1. Entanglement swapping protocol

Imagine four parties A, B, C, D such that A and B are very distant, C and D are very distant, but B and C sit in the same lab. We further imagine that A and B manage to share an entanglement link in state

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A|1\rangle_B)$$

and similarly for C and D

$$|\Phi_{CD}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_C \otimes |0\rangle_D + |1\rangle_C|1\rangle_D)$$

We want to create a direct entanglement link between A and D. This can be done by "entanglement swapping" as you will show here.

a) What is the total Hilbert space of A, B, C, D? what is the dimension of this space? and what is their global state?

b) Imagine that B and C (who sit close by) do a joint measurement in the Bell basis. Meanwhile A and D do not perform any specific operation. What will be the possible states of BC after the measurement? What is the global state after the measurement? And the state of AD?

2. Secret sharing protocol: a simple example with three parties and qutrit states

Suppose n distant parties want to share a common secret so that each party gets only a share of the secret. The secret is encoded in a string of n bits, such that any k parties that cooperate together can reconstruct the secret, but any $k-1$ of them (or less) cannot reconstruct it. These are called (k, n) secret sharing schemes in the classical case.

In quantum secret sharing schemes the secret is (typically) a quantum state which is suitably "encoded" into a state state of n qubits (or qutrits, qudits,...). These are distributed to n parties. We require that any k parties that cooperate together can reconstruct the secret, but any $k-1$ of them (or less) cannot reconstruct it. These are called $((k, n))$ quantum secret sharing schemes. One must necessarily have $k > \frac{n}{2}$ otherwise two disjoint groups of users would be able to reconstruct two copies of the secret state, thereby violating the no-cloning theorem (in other words a quantum secret sharing scheme cannot exist for $k \leq n/2$).

In this problem we scratch the surface of this topic by looking at the following simple example. Suppose the quantum secret is a qutrit state in the Hilbert space $\mathcal{H} = \mathbb{C}^3$ with orthonormal "computational basis" basis $\{|0\rangle, |1\rangle, |2\rangle\}$:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$$

To distribute the secret among 3 parties we first map it to (this can be done via some unitary transform in $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ where we add two ancilla qubits):

$$|\Psi\rangle \otimes |0\rangle \otimes |0\rangle \rightarrow \frac{\alpha}{\sqrt{3}}\big(|000\rangle + |111\rangle + |222\rangle\big) + \frac{\beta}{\sqrt{3}}\big(|012\rangle + |120\rangle + |201\rangle\big) + \frac{\gamma}{\sqrt{3}}\big(|021\rangle + |102\rangle + |210\rangle\big)$$

This is a three-qubit state and each qubit is distributed to Alice, Bob, Charlie.

a) Each of them alone (Alice, Bob, Charlie) has no information to reconstruct the original state. This can be neatly proved by computing the reduced density matrix and the association von Neumann entropy. Prove it!

b) What are the measurement outcomes and their respective probabilities, of say A, when she measures in the computational basis? Same question for B and C?

c) Now we want to show that there exists a $((2, 3))$ threshold scheme. Suppose A and B cooperate by doing the following unitary operation (or circuit) $\mathrm{CNOT}_{B\to A}\mathrm{CNOT}_{A\to B}$ defined as (sums are modulo 3)

$$\mathrm{CNOT}_{A\to B}|x\rangle_A \otimes |y\rangle_B = |x\rangle_A \oplus |y \oplus x\rangle_B, \quad \mathrm{CNOT}_{B\to A}|x\rangle_A \otimes |y\rangle_B = |x \oplus y\rangle_A \oplus |y\rangle_B$$

Draw the corresponding circuit and give the resulting state at the output of the corresponding circuit?
It turns out that A or B, but not both, gets the initial secret in their Hilbert space: who gets it?

3. W states, reduced density matrices, and von Neumann entropy

The W_θ state is defined here as

$$|W_\theta\rangle = \frac{\cos\theta}{\sqrt{2}}|100\rangle + \frac{\cos\theta}{\sqrt{2}}|010\rangle + \sin\theta|001\rangle$$

This and similar ones play an important role in quantum communication protocols. In this exercise we look at a few of its properties in order to illustrate the concept of reduced density matrix, partial trace, and von Neumann entropy. In what follows we assume that Alice, Bob and Charlie each have a one-qubit share of the state.

a) Compute the reduced density matrices ρ_C and ρ_{AB}.

b) What is the dimension of these matrices, their eigenvectors and corresponding eigenvalues of each density matrix? Check that your results are consistent with the Schmidt theorem.

c) What is the von Neumann entropy associated to the C and AB systems?

Remark: We will come back to this exercise later in class. The reduced density matrix of teh AB system has interesting properties. We will show that for θ below a critical value the AB system is "Bell-non-local" in the sense that ρ_{AB} violates the Bell inequality; and that for θ above that value the Bell inequality is not violated although there is still some amount of entanglement. For pure states the situation is simpler: as soon as there is some amount of entanglement the Bell inequality is violated.

4. Dynamics of 1-qubit density matrix

In class we showed that the general form of a 1-qubit density matrix is

$$\rho = \frac{1}{2}(I + \vec{a} \cdot \vec{\sigma})$$

where $\vec{a} = a_x, a_y, a_z)$ is a vector in the unit three dimensional ball (the Bloch *ball*) $\|\vec{a}\| \leq 1$ and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are the three usual Pauli matrices. Consider the dynamics of this mixed state generated by the Hamiltonian of the qubit in a static plus rotating magnetic field in the rotating frame (as seen in class, $\omega_1 \propto$ the strength of the rotating field and and $\delta = \omega - \omega_0$ the detuning between the Larmor and rotating field frequencies)

$$H = \frac{\hbar\delta}{2}\sigma_z - \frac{\hbar\omega_1}{2}\sigma_x$$

a) Show that the density matrix at time t is of the form

$$\rho_t = \frac{1}{2}(I + \vec{a}(t) \cdot \vec{\sigma})$$

and compute the vector $\vec{a}(t)$. *Hint*: From the definition of the density matrix you can infer that

$$\rho_t = U_t \rho U_t^\dagger$$

with U_t the evolution operator.

b) Check that $\|\vec{a}(t)\| = \|\vec{a}\|$. So the vector $\vec{a}(t)$ evolves on a sphere (inside the Bloch ball) of radius given by the initial vector.

c) Find a simple proof of the last statement without ever computing $\vec{a}(t)$.