CS120, Quantum Cryptography, Fall 2016

Homework # 5 **due: 10:29AM, November 8th, 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. (8 points) *A dual formulation for the conditional min-entropy.*
   In the notes the conditional min-entropy of a cq state $\rho_{XE} = \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_x^E$ (where $\mathcal{X}$ is any finite set of outcomes) is defined through the guessing probability, $H_{\min}(X|E) = -\log P_{\text{guess}}(X|E)$ where

   $$P_{\text{guess}}(X|E) = \sup_{\{M_x\}} \sum_{x\in\mathcal{X}} \operatorname{Tr}\left(M_x \rho_x\right), \tag{1}$$

   where the supremum is over all POVM $\{M_x\}$.

   It turns out that the min-entropy can also be written in a different way, and this other expression can be useful in calculations. To derive it, we first rewrite (1) as a semidefinite program (SDP). Recall the primal and dual forms of an SDP from Problem 2 in Homework 3. Consider the map

   $$\Phi(Z) = \sum_{x\in\mathcal{X}} \left(\langle x| \otimes \mathbb{I}_E\right) Z \left(|x\rangle \otimes \mathbb{I}_E\right),$$

where Z is any matrix over the space $\mathcal{H}_X \otimes \mathcal{H}_E$ associated to registers X and E.

(a) Suppose $\{N_x\}$ is a valid POVM. Show that the matrix $Z = \sum_x |x\rangle\langle x| \otimes N_x$ satisfies $Z \geq 0$, and compute $\Phi(Z)$ (the result should be a matrix defined on system E only).

(b) For the same matrix Z as in the previous question, compute $\mathrm{Tr}(Z\rho_{XE})$.

(c) Conversely, suppose $Z \geq 0$ and $\Phi(Z) = \mathbb{I}_E$. Show that the elements $N_x = (\langle x| \otimes \mathbb{I}_E) Z (|x\rangle \otimes \mathbb{I}_E)$ form a valid POVM $\{N_x\}$ over $\mathcal{H}_E$ (with outcomes $x \in \mathcal{X}$).

(d) Use the previous questions to give a semidefinite program in primal form whose optimum is $P_{\mathrm{guess}}(X|E)$. That is, specify the map Φ and matrices A and B that define the SDP.

(e) Show that the map Φ^* associated to Φ is such that $\Phi^*(Y) = \mathbb{I}_X \otimes Y$, for any matrix Y defined over system E (remember the definition of Φ^* from Φ given in Homework 3, Problem 1).

(f) Write the dual program to your SDP explicitly.

(g) Conclude that the guessing probability satisfies

$$P_{\mathrm{guess}}(X|E) = \inf_{\sigma} \mathrm{Tr}(\sigma),$$

where the infimum is taken over all matrices σ defined on system E such that $\sigma \geq \rho_x$ for all $x \in \mathcal{X}$.

In the final two parts of this problem we use the previous parts (whose results you may use even if you didn't prove them) to compute the min-entropy of cq states given as the tensor product of many copies of the same state.

(h) Show that for any σ such that $\sigma \geq \rho_x$ we have $P_{\mathrm{guess}}(X|E) \leq \mathrm{Tr}(\sigma)$. *[Hint: remember Exercise 2 from Homework 3...]*

(i) Suppose that $\rho_{XE} = \tau_{X_1E_1}^{\otimes n}$, where $\tau_{X_1E_1}$ is a cq-state. That is, ρ_{XE} is formed of n identical copies of the same state. Show that $H_{\min}(X|E)_\rho = nH_{\min}(X_1|E_1)_\tau$, where we have used the subscripts ρ and τ to remind ourselves of which states we compute the min-entropy. *[Hint: consider the solutions for the primal and dual SDP from the previous problem for a single instance $\sigma_{X_1E_1}$. Use these solutions to construct matching solutions for the primal and dual SDP associated to the cq state ρ.]*

2. (8 points) *Computing the min-entropy.*
How much can a quantum register E help us guess X? In the following, you will show that $H_{\min}(X|E) \geq H_{\min}(X) - \log|E|$, where E denotes the dimension of the associated Hilbert space (so $\log|E|$ is just the number of qubits of E).

(a) Write out what we want to show in terms of the guessing probability $P_{\mathrm{guess}}(X|E)$ using the definition of the min-entropy.

(b) It will be useful to establish the following fact. Suppose given two Hermitian matrices A and B, which are positive semidefinite: $A \geq 0$ and $B \geq 0$. Show that $\mathrm{Tr}(AB) \leq \lambda_{\max}(B)\,\mathrm{Tr}(A)$, where $\lambda_{\max}(B)$ is the largest eigenvalue of B.

(c) Use this fact to show that for any POVM $\{M_x\}$ and any quantum state ρ_x^E we have $\mathrm{Tr}(M_x\rho_x^E) \leq \mathrm{Tr}(M_x)$.

(d) Using this trick together with what you know about POVMs, show that $H_{\min}(X|E) \geq H_{\min}(X) - \log|E|$.

