CS120, Quantum Cryptography, Fall 2016

Homework # 3 **due: 10:29AM, October 25th, 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.

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. (6 points) **Superdense Coding.**
In Homework 1, you were introduced to the idea of "quantum teleportation". By sending just two bits of classical information, Alice was able to "teleport" her single-qubit quantum state to Bob, provided they shared a pair of maximally entangled qubits to begin with.
In this problem, Alice instead wants to share two classical bits with Bob, but she only has a quantum channel at her disposal, and she is only allowed to use it once (i.e. send only one single-qubit state). Can she succeed?

   (a) The first idea she has is to encode her two classical bits into her preparation of one of four states in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and then send this qubit to Bob.
   Suppose that the a priori distribution of Alice's two classical bits is uniform. What is the maximum probability with which Bob can correctly guess both of Alice's two classical bits?

(b) Suppose that Alice and Bob share a maximally entangled pair of qubits. Alice thinks that it is a good idea to start by performing one of four unitary transformations on the qubit in her possession depending on the value of the two classical bits that she wishes to communicate and send her qubit to Bob. What next? Help Alice (and Bob) devise a scheme that achieves the desired task with certainty.

(c) After all the thought that Alice and Bob put into coming up with a working scheme, they finally decide to employ it.
Unfortunately, the tireless eavesdropper Eve has heard of their new scheme, and as soon as Alice and Bob use it, she intercepts the qubit as it's sent from Alice to Bob. Can Eve recover information about the two confidential classical bits that Alice intended to share with Bob?

2. (10 points) **Semidefinite programming.**
A *semidefinite program* (SDP) is a triple (Φ, A, B), where

- $\Phi : M_d(\mathbb{C}) \to M_{d'}(\mathbb{C})$ is a linear map of the form $\Phi(X) = \sum_{i=1}^k K_i X K_i^\dagger$, for K_i arbitrary $d' \times d$ matrices with complex entries, and
- $A \in M_d(\mathbb{C})$, $B \in M_{d'}(\mathbb{C})$ are Hermitian matrices.

Let $\Phi^*(Y) = \sum_{i=1}^k K_i^\dagger Y K_i$ be the adjoint map to Φ. We associate with the triple (Φ, A, B) two optimization problems, called the primal and dual problems, as follows:

Primal problem	Dual problem
$\alpha := \max_X \operatorname{Tr}(AX)$	$\beta := \min_Y \operatorname{Tr}(BY)$
$s.t.\quad \Phi(X) = B,$	$s.t.\quad \Phi^*(Y) \geq A,$
$X \geq 0.$	$Y = Y^\dagger.$

(a) Show that it is always the case that $\alpha \leq \beta$. This condition is called *weak duality.*

(b) Remember that the inequality $M \geq N$, for M, N Hermitian $d \times d$ matrices, is always taken to mean $M - N \geq 0$, or equivalently all eigenvalues of $(M - N)$ are non-negative. What does the condition $M \leq \lambda \mathbb{I}$, for some fixed Hermitian $M \in M_d(\mathbb{C})$ and $\lambda \in \mathbb{R}$, mean on the eigenvalues of M?

(c) Express the problem of computing the largest eigenvalue $\lambda_1(M)$ of a given $d \times d$ Hermitian matrix M in the form of a *dual problem* as above. That is, specify the map Φ (via the matrices K_i) and the matrices A and B such that $\beta = \lambda_1(M)$. Write the primal problem. Show that, in this case, its optimum $\alpha = \beta$.

(d) Suppose given a Hermitian matrix M that is the difference of two density matrices, $M = \rho - \sigma$. Express the problem of computing $\|M\|_{tr} = \frac{1}{2}\|M\|_1$ in the form of a *primal problem* as above. That is, specify the map Φ and the matrices A and B such that $\alpha = \|M\|_{tr}$. *[Hint: recall the operational interpretation of the trace distance as optimal distinguishing probability.]* Write the dual problem. Show that, in this case, its optimum $\beta = \alpha$.

(e) Suppose you are given one of k possible density matrices, $\rho_1, \ldots, \rho_k$, each with a priori probability $p_1, \ldots, p_k$ respectively. Your goal is to find the optimal guessing measurement: this is the k-outcome POVM which maximizes your chances of producing the index $j \in \{1, \ldots, k\}$, given one copy of ρ_j (which is assumed to occur with probability p_j). First write a formula that expresses the success probability of distinguishing with a POVM $\{M_x\}$. Show that the problem of optimizing this quantity can be expressed as a semidefinite program in primal or dual form (whichever you find most convenient).

It turns out that in many cases (essentially all "well-behaved" cases) the optimum of the primal problem of a semidefinite program equals the optimum of the dual problem. This is useful for several reasons. First of all, note how the primal is a maximization problem, while the dual is a minimization problem. Therefore any feasible solution (a candidate solution that satisfies all the constraints) to the primal provides a lower bound on the optimum, while a feasible solution to the dual provides an upper bound. The fact that they are equal shows that one can get tight bounds in this way. In addition, formulating a problem in, say, primal form, and then looking at the dual formulation, can provide useful insights on the problem. We will see examples of this later on in the course, when we discuss the relation between "guessing probability" and "conditional min-entropy".

