Part III Quantum Information Theory: Example Sheet 4
Class 4: Friday 29th Jan 2016, 14:00, MR14.

December 26, 2015

1. Prove that the Holevo information is superadditive. That is:

   Proposition 1. For any two operations $\mathcal{M}$ and $\mathcal{N}$, $\chi(\mathcal{N} \otimes \mathcal{M}) \geq \chi(\mathcal{N}) + \chi(\mathcal{M})$.

2. Show that the following statements about an operation $\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}}$ are equivalent

   (a) $\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}}$ is entanglement-breaking;

   (b) Its operator representation $\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}} \Phi^{+}_{\mathsf{A}'\mathsf{A}}$ is separable with respect to $\mathsf{A}' : \mathsf{B}$ bipartition;

   (c) It is a *measure-prepare* operation, that is, there exists a POVM $E : \mathcal{A}_X \to \mathcal{L}(\mathcal{H}_\mathsf{A})$ and map $\underline{\sigma} : \mathcal{A}_X \to \mathcal{L}(\mathcal{H}_\mathsf{B})$, taking $\mathcal{A}_X$ to states of B, such that

   $$\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}} : \rho_\mathsf{A} \mapsto \sum_{x \in \mathcal{A}_X} \underline{\sigma}(x)_\mathsf{B} \mathrm{Tr} E(x)_\mathsf{A} \rho_\mathsf{A}.$$

3. (a) A memoryless classical channel can be specified by giving the conditional probability distribution $N_{Y|X}$ which gives the distribution of the output symbol Y given the input symbol X for a single use of the channel. Given a conditional probability distribution $N_{Y|X}$ we can define an associated operation $\mathcal{N}^{\tilde{\mathsf{Y}} \leftarrow \tilde{\mathsf{X}}}$ by

   $$\mathcal{N}^{\tilde{\mathsf{Y}} \leftarrow \tilde{\mathsf{X}}} : \rho_{\tilde{\mathsf{X}}} \mapsto \sum_{y \in \mathcal{A}_Y} \sum_{x \in \mathcal{A}_X} |y\rangle\langle y|_{\tilde{\mathsf{Y}}} N_{Y|X}(y|x) \mathrm{Tr}_{\tilde{\mathsf{X}}} |x\rangle\langle x|_{\tilde{\mathsf{X}}} \rho_{\tilde{\mathsf{X}}}.$$

   This is a representation of one use of the classical channel, as a quantum operation, where the input and output are encoded in the computational bases. Use the HSW theorem to show that

   $$C(\mathcal{N}^{\tilde{\mathsf{Y}} \leftarrow \tilde{\mathsf{X}}}) = \max_{P_X} I(X : Y) \text{ where } P_{XY}(x, y) = N_{Y|X}(y|x) P_X(x),$$

   and where the maximisation is over probability distributions P_X on $\mathcal{A}_X$. This result, giving the classical capacity of a memoryless classical channel, is known as Shannon's noisy channel coding theorem.

   (b) Use this result to find an expression for the capacity of a binary symmetric channel in terms of its 'bit-flip' probability f.

4. Show that the Holevo information of an operation is always attained by an ensemble of *pure* states: That is

   $$\chi(\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}}) = I(\tilde{\mathsf{X}} : \mathsf{B})_\sigma$$

   where $\sigma_{\tilde{\mathsf{X}}\mathsf{B}} = \mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}} \rho_{\tilde{\mathsf{X}}\mathsf{A}}$ for some $\rho_{\tilde{\mathsf{X}}\mathsf{A}} = \sum_x P_X(x) |x\rangle\langle x|_{\tilde{\mathsf{X}}} \otimes |\psi^{(x)}\rangle\langle \psi^{(x)}|_\mathsf{A}$ where each $|\psi^{(x)}\rangle_\mathsf{A}$ is a state vector. (You can use without proof the fact that it is attained for an ensemble with a finite number of states.)

5. Show $C(\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}}) = 0$ iff there is some state σ_B such that $\mathcal{N}^{\mathsf{B} \leftarrow \mathsf{A}}$ maps every state of A to σ_B.

6. For $\lambda \in [0,1]$, the **depolarising operation** (of dimension two) with parameter λ is

$$\mathcal{D}_p^{\mathsf{B}\leftarrow\mathsf{A}}\rho_{\mathsf{A}} \mapsto (1-\lambda)\mathbf{id}^{\mathsf{B}\leftarrow\mathsf{A}}\rho_{\mathsf{A}} + \lambda\tau_{\mathsf{B}}\mathrm{Tr}_{\mathsf{A}}\rho_{\mathsf{A}}$$

where $\dim(\mathsf{A}) = \dim(\mathsf{B}) = 2$ and $\tau_{\mathsf{B}} = \mathbb{1}_{\mathsf{B}}/2$ is the maximally mixed state of B.

It can be shown (King 2003 `10.1109/TIT.2002.806153`) that the Holevo information is additive when one of the operations is a depolarising operation (i.e. for any $\mathcal{N}$, $\chi(\mathcal{D}_\lambda \otimes \mathcal{N}) = \chi(\mathcal{D}_\lambda) + \chi(\mathcal{N})$) so the HSW theorem tells us that $C(\mathcal{D}_\lambda) = \chi(\mathcal{D}_\lambda)$. Find an expression for $\chi(\mathcal{D}_\lambda)$.

7. The *mutual information* of an operation $\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}$ is defined by

$$I(\mathcal{N}^{\mathsf{B}\leftarrow\mathsf{A}}) := \sup\{I(\mathsf{R}:\mathsf{B})_{\mathcal{N}_{\mathsf{B}\leftarrow\mathsf{A}}\rho_{\mathsf{RA}}} : \text{ systems } \mathsf{R}, \text{ pure states } \rho_{\mathsf{RA}}\}. \tag{1}$$

If $\mathcal{N}$ is the operation for a single use of a memoryless quantum channel, then that channel has entanglement-assisted classical capacity $I(\mathcal{N})$ (for more details see Chapter 21 of Mark Wilde's book `http://http://arxiv.org/abs/1106.1445`.)

(a) Show that we can remove the restriction to pure states without changing the value of the supremum.

(b) Show that we can restrict to systems R of dimension d_{A} without changing the value of the supremum.

(c) Given a composite system $\mathsf{RB_1B_2}$ in an arbitrary state, use the chain rule for mutual information and positivity of mutual information to show that

$$I(\mathsf{R}:\mathsf{B_1B_2}) \leq I(\mathsf{R}:\mathsf{B_1}) + I(\mathsf{RB_1}:\mathsf{B_2}). \tag{2}$$

(d) Using the previous part, show that the mutual information of operations is additive in the sense that, given operations $\mathcal{N}_1^{\mathsf{B_1}\leftarrow\mathsf{A_1}}$ and $\mathcal{N}_2^{\mathsf{B_2}\leftarrow\mathsf{A_2}}$, we have

$$I(\mathcal{N}_1 \otimes \mathcal{N}_2) = I(\mathcal{N}_1) + I(\mathcal{N}_2). \tag{3}$$