Quantum Information Theory
Problem Set 9

Spring 2008
Prof. R. Renner

Problem 9.1 Some properties of von Neumann entropy

We will now derive some properties of the von Neumann entropy that will be useful in later exercises. The von Neumann entropy of a density operator $\rho \in \mathcal{S}(\mathcal{H})$ is defined as

$$S(\rho) = -\mathrm{tr}\big(\rho \log \rho\big) = -\sum_i \lambda_i \log \lambda_i. \tag{1}$$

where $\{\lambda_i\}_i$ are the eigenvalues of ρ. Given a composite system $\rho_{\mathrm{ABC}} \in \mathcal{S}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{C}})$ and $\rho_{\mathrm{AB}} = \mathrm{tr}_{\mathrm{C}}(\rho_{\mathrm{ABC}})$ etc., we often write $S(AB)$ instead of $S(\rho_{\mathrm{AB}})$ to denote the entropy of a subsystem. The strong sub-additivity property of the von Neumann entropy proves very useful:

$$S(ABC) + S(B) \leq S(AB) + S(BC). \tag{2}$$

Prove the following properties of the von Neumann entropy:

a) If ρ_{AB} is pure, then $S(A) = S(B)$.

b) If two subsystem are independent $\rho_{\mathrm{AB}} = \rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}$ then $S(AB) = S(A) + S(B)$.

c) If the system is classical on a subsystem Z, namely $\rho_{\mathrm{AZ}} = \sum_z p_z |z\rangle\langle z|_{\mathrm{Z}} \otimes \rho_{\mathrm{A}}^z$ for some basis $\{|z\rangle\langle z|_{\mathrm{Z}}\}_z$ of $\mathcal{H}_{\mathrm{Z}}$, then

$$S(AZ) = S(Z) + \sum_z p_z\, S(A|Z{=}z), \tag{3}$$

where $S(A|Z{=}z) = S(\rho_{\mathrm{A}}^z)$.

d) Concavity:

$$\sum_z p_z\, S(A|Z{=}z) \leq S(A). \tag{4}$$

e)

$$S(A) \leq S(AZ). \tag{5}$$

Problem 9.2 Upper bound on von Neumann entropy

Given a state $\rho \in \mathcal{S}(\mathcal{H})$, show that

$$S(\rho) \leq \log \dim \mathcal{H}. \tag{6}$$

Consider the state $\bar{\rho} = \int U \rho U^\dagger \,\mathrm{d}U$, where the integral is over all unitaries $U \in \mathcal{U}(\mathcal{H})$ and $\mathrm{d}U$ is the Haar measure. Find $\bar{\rho}$ and use concavity (4) to show (6). Hint: The Haar measure satisfies $\mathrm{d}(UV) = \mathrm{d}(VU) = \mathrm{d}U$, where $V \in \mathcal{U}(\mathcal{H})$ is any unitary.