CS120, Quantum Cryptography, Fall 2016

Homework # 6 **due: 10:29AM, November 15th, 2016**

Ground rules:

Your homework should be submitted to the marked bins that will be by Annenberg 241.

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are strongly encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Some of the problems are inspired from problems available on EdX. You are not allowed to look up the EdX problems for hints (such as the multiple answers provided). Focus on the present pset!

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the quarter will be dropped from your final grade.

Place all your problems in the first (top) bin in the box by Annenberg 241. Start each problem on a new page, with your name clearly marked at the top of the page.

Problems:

1. *(4 points)* **The Pretty-Good-Measurement is not Optimal.**

   The pretty-good-measurement is useful when we have an ensemble that we don't understand very well and we need to distinguish the states in the ensemble with some success probability.

   (a) Suppose Alice sends Bob one of the three states $\rho_0 = |0\rangle\langle 0|, \rho_1 = \frac{1}{2}\mathbb{I}, \rho_2 = |1\rangle\langle 1|$ with equal probability. Bob wants to figure out which state Alice sent. Compute the success probability achieved by Bob if he uses the pretty-good-measurement.

   (b) In Homework 5, problem 1(h), you showed the following formulation of the guessing probability:

   $$P_{\text{guess}}(X \mid E) = \inf_{\sigma : p_i \rho_i \leq \sigma \, \forall i} \operatorname{Tr} \sigma, \tag{1}$$

   where each ρ_i is a density matrix which appears with a priori probability p_i in the ensemble. Use this formulation to give an upper bound on the guessing probability for the ensemble from (a). Make the upper bound as tight as you can.

(c) Notice that there is a gap between the success probability calculated in parts (a) and (b). Find a measurement whose success probability matches the bound from part (b).

2. *(3 points)* **Properties of the Pretty-Good-Measurement.**
This problem is adapted from a StackExchange answer by Norbert Schuch.[1] That post is not an allowed resource for this problem. When we make a pretty-good measurement to distinguish the ensemble $\rho = \sum_i p_i \rho_i$, we associate to each ρ_i a measurement operator $M_i = \rho^{-\frac{1}{2}} p_i \rho_i \rho^{-\frac{1}{2}}$. We think of M_i as being "well-fitted" to the state ρ_i, in the sense that when we measure Π_i, we conclude that ρ_i is the most likely state. This may lead us to believe that ρ_i is "well-fitted" to M_i in the sense that it is the state for which the measurement is most likely to result in Π_i. In other words, we may like to believe the following inequality:

$$\mathrm{Tr}(M_i \rho_i) \geq \mathrm{Tr}(M_i \rho_k), \tag{2}$$

for any i and k.

(a) Prove inequality 2 for the case where the ensemble has only two states.

(b) Let $\rho_0 = \frac{1}{3}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \rho_1 = \frac{1}{3}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, and $\rho_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Consider the ensemble $\rho = \frac{2}{5}\rho_0 + \frac{2}{5}\rho_1 + \frac{1}{5}\rho_2$. Show that inequality 2 is not satisfied.

3. *(6 points)* **Deterministic Extractors on Bit-Fixing Sources.**
We saw in the edX lecture notes that no deterministic function can serve as an extractor for all random sources of a given length. However, this doesn't rule out the possibility that a deterministic extractor can work for some restricted class of sources.

(a) Fix an even integer n and integer $t < n$. Consider the following sources.

- X_0 is all 1s on the first t bits and uniformly random on the last $n - t$ bits.
- X_1 is uniformly random over the set of strings with an even number of 0s.
- X_2 is uniformly random over the set of strings where the first $\frac{n}{2}$ bits are the same as the last $\frac{n}{2}$ bits.

Compute the min-entropy $H_{\min}(X_i)$ for each $i \in \{0, 1, 2\}$.

(b) Consider the following deterministic functions:

- $f_0(x) := \bigoplus_{i=1}^{t} x_i$, the XOR of the first t bits of x.
- $f_1(x) := x_L \cdot x_R = \bigoplus_{i=1}^{n/2} x_i x_{i+\frac{n}{2}}$, where $x = (x_L, x_R)$ are the left and right halves of x.
- $f_2(x) := \bigoplus_{i=1}^{n} x_i$ the XOR of all of the bits of x.

