<div style="border:1px solid">

Quantum Information Theory - 67749
Recitation 2, May 8, 2025

</div>

1 Overview - Quantum States as Computational Resources.

In the last lectures, we saw that quantum states can be considered as resources. In particular, we saw that shared **EPR** pair (**Bell**$_{00}$) enables one:

1. Transmit two classical bits by sending a single qubit, via the superdense-coding.

2. 'Teleoperate' a qubit by sending two classical bits. From an engineering point of view, it means that for having a complete quantum internet, it's enough to provide a mechanism to distribute **EPR** pairs.

2 Superdense Encoding.

The idea behind superdense coding is that a local operation over $|\mathbf{EPR}\rangle = |\beta_{00}\rangle$, namely an operation on the partition held by Alice, sends it to any of the other Bell states. For example, $X \otimes I_{\text{Bob}} |\mathbf{EPR}\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Thus, Alice can change the complete encoded state shared between Alice and Bob by acting only over her local system. Yet, as we have seen, for Bob to infer what that state is, he has to hold both qubits, otherwise, his local view is the uniformly mixed state over a single qubit. So the protocol works as follows:

1. We assume that Alice and Bob share an $|\mathbf{EPR}\rangle$, each holding a single qubit.

2. Alice applies one of I, X, Z, XZ on her qubit to transform the shared state to one of the following $\beta_{00}, \beta_{10}, \beta_{01}, \beta_{11}$ and sends it to Bob.

3. Bob decodes the qubit pair by rotating the state into the computational basis and then measuring.

In total, we have a protocol that, by sending a single qubit through the channel, passes two classical bits. Notice that any attempt to listen to the channel[1] would reveal no information since, again, when squeezing the view into a single qubit, it seems uniformly mixed.

3   Quantum Teleportation.

Quantum teleportation is a gadget (method) to transfer a quantum state from one location to another, without the physical transfer of the underlying particles themselves. This is achieved through the consumption of **EPR** pairs.
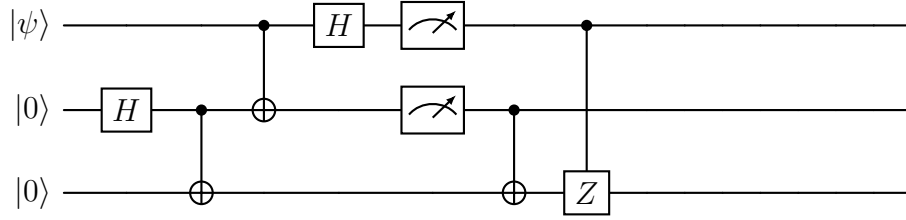

Figure 1: Measuring the single-qubit state $|\psi\rangle$ at the $\{|+\rangle,|-\rangle\}$ base.

For understanding the protocol, let's first examine a much simpler circuit. Consider the state given by the partial circuit obtained by first omitting the phase correction, and second by pulling the XORing of $|\psi\rangle$ and Alice's part into a third ancilla. The circuit is presented in Figure 2.

Let's assume the measurement result is zero. Hence, we know that in the computational basis, Alice's **EPR** part agrees with $|\psi\rangle$, or in other words, if we measure the entire system in the computational basis, then the $|\psi\rangle$ bit would be equal to Alice's bit, and therefore would also be equal to Bob's bit. From here, we understand that the probability of Bob's bit being measured as zero equals the probability of $|\psi\rangle$ being measured as zero.

What happens if the result measurement is 1? In that case, we find that $|\psi\rangle$ disagrees with Alice's part and hence also disagrees with Bob's part. We can fix it by applying a Pauli correction, and that is the reason for the controlled XOR at the end of the teleportation.

$$] |\psi\rangle \otimes |\mathbf{EPR}\rangle \left(\alpha |0\rangle + \beta |1\rangle\right)$$
$$\rightarrow \frac{1}{\sqrt{2}}\alpha |000\rangle + \frac{1}{\sqrt{2}}\beta |110\rangle \frac{1}{\sqrt{2}} + \alpha |011\rangle + \frac{1}{\sqrt{2}}\beta |101\rangle$$
$$\rightarrow \frac{1}{2}\alpha |000\rangle + \frac{1}{2}\alpha |100\rangle + \frac{1}{2}\beta |010\rangle \frac{1}{2} - \frac{1}{2}\beta |110\rangle + \frac{1}{2}\alpha |011\rangle + \frac{1}{2}\alpha |111\rangle + \frac{1}{2}\beta |001\rangle - \frac{1}{2}\beta |101\rangle$$
$$= \frac{1}{2} |00\rangle |\psi\rangle + \frac{1}{2} |01\rangle X |\psi\rangle + \frac{1}{2} |10\rangle Z |\psi\rangle + \frac{1}{2} |11\rangle XZ |\psi\rangle$$

---

[1]The assumption that Alice and Bob initially held a valid **EPR** pair is important, yet much weaker than assuming they have a private key.

