Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2024/25

— Exercise Sheet #6 —

Problem 1: LOCC protocols

A general LOCC protocol (local operations assisted with classical communication) describes a certain way n parties $1, 2, \ldots, n$ can perform operations on a shared quantum state $|\Psi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$. The protocol consists of rounds of local operations performed on the shared state; the parties can share information (such as measurement outcome) between the rounds. That is, in round k, in addition to the shared state $|\Psi_k\rangle$ ($|\Psi_1\rangle = |\Psi\rangle$), the parties have access to a shared "history" $h_k = (o_1, \ldots, o_{k-1}) \subseteq \mathbb{Z}^{k-1}$ ($h_1 = \emptyset$). One round consists of the following steps:

- In round k, one of the parties $X \in \{1, 2, \ldots, n\}$ performs a measurement on $|\Psi_k\rangle$ obtaining outcome o_k and post-measurement state $|\Phi_k\rangle \in \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n$; the measurement itself might depend on the history h_k. They append the measurement outcome o_k to the history: $h_{k+1} := (h_k, o_k)$.
- Then each party performs a local unitary (that depends on the history) on $|\Phi_k\rangle$, i.e., they transform $|\Phi_k\rangle$ into $|\Psi_{k+1}\rangle := (U_1(h_{k+1}) \otimes \ldots \otimes U_n(h_{k+1}))|\Phi_k\rangle$.

In this problem, we will show that any two-party (i.e., n=2) LOCC protocol can be realized in a single round with only one-way communication, i.e., a protocol involving just the following steps: Alice performs a single measurement described by POVM operators M_j, sends the result j to Bob, and then they perform a unitary operation $U_j \otimes V_j$ depending on the outcome of the measurement.
The idea is to show that the effect of any measurement which Bob can do can be simulated by Alice – up to local unitaries – so all of Bob's actions can be replaced by actions by Alice, except for a final unitary rotation. For simplicity, we assume that the Hilbert spaces of A and B are the same, $\mathcal{H}$, i.e., they share a state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$.

1. Show that a square matrix U is unitary if and only if U^T is unitary.
2. Using the existence of SVD (singular value decomposition), show that for any square matrix A there are unitaries U and V such that $A^T = UAV$.
3. Remember that every state $|\Psi\rangle$ can be written as $(\mathrm{I} \otimes X)|\Omega\rangle$, where $|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_i |ii\rangle$. Remember as well that $(\mathrm{I} \otimes O)|\Omega\rangle = (O^T \otimes \mathrm{I})|\Omega\rangle$. Using these identities show that for every state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ there is a unitary $U \in \mathcal{B}(\mathcal{H})$ such that for every matrix $M \in \mathcal{B}(\mathcal{H})$ there are two more unitaries $V, W \in \mathcal{B}(\mathcal{H})$ such that $(\mathrm{I} \otimes M)|\Psi\rangle = (VMU \otimes W)|\Psi\rangle$.
4. Show that given a unitary $U \in \mathcal{B}(\mathcal{H})$, another set of unitaries $\{V_i\}_{i=1}^n \subseteq \mathcal{B}(\mathcal{H})$ and a measurement $\{M_i\}_{i=1}^n \subseteq \mathcal{B}(\mathcal{H})$, the set of operators $\{V_i M_i U\}_{i=1}^n$ also forms a measurement. Using all the previous, show that given a state state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ and measurement $\{M_i\}_{i=1}^n \subseteq \mathcal{B}(\mathcal{H})$, there is a measurement $\{N_i\}_{i=1}^n \subseteq \mathcal{B}(\mathcal{H})$ and unitaries $\{W_i\}_{i=1}^n \subseteq \mathcal{B}(\mathcal{H})$ such that for all $i = 1, \ldots, n$,
$$(\mathrm{I} \otimes M_i)|\Psi\rangle = (N_i \otimes W_i)|\Psi\rangle.$$
5. Use this to explain how Alice can simulate any POVM measurement of Bob, and how this can be used to implement an arbitrary multi-round protocol with a single POVM measurement $\{M_j\}$ performed by Alice, followed by a local unitary operation $\{U_j \otimes V_j\}$ which depends on Alice's outcome.

