Freie Universität Berlin

Tutorials on Quantum Information Theory

Winter term 2020/21

Problem Sheet 7
Quantum Shannon Theory and Key Distribution

J. Eisert, J. Haferkamp, J. C. Magdalena De La Fuente

---

1. **On Shannon entropy...**

   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.

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

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

   $$(3)\, I(X:Y) = H(Y) - H(Y|X) \text{ (Mutual information)} \tag{3}$$

   a) Show that $0 \leq H(X) \leq \log|\mathcal{X}|$, 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 $H(X,Y) \leq H(X)+H(Y)$.

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

   c) Show that $H(Y|X) \geq 0$ and hence $I(X:Y) \leq H(Y)$ with equality if and only if Y is a (deterministic) function of X.

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

   d) Show that $H(Y|X) \leq H(Y)$ and hence that $I(X:Y) \geq 0$ with equality if and only if X and Y are independent random variables.

2. **... and the von-Neumann entropy**

   For any state $\rho \in \mathcal{D}(\mathcal{H})$ with $\dim\mathcal{H} = d$ the von-Neumann entropy is defined as $S(\rho) = -\operatorname{Tr}(\rho\log\rho)$.

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

   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 $S(A,B) \leq S(A) + S(B)$.

   Hint: You may use the inequality $S(\rho) \leq -\operatorname{Tr}[\rho\log\sigma]$ *for an arbitrary quantum state* σ.

   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.

3. **Classical capacities of quantum channels**

Although this exercise might look very long, it isn't. In the next paragraphs we just want to give you an overview on the formalism introduced in the lecture and needed for this exercise in a compressed fashion. No need to be intimidated ;)

In the lecture, we saw two alternative characterisations of the classical channel capacity of a quantum channel $\mathcal{E}$, which is given by the its Holevo-information $\chi(\mathcal{E})$. The task here is to establish the equivalence of these expressions.

To this end, recall the definition of the quantum mutual information of a bi-partite quantum system in a state ρ_{AB}

$$I(A:B)_{\rho_{AB}} \coloneqq S(\rho_A) + S(\rho_B) - S(\rho_{AB}). \tag{4}$$

The Holevo information of channel can be defined using the following scheme: Alices encodes the information of a classical random variable X taking values in $\mathcal{X}$ with probability distribution p_X into a quantum state using a set of states $\{\rho_x\}_{x\in\mathcal{X}}$. To keep track of the classical random variable but formulating everything quantum mechanically, we think of Alice encoding the result in another faithfully register N using orthogonal basis $\{|x\rangle\}_{x\in\mathcal{X}}$. From this notebook register N the classical information of X can be completely recovered. Altogether, Alice prepares the bi-partite state

$$\rho_{NA} = \sum_x p_X(x)\, |x\rangle\langle x|_N \otimes \rho_A^x. \tag{5}$$

Then, the state in system A is sent to Bob using the channel $\mathcal{E}$. Thus, we end up with a final state shared between Alice's notebook and Bob

$$\rho_{NB} = \sum_x p_X(x)\, |x\rangle\langle x|_N \otimes \mathcal{E}(\rho_A^x)_B. \tag{6}$$

We can now ask for the mutual information between the variable X encoded in N and Bob's output of the channel. Analogously to the classical result, maximizing the mutual information over all possible input variables X and encodings yields the capacity of the quantum channel to transmit classical informations, i.e.

$$\chi(\mathcal{E}) = \max_{(X,p_X,\{\rho^x\})} I(N,B)_{\rho_{NA}}. \tag{7}$$

a) Show that

$$\chi(\mathcal{E}) = \max_{(X,p_X,\{\rho^x\})} \left\{ S(\mathcal{E}(\sum_x p_X(x)\rho^x)) - \sum_x p_X(x) S(\mathcal{E}(\rho^x)) \right\}. \tag{8}$$

Remember that Shannon's noisy channel coding theorem states that the capacity of a noisy channel T is given by the maximum over all inputs of the mutual information:

$$C(T) = \max_{X,p_X} I(X:Y),$$

where Y is the random variable describing the output of the channel T with input X.

b) Determine the channel capacity of the binary symmetric channel defined by

$$\Pr(0|0) = \Pr(1|1) = 1 - p$$
$$\Pr(1|0) = \Pr(0|1) = p.$$

Hint: It may be useful to expand $H(Y|X)$ *as* $\sum_x p(x)H(Y|X = x)$.

We now want to determine the channel capacity of the binary erasure channel as defined by

$$\Pr(0|0) = \Pr(1|1) = 1 - p$$
$$\Pr(e|0) = \Pr(e|1) = p.$$

c) First, use the expansion $H(Y) = H(Y, Z) = H(E)+H(Y|Z)$ to show that $H(Y) = H(p)+(1-p)H(\pi)$. Here, we let Z be the random variable distinguishing between the event $E = \{Y = e\}$ and $\neg E = \{Y \neq e\}$. We have that $\Pr(Z = E) = p$. Furthermore we call the propability defining the distribution of the input variable $\pi = \Pr(X = 1)$.

Hint: Use Eq. (2) *and* $\Pr(Y = y|Y \neq e) = \Pr(X = y)$.

d) Use this result and proceed analogously to the binary symmetric channel to determine the channel capacity of the erasure channel.

4. **Detecting Eve.** One key feature of the BB'84 protocol for quantum key distribution is that Alice and Bob are able to estimate how many bits were corrupted by the channel or Eve by comparing their results on a subset.

In this excercise, we will prove this statement. More precisely, let Alice and Bob randomly select n of their $2n$ bits check for errors. We denote the number of errors in the test bits by e_T and the number of errors in the remaining, untested n bits by e_R. Then, for any $\delta > 0$

$$p \coloneqq \Pr\{e_T \leq \delta n \ \wedge \ e_R \geq (\delta + \epsilon)\} \leq \exp\left[-\mathcal{O}(n\epsilon^2)\right]. \tag{9}$$

In other words, the probability that the number of errors in the unknown bits deviatiates by more than ϵ from the observed fraction δ in the test bits gets very small large n and ϵ.

We denote the total number of errors that occur in the $2n$ bits by μn.

a) Argue that

$$p \leq \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n. \tag{10}$$

We will need a few identities to massage this term. To this end, let $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ be the binary entropy.

b) Show that

$$nH(p) + \mathcal{O}(\log_2 n) \leq \log_2 \binom{n}{pn} \leq nH(p) + \mathcal{O}(\log_2 n). \tag{11}$$

Hint: Recall Stirling's bound $\sqrt{2\pi}\sqrt{n}\, n^n \mathrm{e}^{-n} \leq n! \leq \mathrm{e}\sqrt{n}\, n^n \mathrm{e}^{-n}$.

Furthermore, one can derive the following simple bound for the binary entropy $H(x) \leq 1 - 2\left(x - \frac{1}{2}\right)^2$. (If you are curious, it is a good excercise to use Taylor's theorem including an estimate for the remainder to derive this bound.)

c) Plug everything together and show that $p \leq \exp\left[-\mathcal{O}(n\epsilon^2)\right]$.