Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2022/23

— Exercise Sheet #3 —

Problem 8: Ambiguity of ensemble decomposition.

Complete the proof given in the lecture for the relation

$$\sqrt{p_i}|\psi_i\rangle = \sum u_{ij}\sqrt{q_j}|\phi_j\rangle$$

of different ensemble decompositions

$$\rho = \sum p_i|\psi_i\rangle\langle\psi_i| = \sum q_j|\phi_j\rangle\langle\phi_j| \ .$$

1. Show that for any ensemble decomposition $\rho = \sum q_i|\phi_i\rangle\langle\phi_i|$ with $q_i > 0\ \forall\, i$, it holds that $|\phi_i\rangle \in \mathrm{supp}(\rho)$. Here, $\mathrm{supp}(\rho)$ is the support of ρ as a linear map, that is, the orthogonal complement of its kernel $\ker(\rho)$. How does this justify the restriction $q_i \neq 0$ made in the lecture?

2. Show that any ensemble decomposition must have at least as many terms as the eigenvalue decomposition $\rho = \sum \lambda_k|e_k\rangle\langle e_k|$.

3. Show that the proof from the lecture extends to the case where the other decomposition has more terms than the eigenvalue decomposition, to show

$$\sqrt{p_i}|\psi_i\rangle = \sum u_{ik}\sqrt{\lambda_k}|e_k\rangle \ . \qquad (*)$$

   What property does this imply for $U = (u_{ik})$?

4. Show that that the relation $(*)$ can be inverted to give a formula for $\sqrt{\lambda_k}|e_k\rangle$.

5. Now consider the case where neither of the two ensembles is an eigenvalue decomposition. Use the fact that there are $U = (u_{ik})$ and $V = (v_{jk})$ which connect them to the eigenvalue decomposition to derive the general relation between two ensemble decompositions of a given state ρ. What is the form of the transformation matrix $W = (w_{ij})$ in terms of U and V? What properties do $W^\dagger W$ and $WW^\dagger$ satisfy?

Problem 9: Measurements and filtering

Suppose that a bipartite system AB is initially in the state

$$|\phi_\lambda\rangle = \sqrt{\lambda}|00\rangle + \sqrt{1-\lambda}|11\rangle \ .$$

The goal of Alice and Bob is to obtain a maximally entangled state

$$|\Omega\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

with some probability by applying local operations only. Specifically, the plan is that Alice will apply a POVM measurement to achieve that.

1. Show that the operators $M_0 = (|0\rangle\langle 0| + \sqrt{\gamma}|1\rangle\langle 1|)_A \otimes I_B$ and $M_1 = \sqrt{1-\gamma}|1\rangle\langle 1|_A \otimes I_B$, with $0 \leq \gamma \leq 1$, define a POVM measurement. (Note that these describe measurements carried out on Alice's side only!)

2. Determine the outcome probabilities and the post-measurement states for both measurement outcomes.

3. Find a value γ such that one of post-measurement states becomes a maximally entangled state. Calculate the corresponding probability with which the initial state becomes a maximally entangled state.

4. In the lecture, we have shown that any POVM measurement can be implemented by adding an auxiliary system in state $|0\rangle$, applying a unitary, and measuring the auxiliary system in the computational basis. Construct such a unitary for the POVM of Alice above.

Problem 10: SIC-POVMs

A *symmetric informationally complete POVM* (SIC-POVM) in d dimensions is a POVM $\{F_i\}_{i=1,\dots,d^2}$ consisting of d^2 operators $F_i = \lambda \Pi_i$, where the $\Pi_i = |\phi_i\rangle\langle\phi_i|$ are rank-1 projectors $\Pi_i^2 = \Pi_i$, such that

i) $\sum_{i=1}^{d^2} F_i = I$ (i.e. the F_i form a POVM), and

ii) $\mathrm{tr}(F_i F_j) = K$ for $i \neq j$, where K is independent of i and j (that is, the POVM is *symmetric*).

1. Use the two conditions (i) and (ii) to determine the values of λ and K.
2. Now consider $d = 2$ (qubits). Consider four states $|\phi_i\rangle$ sitting at the four corners of a tetrahedron. (Any tetrahedron is good, but it might be convenient to have one corner along the z axis and another one in the x-z-plane.) Derive the form of $|\phi_i\rangle$, and show that they give rise to a SIC-POVM (following the convention above).
3. Show that the operators $\{F_i\}$ of a SIC-POVM (with the conditions (i) and (ii) above, for arbitary d) are linearly independent. (*Easier version:* Show this only for the qubit SIC-POVM constructed in point 2.)
4. Show that the linear independence of the $\{F_i\}$ implies that there exist K_i such that we can write

$$\rho = \sum_{i=1}^{d^2} G_i \,\mathrm{tr}[K_i \rho]$$

– that is, the POVM is *informationally complete*, i.e., we can reconstruct any state ρ from the outcome probabilities of the POVM. What is the form of the K_i?