

**Exercise 10.1 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

$$S(\rho) = -\text{tr}(\rho \log \rho) = -\sum_i \lambda_i \log \lambda_i. \quad (1)$$

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

$$S(ABC) + S(B) \leq S(AB) + S(BC). \quad (2)$$

Prove the following properties of the von Neumann entropy:

- a) If  $\rho_{AB}$  is pure, then  $S(A) = S(B)$ .
- b) If two subsystem are independent  $\rho_{AB} = \rho_A \otimes \rho_B$  then  $S(AB) = S(A) + S(B)$ .
- c) If the system is classical on a subsystem  $Z$ , namely  $\rho_{AZ} = \sum_z p_z |z\rangle\langle z|_Z \otimes \rho_A^z$  for some basis  $\{|z\rangle\langle z|_Z\}_z$  of  $\mathcal{H}_Z$ , then

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

where  $S(A|Z=z) = S(\rho_A^z)$ .

- d) Concavity:

$$\sum_z p_z S(A|Z=z) \leq S(A). \quad (4)$$

- e)

$$S(A) \leq S(AZ). \quad (5)$$

*Remark: Eq (5) holds in general only for classical  $Z$ . Consider, e.g., the Bell-States as an immediate counterexample in the fully quantum case.*

**Exercise 10.2 Upper bound on von Neumann entropy**

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

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

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