Freie Universität Berlin

Tutorials on Quantum Information Theory

Winter term 2021/22

Problem Sheet 6

Entropies and LOCC

J. Eisert, A. Nietner, F. Arzani, C. Bertoni, S. Suzuki

---

1. **On Shannon entropy...** (5 points: 1+2+2)

   To begin with let us first show some simple properties of entropies, in particular, of the mutual information.

   Recall the definition of the Shannon entropies for random variables X, Y which take values in $\mathcal{X}, \mathcal{Y}$ and are distributed according to probability distributions p, q over $\mathcal{X}$ and $\mathcal{Y}$, respectively.

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log p(x) \text{ (Shannon entropy)} \tag{1}$$

$$H(X|Y) = H(X,Y) - H(Y) = \sum_{x\in\mathcal{X}} p(x)H(Y|X=x) \text{ (Conditional entropy)} \tag{2}$$

   a) Show that $0 \le H(X) \le \log|\mathcal{X}|$, where the first equality holds *iff* there is an $x \in \mathcal{X}$ for which $p(x) = 1$ and the second inequality holds *iff* $p(x) = 1/|\mathcal{X}|$ for all x.

   b) Show that the Shannon entropy is *subadditive*, i.e., that $H(X,Y) \le H(X) + H(Y)$ with equality if X and Y are independent..

      Hint: Show that $H(X,Y) - H(X) - H(Y) \le 0$ *using that* $\log_2 x \ln 2 = \ln x \le x - 1$.

   c) Show that $H(Y|X) \ge 0$ equality if and only if Y is a (deterministic) function of X.

      Hint: Use Bayes' rule: $p(x,y) = p(y|x)p(x)$

2. **... and the von-Neumann entropy** (9 points: 1+2+2+2+1+1)

   For any state $\rho \in \mathcal{D}(\mathcal{H})$ with $\dim\mathcal{H} = d$ the von-Neumann entropy is defined as $S(\rho) = -\operatorname{Tr}(\rho\log\rho)$. Throughout this problem, if the global state being referred to is clear, we will denote entropies of the reduced states using the corresponding Hilbert space as an argument, e.g. the entropy of a state ρ_{AB} reduced on subsystem A is denoted $S(A)$.

   a) Show that $0 \le S(\rho)$ with equality if and only if ρ is pure. (One can also show the upper bound $S(\rho) \le \log d$.)

   b) Show that the von-Neumann entropy is *subadditive* in the sense that if two distinct systems A and B have a joint quantum state ρ^{AB} then $S(A,B) \le S(A) + S(B)$, with equality if $\rho_{AB} = \rho_A \otimes \rho_B$.

      Hint: You may use the inequality $S(\rho) \le -\operatorname{Tr}[\rho\log\sigma]$ *for an arbitrary quantum state* σ *and that for two matrices* A *and* B, $\log(A\otimes B) = \log(A)\otimes\mathbb{1} + \mathbb{1}\otimes\log(B)$.

   c) Suppose that $p = (p_i)_i$ is a probability vector and the states ρ_i are mutually orthogonal. Show that

$$S\left(\sum_i p_i\rho_i\right) = H(p) + \sum_i p_i S(\rho_i).$$

and use this result to infer that

$$S\left(\sum_i p_i \rho_i \otimes |i\rangle\langle i|\right) = H(p) + \sum_i p_i S(\rho_i),$$

where $\langle i|j\rangle = \delta_{ij}$ and the ρ_i are arbitrary quantum states.

d) Use the results from b) and c) to infer that the von-Neumann entropy S is concave, that is, $S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i)$ for a probability distribution $\{p_i\}$.

e) let Ω_{AB} be the maximally entangled state on two Hilbert spaces of equal dimension d, i.e. $\Omega = |\Omega\rangle\langle\Omega|$ with

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle . \tag{3}$$

Compute $S(A|B)$. What do you conclude?

f) Let ρ_{AB} be a bipartite state. Use the result of point c) to show that if ρ_A is separable, i.e. $\rho_{AB} = \sum_i p_i \sigma_A^i \otimes \tau_B^i$ where σ^i and τ^i are states, then $S(A|B) \geq 0$.

3. **Local operations and classical communication (LOCC).** (6 points: 2+2+1+1)

At the heart of entanglement theory lies the notion of LOCC. To see why, imagine two parties that are a large distance apart from each other, say, Alice is in Berlin and Bob in New York. While they may obtain access to shared entanglement from a third party, it is unreasonable to assume that they are able to perform global operations on the state they share. On the other hand, it is perfectly conceivable that they transmit classical messages, for example, to communicate measurement results.

The goal of this problem is to show that if Alice and Bob are in far away labs, and share a state, any measurement on Alice's part of the state can be simulated as follows: Bob performs a measurement on his side and communicates the result to Alice, who performs a local unitary tranformation. This can be proven for POVMs, but for simplicity we will restrict ourselves to projective measurements.

Consider a bipartite state $|\psi\rangle_{AB}$ with Schmidt decomposition $|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\,|a_i\rangle\,|b_i\rangle$and a projective measurement $\Pi = \{\Pi_i^A\}_i$ acting on Alice's Hilbert space.

a) Expand Π_i^A in the Schmidt basis and define a projective measurement $\Gamma = \{\Gamma_i^B\}_i$ on Bob's system such that the probability p_k^B that Bob observes result k when measuring Γ is the same as the probability p_k^A that Alice observes result k when measuring Π.

b) Determine the post measurement states $\left|\phi_j^A\right\rangle$ after Alice measures Π and obtains result j, and $\left|\phi_j^B\right\rangle$ after Bob measures Γ and obtains result j. (both of these states are defined on the whole Hilbert space AB, the superscripts serve to identify who performed the measurement).

c) Show that $\left|\phi_j^A\right\rangle$ and $\left|\phi_j^B\right\rangle$ are equivalent up to local unitary transformations.

d) Describe the LOCC protocol.