3. (8 points) *Bounding the winning probability in the CHSH game.*
The goal of this problem is to demonstrate that no quantum strategy, however large a quantum state it uses, can succeed with probability larger than $\cos^2(\pi/8) \approx 0.85$ in the CHSH game. The first step consists in having an accurate model for what a "quantum strategy" is. The players, Alice and Bob, should be allowed to use an arbitrary bipartite state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are abbitrary vector spaces (of finite dimension). Next, upon reception of a question $a \in \{0,1\}$, Alice can make an arbitrary measurement (POVM) $\{A_x^0, A_x^1\}$ on her system, and similarly for Bob with $\{B_y^0, B_y^1\}$. It is important to convince yourselves that any kind of strategy can be implemented in this way, including making repeated measurements in sequence, unitaries, etc. Indeed, ultimately a "strategy" receives as input a question, makes some sequence of quantum operations, and returns an answer: it is in any case something that can be modeled via a POVM. So for the remainder of the problem, let us fix an arbitrary entangled state $|\psi\rangle_{AB}$ and POVM $\{A_x^a\}_{a\in\{0,1\}}$ and $\{B_y^b\}_{b\in\{0,1\}}$ on that state. For convenience we also define $A_x = A_x^0 - A_x^1$ and $B_x = B_x^0 - B_x^1$.

(a) Show that if $\{A_x^0, A_x^1\}$ is a valid POVM then $\|A_x\| \leq 1$ (where as usual $\|\cdot\|$ is the operator norm, the largest singular value). Similarly for B_y.

(b) For $x \in \{0,1\}$ define $|u_x\rangle = A_x \otimes \mathbb{I}_B\,|\psi\rangle_{AB}$, and for $y \in \{0,1\}$ define $|v_y\rangle = \mathbb{I}_A \otimes B_y\,|\psi\rangle_{AB}$. Give a bound on the Euclidean norms $\||u_x\rangle\|$, $\||v_y\rangle\|$.

(c) Show that the success probability of the quantum strategy in the CHSH game can be expressed as

$$p_{\mathrm{succ}} = \frac{1}{2} + \frac{1}{8}\big(\langle u_0|\,v_0\rangle + \langle u_1|\,v_0\rangle + \langle u_0|\,v_1\rangle - \langle u_1|\,v_1\rangle\big).$$

(d) Show that for any vectors $|r_0\rangle, |r_1\rangle, |s_0\rangle, |s_1\rangle$, the inequality

$$\big|\langle r_0|\,s_0\rangle + \langle r_1|\,s_0\rangle + \langle r_0|\,s_1\rangle - \langle r_1|\,s_1\rangle\big| \leq 2\sqrt{2}\max\big\{\||r_0\rangle\|, \||r_1\rangle\|, \||s_0\rangle\|, \||s_1\rangle\|\big\}$$

holds.

(e) Conclude that $p_{\mathrm{succ}} \leq \cos^2(\pi/8)$.

4. (4 points) **A Guessing Game**
Imagine Alice and Eve play a guessing game where they share some state ρ_{AE} and

Alice produces a random bit θ, measures her qubit in the standard basis if $\theta = 0$ and measures in the Hadamard basis if $\theta = 1$. In both cases she obtains a bit x as measurement outcome. She then announces θ to Eve. Eve's goal is then to guess the bit x. Now imagine $\rho_{AE} = |\Phi\rangle\langle\Phi|$, where $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, so Alice and Eve share a maximally entangled pair of qubits. In this scenario you know that, if Eve measures in the same basis as Alice, she will get the same outcome and this thus able to guess x perfectly in this situation.

(a) However, Alice wants to foil Eve so, before measuring, she first applies some unitary U to her qubit, and then measures. Of course Eve, being really smart, gets wind of this so she will know what unitary Alice has used before measuring. So they share the state

$$|\Phi_U\rangle = (U_A \otimes \mathbf{1}_E)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and Eve knows θ and U. What would now be Eve's best guessing probability? (Tip: Eve has a quantum computer!)

(b) Consider now a scenario in which Eve doesn't know the local unitary that Alice applies. Suppose that Alice can choose her unitary from a set of three unitaries (and assume that she always applies one unitary from this set before measuring). You should assume that, once Alice decides on a (probabilistic) strategy, this is known to Eve. Provide a strategy for Alice (including the set of three unitaries) that makes Eve's guessing probability the lowest possible.

(c) Suppose we restrict Alice's set of possible unitaries to contain only two. Can she still make Eve's guessing probability as low as in part (b)?

5. (4 points) **Decoherence**
A quantum state can naturally be exposed to a phenomenon called *decoherence*, due to its interaction with the surrounding environment. Suppose the state of a qubit and the surrounding environment is initially $|\Psi\rangle\,|E\rangle$, where $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, and $|E\rangle$ is the initial state of the environment. Suppose that this state undergoes "decoherence", as described by the CPTP map

$$|0\rangle\,|E\rangle \mapsto |0\rangle\,|E_0\rangle\,,$$
$$|1\rangle\,|E\rangle \mapsto |1\rangle\,|E_1\rangle\,,$$

where the states $|E\rangle$, $|E_0\rangle$ and $|E_1\rangle$ are normalized but not necessarily orthogonal. Show that the density matrix of the qubit evolves as

$$|\Psi\rangle\langle\Psi| \mapsto (1-p)\,|\Psi\rangle\langle\Psi| + pZ\,|\Psi\rangle\langle\Psi|\,Z.$$

Assuming $\langle E_0|E_1\rangle$ is real, express p in terms of $\langle E_0|E_1\rangle$, . This means that with the probability $1-p$ the qubit is not affected by the environment and with probability p the qubit undergoes a phase-flip error.