For which pairs (i, j) is $f_i(X_j)$ distributed as a uniformly random bit?

[1] `physics.stackexchange.com/questions/245274/probability-distribution-of-a-pretty-good-measurement`

(c) Alice and Bob share a classical secret $X \in \{0,1\}^n$ generated uniformly at random. Alice and Bob make an error in their secure communication protocol and as a result, Eve learns t bits of X. Give, with proof, a deterministic function f such that $f(X)$ is uniformly random over strings of length $\left\lfloor \frac{n}{t+1} \right\rfloor$ and $f(X)$ is independent of Eve.

4. *(6 points)* **No Chain Rule for Conditional Min-Entropy.**
Recall the definition of conditional Shannon entropy.

$$H(Y \mid X) = \sum_x \Pr[X = x] H(Y \mid X = x) \tag{3}$$

(a) Prove that conditional Shannon entropy satisfies the *chain rule*:

$$H(Y \mid X) = H(XY) - H(X). \tag{4}$$

(b) Prove that the conditional min-entropy satisfies the chain rule on X and Y if X and Y are independent.

(c) For each of the following two distributions, compute $H_{\min}(X_i Y_i)$, $H_{\min}(X_i)$, and $H_{\min}(Y_i \mid X_i)$. Make a conclusion about the form of the general chain rule for conditional min-entropy.

$$p(X_1Y_1 = 00) = \frac{1}{2}, p(X_1Y_1 = 01) = \frac{1}{8}, p(X_1Y_1 = 10) = \frac{1}{4}, p(X_1Y_1 = 11) = \frac{1}{8}.$$

$$p(X_2Y_2 = 00) = \frac{3}{8}, p(X_2Y_2 = 01) = \frac{1}{4}, p(X_2Y_2 = 10) = \frac{5}{16}, p(X_2Y_2 = 11) = \frac{1}{16}.$$

5. *(3 points)* **Optimal qubit strategies in the CHSH game.**
Questions (a), (b) and (d) of this problem are worth one point each. The others are worth zero points and are optional. You should still read the problem to its end, as the conclusion is used in the following problem.
The goal of this problem is to evaluate the maximum success probability that can be achieved in the CHSH game by players sharing a two-qubit entangled state of the form

$$|\psi_\theta\rangle_{AB} = \cos(\theta) |0\rangle_A |0\rangle_A + \sin(\theta) |1\rangle_A |1\rangle_B , \tag{5}$$

where $\theta \in [0, \pi/4]$ (other values of θ can be reduced to this case by simple change of basis or phase flip). Having fixed the state, what are the optimal measurements for the players, and what is their success probability?

We will assume each player makes makes a basis measurement on their qubit. Recall that an observable O is a 2×2 matrix with complex entries such that O is Hermitian ($O^\dagger = O$) and squares to identity ($O^2 = \mathbb{I}$). For any single-qubit basis measurement $\{|u_0\rangle, |u_1\rangle\}$, there is an associated observable $O = |u_0\rangle\langle u_0| - |u_1\rangle\langle u_1|$. Conversely, any observable that is not $\pm\mathbb{I}$ has two non-degenerate eigenvalues $+1$ and -1, so we can uniquely identify it with a basis.

To reduce the number of cases to consider we first make a few symmetry observations.

(a) Let O be a single-qubit observable such that O is non-degenerate ($O \neq \pm\mathbb{I}$). Show that there exists real numbers α, β, γ such that $\alpha^2 + \beta^2 + \gamma^2 = 1$ and $O = \alpha X + \beta Y + \gamma Z$, with X, Y, Z the standard Pauli matrices.

(b) Let $\mathcal{B} = A_0 \otimes B_0 + A_1 \otimes B_0 + A_0 \otimes B_1 - A_1 \otimes B_1$. Show that the success probability of the strategy in the CHSH game is $p_s = \frac{1}{2} + \frac{1}{4} \langle\psi_\theta| \mathcal{B} |\psi_\theta\rangle$.

