Lecture & Proseminar 250120/250122
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2020/21

— Exercise Sheet #6 —

Problem 1: Remote state preparation.
Remote state preparation is a 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.

Problem 2: Gate teleportation.
Gate teleportation is a variation of quantum teleportation that is being used in fault-tolerant quantum computation (coming up later in 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, $U\sigma_j U^\dagger$, 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 $|\Phi^+\rangle$ as before. (U_B is still hard, 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.

Problem 3: LOCC protocols.
A general LOCC protocol can involve an arbitrary number of rounds of measurement and classical communication. In this problem, we will show that any 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 Bob performs a unitary operation U_j on his system.
The idea is to show that the effect of any measurement which Bob can do can be simulated by Alice – in a specific sense, namely up to local unitaries – so all of Bob's actions can be replaced by actions by Alice, except for a final unitary rotation.

1. First, suppose Alice and Bob share the state $|\psi\rangle = \sum \lambda_l |l\rangle_A |l\rangle_B$, and suppose Bob performs a measurement with POVM operators $K_j = \sum_{kl} K_{j,kl} |k\rangle_B \langle l|_B$. Let us denote the post-measurement state by $|\alpha_j\rangle$. On the other hand, suppose that Alice does a measurement with POVM operators with operators $L_j = \sum_{kl} K_{j,kl} |k\rangle_A \langle l|_A$, and denote the post-measurement state by $|\beta_j\rangle$.

   Show that there exist unitaries V_j on system A and W_j on system B such that $|\alpha_j\rangle = (V_j \otimes W_j)|\beta_j\rangle$.

2. 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 unitary operation $\{U_j\}$ on Bob's side by Bob which depends on Alice's outcome.
   (*Hint:* The bases $|l\rangle_A$ and $|l\rangle_B$ above could be an arbitrary orthonormal basis!)