Quantum Information Theory
Series 10

Exercise 10.1 Fidelity and Uhlmann's Theorem

Given two states ρ and σ on $\mathcal{H}_A$ with fixed basis $\{|A\rangle_i\}_i$ and a reference Hilbert space $\mathcal{H}_B$ with fixed basis $\{|B\rangle_i\}_i$, which is a copy of $\mathcal{H}_A$, Uhlmann's theorem claims that the fidelity can be written as

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle| \,, \tag{1}$$

where the maximum is over all purifications $|\psi\rangle$ of ρ and $|\phi\rangle$ of σ on $\mathcal{H}_A \otimes \mathcal{H}_B$. Let us introduce a state $|\psi\rangle$ as:

$$|\psi\rangle = (\sqrt{\rho} \otimes U_B)\,|\gamma\rangle, \qquad |\gamma\rangle = \sum_i |A\rangle_i \otimes |B\rangle_i, \tag{2}$$

where U_B is any unitary on $\mathcal{H}_B$.

a) Show that $|\psi\rangle$ is a purification of ρ.

b) Argue why every purification of ρ can be written in this form.

c) Use the construction presented in the proof of Uhlmann's theorem to calculate the fidelity between $\sigma' = \mathbb{1}_2/2$ and $\rho' = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ in the 2-dimensional Hilbert space with computational basis.

d) Give an expression for the fidelity between any pure state and the completely mixed state $\mathbb{1}_n/n$ in the n-dimensional Hilbert space.

Exercise 10.2 Classical Stein lemma

The aim of this exercise is to prove the classical version of the Chernoff-Stein Lemma.
We first define few notions we will need.
For a fixed n and $\epsilon > 0$, a sequence $(x_1, ..., x_n) \in X^n$ is said to be *relative entropy typical* if and only if:

$$D(P_1||P_2) - \epsilon \le \frac{1}{n}\log\frac{P_1(x_1,...,x_n)}{P_2(x_1,...,x_n)} \le D(P_1||P_2) + \epsilon$$

The set of relative entropy typical sequences is called the relative entropy typical set $A_\epsilon^{(n)}(P_1||P_2)$.
Now prove the following (use the first statement to prove the others):

- (AEP for relative entropy) Let $X_1, ..., X_n$ be a sequence of RV drown i.i.d. according to $P_1(x)$, and let $P_2(x)$ be any other distribution on X. Then

$$\frac{1}{n}\log\frac{P_1(X_1,...,X_n)}{P_2(X_1,...,X_n)} \to D(P_1||P_2)$$

  in probability.

- For $(x_1, x_2, ..., x_n) \in A_\epsilon^{(n)}(P_1||P_2)$,

$$P_1(x_1,..,x_n)2^{-n(D(P_1||P_2)+\epsilon)} \le P_2(x_1,..,x_n) \le P_1(x_1,..,x_n)2^{-n(D(P_1||P_2)-\epsilon)}$$

- $P_1(A_\epsilon^n(P_1||P_2)) > 1-\epsilon$, for sufficiently large n.
- $P_2(A_\epsilon^n(P_1||P_2)) < 2^{-n(D(P_1||P_2)-\epsilon)}$
- $P_2(A_\epsilon^n(P_1||P_2)) > (1-\epsilon)2^{-n(D(P_1||P_2)+\epsilon)}$

Now let $X_1, ..., X_n$ be i.i.d $\sim Q$. Consider the hypothesis test between two alternatives, $Q = P_1$ and $Q = P_2$, where $D(P_1||P_2) < \infty$. Let $A_n \in X^n$ be an acceptance region for hypothesis H_1. Let the probabilities of error be

$$\alpha_n = P_1^n(A_n^c),\ \beta_n = P_2^n(A_n)$$

Prove that for any $0 < \epsilon < \frac{1}{2}$

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n \leq -(D(P_1||P_2) - \epsilon)$$

In particular, no other sequence of sets B_n can do better than A_n, *i.e.*:

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n^{\epsilon} = -D(P_1||P_2)$$

where $\beta_n^{\epsilon} = \min_{A_n \in X^n, \alpha_n < \epsilon} \beta_n$.

Exercise 10.3 Resource inequalities

Show that following inequality can hold:

$$\beta[q \to q] + \alpha[qq] \geq 2[c \to c]$$

only if $\alpha + \beta \geq 2$
Hint: Use Holevo's bound.