Figure 2: Measuring the single-qubit state $|\psi\rangle$ at the $\{|+\rangle, |-\rangle\}$ base.

4 Gate Teleportation.

Gate teleportation is a method to 'encode' operations by states. At the high level, given a precomputed state, it allows one to apply an operation (gate) by using (probably) simpler gates. The precomputed states are called **Magic States**.

4.1 Leading Example: T-Teleportation.

Recall that the Clifford[2] + T is a universal quantum gate set. The Clifford group alone is considered from the computer science point of view a simple/weak computational class since it can be classically simulated [3]. Yet, we will see that given access to the magic $|T\rangle = T|+\rangle$, one can simulate the T gate using only Clifford gates and measurements.

Figure 3: Measuring the single-qubit state $|\psi\rangle$ at the $\{|+\rangle, |-\rangle\}$ base.

$$\left(\sum_x \alpha_x |x\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle\right) \xmapsto{\mathbf{CX}} \sum_{x,y} \frac{1}{\sqrt{2}}\alpha_x |x\rangle |x \oplus y\rangle e^{i\frac{\pi}{4}y}$$

$$\mapsto \begin{cases} \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}x} = T|\psi\rangle & \text{measured 0} \\ \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}\bar{x}} & \text{measured 1} \end{cases}$$

$$\xmapsto{\mathbf{CS}} \begin{cases} T|\psi\rangle \\ \sum_x \alpha_x |x\rangle e^{i\left(\frac{\pi}{4}\bar{x}+\frac{\pi}{2}x\right)} = \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}}e^{i\left(\frac{\pi}{4}\bar{x}+\frac{\pi}{4}x\right)} \end{cases}$$

$$= \begin{cases} T|\psi\rangle \\ e^{i\frac{\pi}{4}}\sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}} = e^{i\frac{\pi}{4}}T|\psi\rangle \end{cases}$$

---

[2] Generated by H, S and CX

[3] And conjectured to be strictly weaker than **P**

4.2 Extends it.

Let's extends it to a general gate. First create $|\mathbf{GHZ}_{2n}\rangle$ state, then
Let's split upon the measurement result.

1. If we measured 0, means the states 'agreed' in the computational base.

$$|\psi\rangle \otimes \left(\sum_x |x\rangle \otimes U |x\rangle \right)$$

5 Uhlmann's theorem

Claim 5.1.

$$\langle \Omega | A \otimes B | \Omega \rangle = \mathbf{Tr} AB^\dagger$$

Proof.

$$\langle \Omega | A \otimes B | \Omega \rangle = \sum_{ij} \langle i; i | AB | j; j \rangle = \sum_{ij} \langle i | A | j \rangle \langle i | B | j \rangle = \sum_{ij} \langle i | A | j \rangle \langle j | B^\dagger | i \rangle$$

$$= \sum_i \langle i | AB^\dagger | i \rangle = \mathbf{Tr} AB^\dagger$$

$\square$

$$|\psi_\rho\rangle = \sum_i \left(\rho^{\frac{1}{2}} |\psi_i\rangle \right) |i\rangle = \sum_i \left(\rho^{\frac{1}{2}} U_\rho |i\rangle \right) |i\rangle = \left(\rho^{\frac{1}{2}} U_\rho \right) \otimes I |\Omega\rangle$$

$$|\psi_\sigma\rangle = \sum_i \left(\sigma^{\frac{1}{2}} |\psi'_i\rangle \right) |i'\rangle = \sum_i \left(\sigma^{\frac{1}{2}} U_\sigma |i\rangle \right) V |i\rangle = \left(\sigma^{\frac{1}{2}} U_\sigma \right) \otimes V |\Omega\rangle$$

Claim 5.2. *For any square matrix A:*

$$\max_{U \in \mathcal{U}} \mathbf{Tr} AU = \mathbf{Tr} \sqrt{A^\dagger A}$$

$$\max |\langle \psi_\rho | \psi_\sigma \rangle|^2 = \max |\langle \Omega | \left(U_\rho^\dagger \rho^{\frac{1}{2}} \right) \otimes I \left(\sigma^{\frac{1}{2}} U_\sigma \right) \otimes V |\Omega\rangle |^2$$

$$= \max |\mathbf{Tr} \left[\left(U_\rho^\dagger \rho^{\frac{1}{2}} \sigma^{\frac{1}{2}} U_\sigma \right) V^\dagger \right] |^2$$

$$= \max |\mathbf{Tr} \left[\rho^{\frac{1}{2}} \sigma^{\frac{1}{2}} V^\dagger \right] |^2$$

$$\leq \left| \mathbf{Tr} \sqrt{\rho^{\frac{1}{2}} \sigma^{\frac{1}{2}} \sigma^{\frac{1}{2}} \rho^{\frac{1}{2}}} \right|^2 = \left| \mathbf{Tr} \sqrt{\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}}} \right|^2$$

4

6 Monotonicity of Fidelity.

Let $\rho_{AB}, \sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then the fidelity is non-decreasing with respect to the partial trace:

$$F(\rho_{AB}, \sigma_{AB}) \leq F(\rho_A, \sigma_A),$$

where $\rho_A = \text{Tr}_B\{\rho_{AB}\}$ and $\sigma_A = \text{Tr}_B\{\sigma_{AB}\}$.

