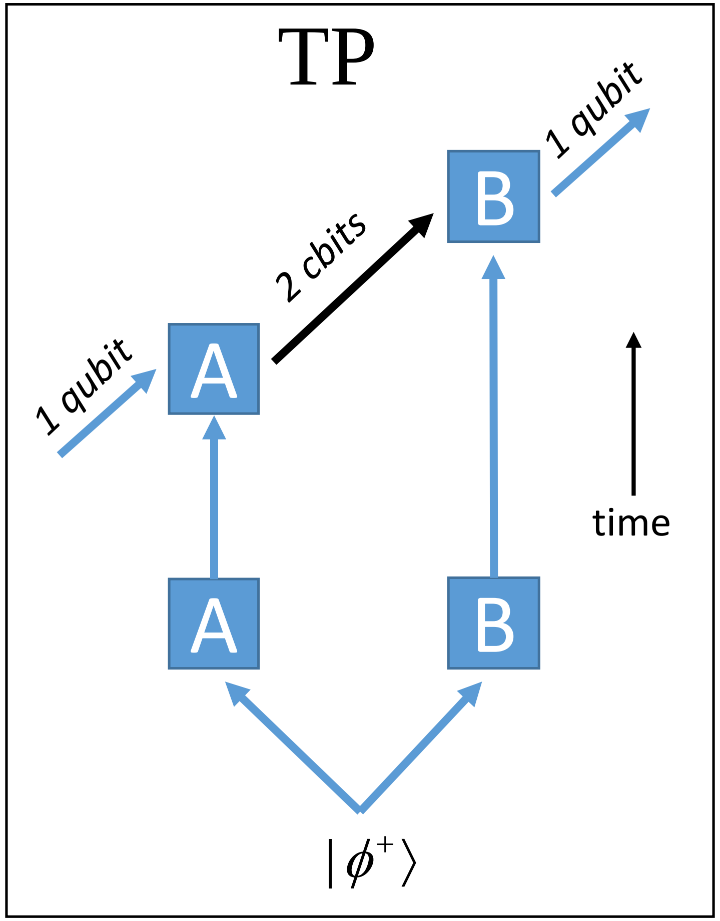
To understand teleportation:

$$_{CA}\langle\Phi|\Phi\rangle_{AB} = \frac{1}{N}\sum_{i,j}\left({}_{C}\langle i|\otimes{}_{A}\langle i|\right)\left(|j\rangle_{A}\otimes|j\rangle_{B}\right) = \frac{1}{N}\sum|i\rangle_{B}\;{}_{C}\langle i| = \frac{1}{N}T_{C\to B}$$

This is a *transfer operator* (defined relative to a *reference frame*).

$$T_{C\to B}: |\psi\rangle_{C} \to |\psi\rangle_{B}$$

Note that, if we want to verify teleportation from system C to system B, we need a *shared reference frame* for the two systems.



# Quantum Teleportation

$$ {}_{CA}\langle \Phi | \Phi \rangle_{AB} = \frac{1}{N}\sum_{i,j} \left( {}_{C}\langle i | \otimes {}_{A}\langle i | \right)\left( | j\rangle_A \otimes | j\rangle_B \right) = \frac{1}{N}\sum |i\rangle_B \ {}_{C}\langle i | = \frac{1}{N} T_{C\to B} $$

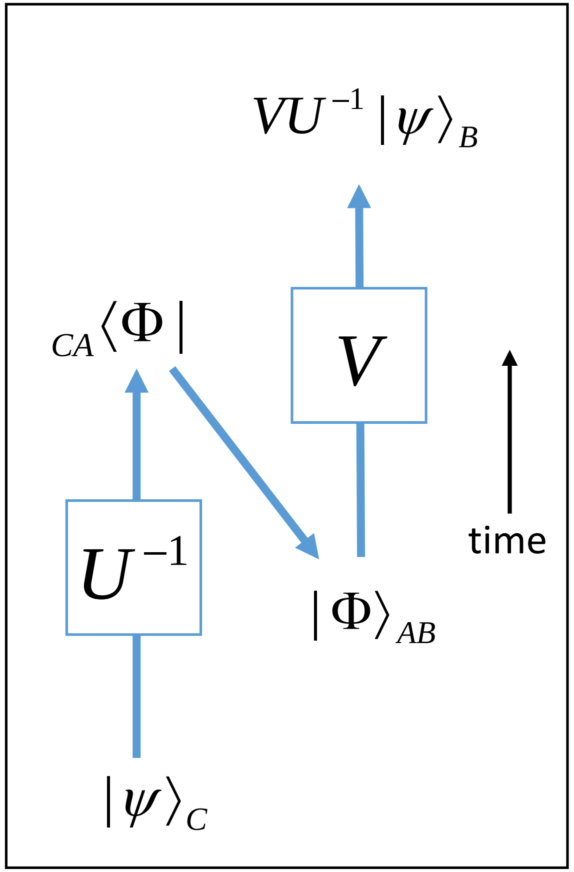
$$ |\Phi(V^T)\rangle_{AB} = V^T \otimes I |\Phi\rangle_{AB} = I \otimes V |\Phi\rangle_{AB}, \quad |\Phi(U)\rangle_{CA} = U \otimes I |\Phi\rangle_{CA} $$