(c) Argue that for the purposes of computing the maximum success probability in the CHSH game of players using state $|\psi_\theta\rangle_{AB}$ as in (5) we may without loss of generality restrict our attention to observables of the form $A_x = \cos(\alpha_x)X + \sin(\alpha_x)Y$ and $B_y = \cos(\beta_y)X + \sin(\beta_y)Y$ for some angles $\alpha_x, \beta_y \in [0, 2\pi)$. *[Hint: do a rotation on the Bloch sphere.]*

Based on the symmetry argument from the previous questions we have reduced our problem to understanding the maximum value that $\langle\psi_\theta| \mathcal{B} |\psi_\theta\rangle$ can take, when $|\psi_\theta\rangle$ is as in (5) and $\mathcal{B}$ is defined from observables A_x, B_y as in (b). To understand this maximum value we compute the spectral decomposition of $\mathcal{B}$.

(d) Show that $(Z \otimes \mathbb{I})\mathcal{B}(Z \otimes \mathbb{I}) = (\mathbb{I} \otimes Z)\mathcal{B}(\mathbb{I} \otimes Z) = -\mathcal{B}$. *[Hint: use the special form of A_x and B_y you obtained from question (c).]*

(e) Show that $\mathcal{B}$ has a basis of eigenvectors of the form $|\phi_{ab}\rangle = e^{i\theta_{ab}} |ab\rangle + |\overline{a}\overline{b}\rangle$, where $a, b \in \{0, 1\}$ and $\overline{a} = 1 - a$, $\overline{b} = 1 - b$. Note that up to local rotations this is the Bell basis.

(f) Write $\mathcal{B}^2$ as a 4×4 matrix depending on the angles α_x, β_y, and show that $\mathrm{Tr}(\mathcal{B}^2) \leq 16$.

(g) Show that the largest success probability achievable in the CHSH game using $|\psi_\theta\rangle_{AB}$ is at most $\frac{1}{2} + \frac{1}{4}\sqrt{1 + \sin^2(2\theta)}$. *[Hint: Decompose $|\psi_\theta\rangle$ in the eigenbasis of $\mathcal{B}$. Use (f) and the symmetries from (d) to bound the bound the success probability via the expression found in (b).]*

(h) Give a strategy for the players which achieves this value, i.e. specify the players' observables.

6. *(8 points)* **Trading success probability for randomness in the CHSH game.** The goal of this problem is to show that, if players succeed with higher and higher probability in the CHSH game then Alice's outputs in the game must contain more and more randomness.

(a) Suppose that Alice and Bob play the CHSH game using a two-qubit entangled state $|\psi_\theta\rangle_{AB}$ as in (5). Let $p_\theta(a|x)$ be the probability that, in this strategy, Alice returns answer $a \in \{0, 1\}$ to question $x \in \{0, 1\}$. Show that $\max_{a,x} p_\theta(a|x) \leq \cos^2(\theta)$.

(b) Let $p_s = \frac{1}{2} + \frac{1}{8} I$ be the players' success probability in CHSH, where $I \in [-4, 4]$ ($I = 2\sqrt{2}$ for the optimal quantum strategy). Using (g) from the previous problem,

deduce from (a) that

$$\forall a, x \in \{0,1\}, \qquad p_\theta(a|x) \leq \frac{1}{2}\Big(1 + \sqrt{2 - \frac{I^2}{4}}\Big).$$

(c) Suppose now the players use any single-qubit strategy (not necessarily using $|\psi_\theta\rangle$). Prove a lower bound on the conditional min-entropy $H_{\min}(A|X = x)$, for any $x \in \{0,1\}$, that is generated in Alice's outputs, as a function of the players' success probability in the CHSH game.

(d) Show that the bound from (b) is tight: for any $\theta \in [0, \pi/4]$ find a strategy for the players using $|\psi_\theta\rangle$ such that $\max_{a,x} p_\theta(a|x) = \frac{1}{2}(1 + \sqrt{2 - I^2/4})$.