Proof. Consider fixed purifications $|\psi\rangle_{RAB}$ and $|\phi\rangle_{RAB}$ of ρ_{AB} and σ_{AB}, respectively, which also purify ρ_A and σ_A. By Uhlmann's theorem,

$$F(\rho_{AB}, \sigma_{AB}) = \max_{U_R} |\langle\psi|U_R \otimes I_A \otimes I_B|\phi\rangle|^2.$$

On the other hand, since $U_R \otimes I_A$ is a subset of the larger class of unitaries U_{RB} on RB,

$$F(\rho_A, \sigma_A) = \max_{U_{RB}} |\langle\psi|U_{RB} \otimes I_A|\phi\rangle|^2 \geq F(\rho_{AB}, \sigma_{AB}).$$

Thus, we conclude that

$$F(\rho_{AB}, \sigma_{AB}) \leq F(\rho_A, \sigma_A).$$

$\square$

Notice that $|i\rangle\langle j|$ is unitray since.

7 $|\text{EPR}\rangle$ Distillation.

Distillation of entanglement is a process in quantum information theory where a mixed entangled state is transformed into a more pure form of entanglement. This is achieved by using local operations and classical communication (LOCC) to extract a smaller number of highly entangled pairs from a larger number of weakly entangled pairs. The goal is to maximize the quality of entanglement, making it more suitable for quantum communication and computation tasks.

The process involves multiple copies of a mixed entangled state, which are manipulated to increase the fidelity of the entanglement. Distillation protocols, such as the Bennett-Brassard protocol, are used to achieve this transformation. The distilled entangled states are more robust and can be used for tasks like quantum teleportation and superdense coding, where high-quality entanglement is crucial for optimal performance.

$$\rho = p\,|\beta_{00}\rangle\langle\beta_{00}| + \frac{1-p}{3}\sum_{j \neq 00}|\beta_j\rangle\langle\beta_j|$$

The density matrix over each qubit is $\frac{1}{2}I$, so the measurement is equivalent to flipping coins and asking if the first pair and second pair are the same. Thus, the success
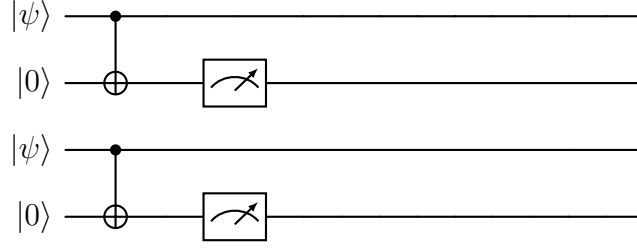
Figure 4: Measuring the single-qubit state $|\psi\rangle$ at the $\{|+\rangle, |-\rangle\}$ base.

probability is $\frac{1}{4}$. Now the state that is left is the projection of ρ into the space in which both the bits of Alice and Bob are equal, namely:

$$\frac{1}{4}((|00\rangle \pm |11\rangle) \otimes (|00\rangle \pm |11\rangle)) \rightarrow (|0000\rangle + |1111\rangle)$$

$$\frac{1}{4}((|00\rangle \pm |11\rangle) \otimes (|00\rangle \mp |11\rangle)) \rightarrow (|0000\rangle - |1111\rangle)$$

$$\frac{1}{4}((|00\rangle \pm |11\rangle) \otimes (|01\rangle \pm |01\rangle)) \rightarrow \emptyset$$

$$\frac{1}{4}((|01\rangle \pm |10\rangle) \otimes (|01\rangle \pm |10\rangle)) \rightarrow (|0101\rangle + |0101\rangle)$$

$$\frac{1}{4}((|01\rangle \pm |10\rangle) \otimes (|01\rangle \mp |10\rangle)) \rightarrow (|0101\rangle - |0101\rangle)$$

$$p^2 + 2\frac{p(1-p)}{3} + \frac{1}{3}(1-p)^2 + 4\frac{1}{3}(1-p)^2$$

$$p' \leftarrow \frac{p^2 + \frac{1}{3}(1-p)^2}{p^2 + 2\frac{p(1-p)}{3} + \frac{1}{3}(1-p)^2 + 4\frac{1}{3}(1-p)^2}$$

8 Magic State Distillation.

Question. Can we purify noisy magic states into high-fidelity ones, using only Clifford operations?

Magic state distillation is a procedure that uses many copies of noisy magic states, plus only Clifford gates and measurements, to produce fewer, higher-fidelity magic states.