Freie Universität Berlin
Tutorials on Quantum Information Theory
Summer Term 2018

Problem Sheet 8
Quantum Shannon Theory and Quantum Key Distribution

Discussed in Tutorial: 21/06/2018 J. Eisert, D. Hangleiter, I. Roth

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_i are probabilities and the eigenspaces of the states ρ_i are orthogonal. Show that

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

and use this result to infer that

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

where $\langle i \mid j\rangle = \delta_{ij}$ 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 and quantum channels.**

In this problem we will take a closer look at some aspects of classical and quantum channels. We saw two alternative characterisations of the classical channel capacity $C^{(1)}(\mathcal{E})$ of a quantum channel $\mathcal{E}$ with product inputs as given by Holevo information $\chi(\mathcal{E})$. The Holevo information is defined as

$$\chi(\mathcal{E}) = \max_{X,\rho_x} I(X:B) \tag{4}$$

$$= \max_{X,\rho_x} \left(S(\mathcal{E}(\rho)) - \sum_x p_x S(\mathcal{E}(\rho_x)) \right), \tag{5}$$

where we assumed that the quantum state shared by Alice and Bob after the protocol is given by $\rho^{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{E}(\rho_x)$ and X denotes the random variable of Alice's source.

a) Show the equality between Eqs. (4) and (5).

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 we let $Y = T(X)$ be the random variable obtained from applying the channel T to 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 $H(Y) = H(Y,E) = H(E) + H(Y|E)$ to show that $H(Y) = H(p) + (1-p)H(\pi)$. Here, we let E be the event $\{Y = e\}$ that obtains with probability p and we call $\pi = \Pr(X = 1)$.

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 $\delta > 0$

$$p \coloneqq \Pr\{e_T \leq \delta n \ \wedge \ e_R \geq (\delta + \epsilon)\} \leq \exp\left[-\mathcal{O}(n\epsilon^2)\right]. \tag{6}$$

   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

$$p \leq \binom{2n}{n}^{-1} \binom{\mu n}{\delta n} \binom{(2-\mu)n}{(1-\delta)n} \delta n. \tag{7}$$

   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

$$nH(p) + \mathcal{O}(\log_2 n) \leq \log_2 \binom{n}{pn} \leq nH(p) + \mathcal{O}(\log_2 n). \tag{8}$$

   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 $p \leq \exp\left[-\mathcal{O}(n\epsilon^2)\right]$.