Problem 2: Majorization

Let $x, y \in \mathbb{R}^n_{\geq 0}$. Let $x^\downarrow$ ($y^\downarrow$) be the vector obtained by ordering the entries of x (y) in decreasing order, $x_1^\downarrow \geq x_2^\downarrow \geq \ldots x_n^\downarrow$ and $y_1^\downarrow \geq y_2^\downarrow \geq \ldots y_n^\downarrow$. We say that y majorizes x, and write $x \prec y$, if for all $k = 1, 2, \ldots, n$,
$$x_1^\downarrow + \ldots + x_k^\downarrow \leq y_1^\downarrow + \ldots + y_k^\downarrow.$$

In this problem, we prove that $x \prec y$ implies that $x = \sum_j q_j P_j y$ for some probability distribution q_j and permutation matrices P_j. The proof will proceed by induction in the dimension n of the space.

1. Let $x, y \in \mathbb{R}^d_{\geq 0}$, $x \prec y$, and let the entries of x and y (denoted by x_k, y_k) be ordered descendingly.
2. Show that there exist k and $t \in [0, 1]$ such that $x_1 = ty_1 + (1 - t)y_k$. For which k does this work? For the following steps, we choose the *smallest such k*.
3. Define $D = tI + (1 - t)T$, where T is the permutation matrix which transposes the 1st and k-th matrix elements. What are the components of the vector Dy?
4. Define x' and y' by eliminating the first entry from x and Dy, respectively. Show that $x' \prec y'$.
5. Show that this way, we can inductively prove the claim.

Problem 3: Teleportation-insired protocols.

In this problem, we will get to know two variants of the teleportation protocol.

Part 1: Gate teleportation.

Gate teleportation is a variation of quantum teleportation that is being used in fault-tolerant quantum computation (a topic which will be covered later in the course of the lecture).
Suppose that we would like to perform a single-qubit gate (i.e., unitary) U on a qubit in state $|\psi\rangle$, but the gate is difficult to perform – e.g., it might fail and thereby destroy the state on which we act on. On the other hand, the gate $U\sigma_j U^\dagger$, where σ_j is any one of the three Pauli matrices, is easy to perform.

1. Verify that such a situation is given when the difficult operation is $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{smallmatrix}\right)$, while Paulis and $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$ are easy to realize.
2. Consider the following protocol to implement U on a state $|\psi\rangle_{A'}$:
   - Prepare $|\chi\rangle_{AB} = (I_A \otimes U_B)|\Phi^+\rangle_{AB}$, with $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. ($U_B$ is still hard to implement, but we can try as many times as we want without breaking anything.)
   - Perform a measurement of $A'A$ in the Bell basis (A' is the register used to store $|\psi\rangle_{A'}$).
   - Depending on the measurement outcome, apply $U\sigma_j U^\dagger$ on the B system.

   Show that this protocol works as it should – that is, it yields the state $U|\psi\rangle$ in the B register with unit probability.

Part 2: Remote state preparation.

Remote state preparation is another variation on the teleportation protocol. In the variant we consider here, Alice has a *classical description* of a state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$ (on the equator of the Bloch sphere), i.e., she knows ϕ. The task is to prepare the state $|\psi\rangle$ on Bob's side, without Bob learning anything about ϕ.
To this end, let Alice and Bob share a maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

1. Find a state $|\chi\rangle$ such that when Alice's part of $|\Phi^+\rangle$ is projected onto $|\chi\rangle$, Bob is left with $|\psi\rangle$.
2. Now let Alice perform a measurement in the basis $\{|\chi\rangle, |\chi^\perp\rangle\}$, where $|\chi^\perp\rangle$ is the state perpendicular to $|\chi\rangle$ (since the space is 2-dimensional, $|\chi^\perp\rangle$ is unique up to a phase). Determine the post-measurement state of Bob for both of Alice's outcomes.
3. Show that if Alice communicates one bit to Bob, and Bob performs an operation which depends on this bit (which information is in the bit? what operation does Bob have to perform?), then Bob recovers $|\psi\rangle$ with unit probability.
4. A more "direct" way – given we know the protocol for teleportation – for Alice and Bob to realize the remote state preparation protocol would have been that Alice prepares $|\psi\rangle$ and then teleports it to Bob. Is there a way to relate these two protocols? How can the remote state preparation protocol be interpreted in terms of teleportation? In particular, in the teleportation protocol, Alice would have had to send *two* bits to Bob – what happened to the second bit?