Holevo theorem

Holevo's theorem gives a nice, computable upper bound to the *accessible information* present in an ensemble of quantum states.

Suppose that Alice prepares some classical ensemble $\mathcal{E} = \{p(x), \rho_x\}_{x\in\Sigma}$ and then sends the quantum state to Bob, without telling him the the classical index x, sampled from the distribution p. Bob's task is to determine the classical index x by performing some measurement on the quantum system he received from Alice. The quantity that governs how much information he can learn about random variable X if he possesses random variable Y (the outcome of his measurement) is the mutual information $I(X:Y)$.

Remark. Note that the task is different that the state discrimination problem:

- here we want to maximize the information Bob learns about X
- in state discrimination we want to maximize the *probability of success* that Bob guesses X correctly

Definition. Given an ensemble $\{p(x), \rho_x\}_{x\in\Sigma}$, define its *accessible information* as the maximum correlation (measured by the Mutual information) than can be extracted from it, by using a single measurement. If we call that measurement $M = (M_y)$, we have

$$p_{XY}(x, y) = p_X(x) p_{Y|X}(y|x)$$

with

$$p_{Y|X}(y|x) = \langle M_y, \rho_x \rangle$$

We define

$$I_{\text{acc}} := \sup_{M_y} I(X:Y)_{p_{XY}}$$

Theorem. We have the following upper bound: for any ensemble $\mathcal{E}$

$$I_{\text{acc}}(\mathcal{E}) \leq \chi(\mathcal{E}) := S\Big(\sum_x p(x)\rho_x\Big) - \sum_x p(x) S(\rho_x)$$

In general, it is very hard to compute I_{acc} hence the importance of the upper bound above.

Proof.

Start from Alice's state, which encodes the ensemble:

$$\rho_{AQ} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_x$$

$$\rho_Q = \sum_x p(x) \rho_x$$

Bob then performs a POVM on Q, yielding the state

$$\sigma_{AB} = [\mathrm{id}_A \otimes M_{Q\to B}](\rho_{AQ}) = \sum_x p(x) |x\rangle\langle x| \otimes \langle M_y, \rho_x\rangle |y\rangle\langle y|$$

The resulting distribution is

$$p_{AB}(x, y) = \sum_{x,y} p(x) \langle M_y, \rho_x\rangle$$

We have then

$$\begin{aligned} I(A:B)_p = I(A:B)_\sigma &= D(\sigma_{AB} || \sigma_A \otimes \sigma_B) \\ &= D([\mathrm{id}_A \otimes M_{Q\to B}](\rho_{AQ}) || \rho_A \otimes M_{Q\to B}(\rho_Q)) \\ &\leq D(\rho_{AQ} || \rho_A \otimes \rho_Q) \\ &= S(A)_\rho + S(Q)_\rho - S(AQ)_\rho \\ &= \chi(\mathcal{E}) \end{aligned}$$

finishing the proof.
