IDEA League School - Quantum Information - Aachen 2015
Randomness, Entropy and QKD
(15 points)

February 27, 2015

1. (Distinguishing quantum states) (2 points) Suppose I choose one of the states $\rho_0 = |0\rangle\langle 0|$ or $\rho_1 = |+\rangle\langle +|$ with probabilities $p_0 = p_1 = 1/2$, and send that state to you. Describe a procedure (measurement) that you can use to find out which state I have sent, that is, a procedure to distingiush the two states. What is the probability that your procedure succeeds? Can you show that your procedure is optimal?

2. (Distingiushing classical states) (2 points) Imagine we roll a die with 6 possible outcomes $\{1, 2, 3, 4, 5, 6\}$ Let's play the following game. I have two dice in my possession with possible symbols $\mathcal{R} = \{1, 2, 3, 4, 5, 6\}$. Die 0 is a fair die, i.e., the probability distribution over the possible outcomes $\{1, 2, 3, 4, 5, 6\}$ is uniform $P_X = (1/6, 1/6, 1/6, 1/6, 1/6, 1/6)$. Die 1 however is not quite fair and favors the outcome 6 with probability distribution $P_Y = (1/7, 1/7, 1/7, 1/7, 1/7, 2/7)$. With probability 1/2 I will roll die 0 and with probability 1/2 I will roll die 1. You cannot see which die I used, but I tell you the outcome of my die roll. Can you guess whether I used die 0 or die 1? Explain how this process is related to distinguishing quantum states above.

3. (Min-entropy)

   (a) (1 point) Compute the min-entropy $H_{\min}(X)$ of the classical distribution $P_X = (1/3, 2/3)$.

   (b) (2 points) Compute the min-entropy $H_{\min}(X|E)$ of the cq-state

   $$\rho_{XE} = \frac{1}{2} \sum_{x \in \{0,1\}} |x\rangle\langle x| \otimes \rho_E^x \,, \tag{1}$$

   where $\rho_E^0 = |0\rangle\langle 0|$ and $\rho_E^1 = |+\rangle\langle +|$.

4. (Key exchange) As usual, Alice and Bob are in dire need for a key to encrypt their personal communication. Luckily for them, they have discovered an anonymous message board in the hallway. It allows both Alice and Bob to post messages in such a way that noone can ever find out who the message came from. In particular, any eavesdropper Eve cannot learn whether the message came from Alice or from Bob. The message board simply creates a list of messages posted to it, without indicating a sender.

(a) (6 points) Can you think of a way that Alice and Bob can use the anonymous message board to exchange a key? I.e., at the end of the day, we want that Alice and Bob both share an n-bit key, but Eve is ignorant about the key. Show that your protocol is secure.

(b) (2 points) Suppose now that for any message posted to the board, Eve can actually find out who the sender was. However, as Eve is slowly growing old and tired of intercepting messages, her memory has become very bad. In particular, she can only remember 512 bits of information. Can you think of a way that Alice and Bob can still use the message board to generate a key?

5. (Leftover hash lemma) In this exercise, you'll investigate the proof of the so-called leftover hash lemma for a set of 2-universal hash functions in the purely classical case (classical side information). Note that any classical distribution P_X can be written as a diagonal state

$$\vec{\rho}_X = \sum_x P_X(x)|x\rangle\langle x| \ , \tag{2}$$

where we will use $\vec{\rho}$ to remind ourselves that this is just a classical distribution. In short, we will be proving that for a 2-universal set of hash functions $\mathcal{F} = \{r : \{0,1\}^n \to \{0,1\}^m\}$ with $m = k - 2\log(1/\varepsilon)$ the function given by $Ext(X, r) := r(X)$ is a (k, ε)-randomness extractor. That is, given k bits of min-entropy, the output satisfies

$$D(\rho_{\mathrm{Ext}(X,R),XRE}, \frac{\mathbb{I}}{2^m} \otimes \rho_{RE}) \leq \epsilon \ . \tag{3}$$

For simplicity, we will first consider the unconditional case, ie $H_{\min}(X) \geq k$ without any side information E.

(a) (Bonus) Write down what exactly we want to show, that is, how we can tell that the function forms a (k, ε)-randomness extractor. Since we are in the fully classical case, the trace distance is simply the statistical distance between two probability distributions. The statistical distance btween probability distributions P_X and P_Y is given by

$$D(P_X, P_Y) = \frac{1}{2}\sum_x |P_X(x) - P_Y(x)| \ . \tag{4}$$

(b) (Bonus) We will now proceed in three steps. First of all, let us show a useful aspect of the distribution $\vec{\rho}_{RExt(X,R)}$ for a uniform seed R chosen from $\mathcal{F}$. Let's suppose that we choose a seed R and string X, given a distribution $\vec{\rho}_{RX}$. We now apply Ext to X, yielding a distribution $\vec{\rho}_{RExt(X,R)}$. Let's suppose that we do this again, independently and according to the same distribution giving us a second seed R' and string X'. Let $\vec{\rho}_{R'Ext(X',R')}$ denote the second distribution.
We can now consider the probability of a collision, i.e., the probability that $(R, Ext(X, R)) = (R', Ext(X', R'))$. Show that

$$\Pr[(R, Ext(X, R)) = (R', Ext(X', R'))] \leq \frac{1 + \varepsilon^2}{|\mathcal{F}|2^m} \ . \tag{5}$$

(c) (Bonus) There are many ways to measures distances between distributions, and next to the statistical distance (or L1 distance) the so-called L2-distance often forms a very convenient tool in proofs. For two distributions P_Y and P_Z over some set $\mathcal{S}$ it is defined as

$$L2(\vec{\rho}_Y, \vec{\rho}_Z) = \frac{1}{2}\sqrt{\sum_{s\in\mathcal{S}}(P_Y(s) - P_Z(s))^2} \ . \tag{6}$$

The L2-distance is closely related to the statistical distance by $D(\vec{\rho}_Y, \vec{\rho}_Z) \leq \sqrt{|\mathcal{S}|}L2(\vec{\rho}_Y, \vec{\rho}_Z)$. Show that

$$L2(\vec{\rho}_{REext(X,R)}, \frac{\mathbb{I}}{|\mathcal{F}|} \otimes \frac{\mathbb{I}}{2^m}) \leq \frac{1}{2}\sqrt{\frac{\varepsilon^2}{|\mathcal{F}|2^m}} \ . \tag{7}$$

(d) (Bonus) Show that $D(\vec{\rho}_{REext(X,R)}, \frac{\mathbb{I}}{|\mathcal{F}|} \otimes \frac{\mathbb{I}}{2^m}) \leq \varepsilon$.