$$ \Rightarrow \quad {}_{CA}\langle \Phi(U) | \Phi(V^T)\rangle_{AB} = V_B T_{C\to B} U_C^{-1} = \left( VU^{-1}\right)_B T_{C\to B}. $$

If the outcome of Bell measurement is $|\Phi(U)\rangle_{CA}$,

and the shared entangled state is $|\Phi(U^T)\rangle_{AB}$,

then the tranfer operator is the identity.




Once the CA Bell measurement outcome is determined, we know the transfer would have been perfect if we had shown to foresight to prepare the right entangled state of AB. But it is not too late, because we can "fix" the entangled state acting only on B!

Information flow through spacetime: Forward in time from Charlie's preparation of C to Alice's measurement of CA, backward in time from Alice's measurement to the preparation of the entangled state of AB, forward in time from the preparation of the entangled state to Bob's laboratory.

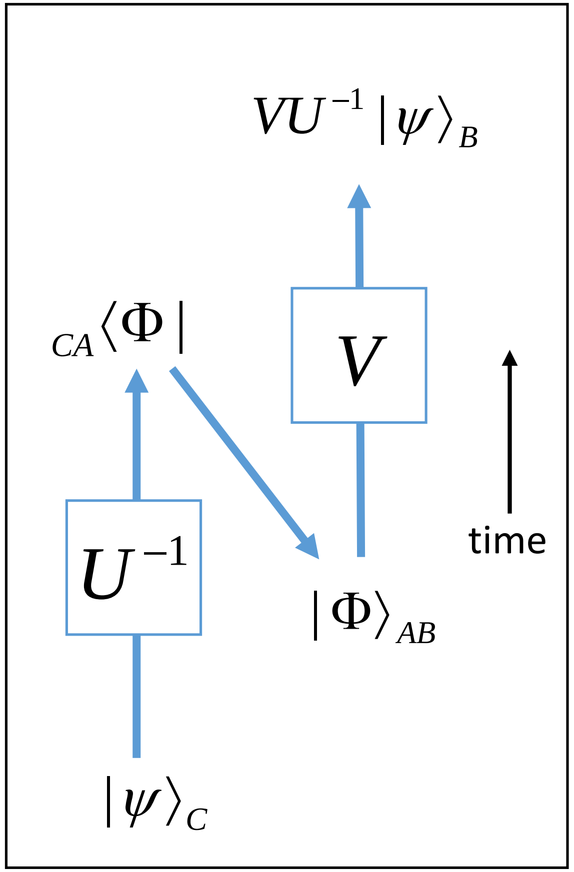
# Quantum Software

I would like to apply $V$ to $|\psi\rangle$, but I don't have suitable hardware for that task.
I do have the ability to create the entangled state $|\Phi(V^T)\rangle$, and I can perform Bell measurement, projecting onto a basis $\{|\Phi(U_a)\rangle\}$.

Via the teleportation protocol, I apply $VU_a^{-1}$ to $|\psi\rangle$,
then complete the task by applying $VU_aV^{-1}$.

This type of scheme really is useful in fault-tolerant quantum computing acting on encoded quantum data protected by a quantum error-correcting code.

How to prepare the quantum software we need, $I \otimes V|\Phi\rangle$, if we cannot apply $V$?
Notably, it is easier to prepare a known quantum state than to apply a unitary to an unknown state. We can check the preparation and if it failed we can try again.




Teleportation itself has a similar character. We might want to use quantum channels to network quantum computers together, or to send quantum information over long distances for applications to cryptography. Quantum channels are typically noisy, so it is a good strategy to first verify that Alice and Bob share robust entanglement, and then to use the entanglement to teleport. This works better than sending quantum information directly.