Lecture & Proseminar 250121/250122
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2025/26

— Exercise Sheet #8—

Problem 20: 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!)

Problem 21: Majorization.

Let $x, y \in \mathbb{R}^d$ be two probability vectors (i.e., $x_1, \ldots, x_d \geq 0$, and $\sum_{i=1}^d x_i = 1$). Recall that $x \prec y$ ("x is majorized by y") by definition if

$$\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow ,$$

where $x^\downarrow$ has the same entries as the vector x, but the entries have been ordered descendingly.

Our goal is to show that $x \prec y$ is equivalent to the existence of a probability distribution q_j and permutation matrices P_j such that $x = \sum_j q_j P_j y$.

First, show that $x = \sum_j q_j P_j y$ implies $x \prec y$. (Don't forget that you have to order the entries of $x = \sum_j q_j P_j y$.)

Next, let us show the converse: That $x \prec y$ implies that there exists a probability distribution q_j and permutation matrices P_j such that $x = \sum_j q_j P_j y$. The proof will use induction in the dimension d of the space. To this end, proceed through the following steps.

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 $x_1 = t y_1 + (1 - t) y_k$. 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 22: Optimality of diagonal POVMs in single-copy entanglement conversion.

In the lecture, we have discussed single-copy entanglement conversion protocols with the restriction that the POVM (carried out by Alice) was diagonal in the Schmidt basis. What we found is that we can convert a state

$$|\phi\rangle = \sum \sqrt{\gamma_i}|i\rangle|i\rangle$$

into a state

$$|\psi\rangle = \sum \sqrt{\mu_i}|i\rangle|i\rangle$$

precisely if $\gamma \prec \mu$. The goal of this problem is to show that we cannot do better even with general POVMs.

In the following, for a hermitian matrix A, let $\lambda(A)$ denote the descendingly ordered eigenvalues of A.

A useful tool will be the Ky-Fan maximum principle. It says for a hermitian operator A,

$$\sum_{i=1}^{k} \lambda_i(A) = \max_P \operatorname{tr}[PA] \ ,$$

where the maximization is over all (hermitian) projectors onto subspaces of dimension k. (This should sound intuitive: The best you can do is to choose P the projector onto the joint eigenspace of the k largest eigenvalues. You are encouraged to prove this based on this observation, but you can use the result without proof.)

1. Use the Ky-Fan maximum principle to prove that
$$\lambda(A+B) \prec \lambda(A) + \lambda(B) \ . \qquad (1)$$

2. Consider an LOCC protocol which converts (deterministically) $|\phi\rangle$ into $|\psi\rangle$, where Alice applies a POVM measurement $\{M_k\}$, with (un-normalized) post-measurement states $|\phi_k\rangle = (M_k \otimes I)|\phi\rangle$. Let $\rho = \operatorname{tr}_A(|\phi\rangle\langle\phi|)$ denote the reduced density matrix of Bob (!) before the measurement, and $\rho_k = \operatorname{tr}_A(|\phi_k\rangle\langle\phi_k|)$ the corresponding (un-normalized) post-measurement reduced state of Bob.
Show that $\sum_k \rho_k = \rho$.

3. Use Eq. (1) to show that
$$\lambda(\rho) \prec \sum \lambda(\rho_k) \ .$$

4. In terms of the Schmidt coefficients of $|\phi\rangle$ and/or $|\psi\rangle$: What are the eigenvalues of ρ, $\lambda(\rho)$? What are the (ordered) eigenvalues of ρ_k, $\lambda(\rho_k)$, given that the we are considering a protocol which converts $|\phi\rangle$ deterministically into $|\psi\rangle$ (which means that for all k, $|\psi\rangle = (I \otimes U_k)|\phi_k\rangle$ for some unitary U_k)?

5. Use this to show that the protocol with diagonal POVMs, as discussed in the lecture is optimal (recall that such a protocol exists *if and only if* $\gamma \prec \mu$).

(*Remark:* Working with the reduced state of Bob makes our life a bit easier, since we can directly use that $\lambda(\sum \rho_k) = \lambda(\rho) = \gamma$. Nevertheless, we could have (unsurprisingly!) achieved the same using the reduced state of Alice, with a little bit more effort: Denoting the reduced state of Alice by $\tilde{\rho}$, and the post-measurement states by $\tilde{\rho}_k$, we have that (by construction) $\tilde{\rho}_k = M_k \tilde{\rho} M_k^\dagger$. We now have to use that the (non-zero part of the) spectrum is cyclic, i.e., $\lambda(AB) = \lambda(BA)$, and thus

$$\lambda\big(\sum \tilde{\rho}_k\big) = \lambda\big(\sum M_k \tilde{\rho} M_k^\dagger\big) = \lambda\big(\sum M_k^\dagger M_k \tilde{\rho}\big) = \lambda(\rho) \ ,$$

using that $\sum M_k^\dagger M_k = I$.)