3. (4 points) **Maximally entangled properties.**
Let A and B be quantum systems of the same dimension d. Let $|\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{0\le i\le d-1} |i\rangle_A \otimes |i\rangle_B$. This is referred to as a *maximally entangled* pair of qudits.

   (i) What is the reduced state on subsystem A?

   (ii) Let $M \in M_d(\mathbb{C})$. Show that $M \otimes \mathbb{I}\, |\phi^+\rangle = \mathbb{I} \otimes M^T\, |\phi^+\rangle$.

4. **Choi's theorem.** *[This problem is optional, and you may use its results to solve the following problem.]*
A linear map $\boldsymbol{T} : M_d(\mathbb{C}) \to M_{d'}(\mathbb{C})$ is said to be *completely positive* if for any $d'' \geq 0$ the map $\boldsymbol{T} \otimes \boldsymbol{id}_{d''} : M_d(\mathbb{C}) \otimes M_{d''}(\mathbb{C}) \to M_{d'}(\mathbb{C}) \otimes M_{d''}(\mathbb{C})$ is *positive*, where $\boldsymbol{id}_{d''} : M_{d''}(\mathbb{C}) \to M_{d''}(\mathbb{C})$ is the identity map. (Recall that a positive map is one which maps positive semidefinite matrices to positive semidefinite matrices. Not every positive map is completely positive: a good example is the transpose map on 2×2 matrices.)
Let $|\Phi^+\rangle = \sum_{0\le i\le d-1} |i\rangle \otimes |i\rangle$ (this is just $\sqrt{d}$ times the maximally entangled state defined in the previous question), and define $\Phi^+ := |\Phi^+\rangle \langle \Phi^+|$. Define the *Choi-Jamiolkowski representation* $J(T) \in M_{d'}(\mathbb{C}) \otimes M_d(\mathbb{C})$ of a linear map $\boldsymbol{T} : M_d(\mathbb{C}) \to$

$M_{d'}(\mathbb{C})$ as follows:

$$J(\boldsymbol{T}) = \boldsymbol{T} \otimes \boldsymbol{id}_d\ (\Phi^+) = \sum_{0 \le i,j \le d-1} \boldsymbol{T}(|i\rangle\langle j|) \otimes |i\rangle\langle j|. \tag{1}$$

In this problem, you will show that, letting $J(\boldsymbol{T})$ be the Choi-Jamiolkowski representation of a linear map $\boldsymbol{T} : M_d(\mathbb{C}) \to M_{d'}(\mathbb{C})$, the following are equivalent:

(1) $J(\boldsymbol{T})$ is positive semidefinite.

(2) There is a set of matrices $\{K_j \in M_{d' \times d}(\mathbb{C})\}$ such that $\boldsymbol{T}(X) = \sum_j K_j X K_j^\dagger$ for $X \in M_d(\mathbb{C})$.

(3) $\boldsymbol{T}$ is completely positive.

(a) Show that (2) $\Rightarrow$ (3), i.e. that if $\boldsymbol{T}$ is such that $\boldsymbol{T}(X) = \sum_j K_j X K_j^\dagger$ for $X \in M_d(\mathbb{C})$, then $\boldsymbol{T}$ is completely positive.

(b) Explain why (3) $\Rightarrow$ (1).

(c) Let $\boldsymbol{t}_d : M_d(\mathbb{C}) \to M_d(\mathbb{C})$ be the linear map defined by $X \mapsto X^T$. $\boldsymbol{t}_d$ transposes the matrix but we take care to define it in this way as we could be taking the transpose just on a single subsystem. Show that the action of $\boldsymbol{T}$ on $X \in M_d(\mathbb{C})$ can be written in terms of its Choi-Jamiolkowski representation $J(\boldsymbol{T})$ as

$$\boldsymbol{T}(X) = \mathrm{Tr}_A[(\boldsymbol{id}_{d'} \otimes \boldsymbol{t}_d(J(\boldsymbol{T})))(\mathbb{I}_B \otimes X_A)], \tag{2}$$

and deduce that there is a one-to-one correspondence between linear maps from $M_d(\mathbb{C})$ to $M_{d'}(\mathbb{C})$ and their operator representations in $M_{d'}(\mathbb{C}) \otimes M_d(\mathbb{C})$.

(d) Define the linear map $\boldsymbol{vec} : M_{d' \times d}(\mathbb{C}) \to M_{d'}(\mathbb{C}) \otimes M_d(\mathbb{C})$ by its action on the standard basis, $\boldsymbol{vec} : |i\rangle\langle j| \mapsto |i\rangle \otimes |j\rangle$ for $0 \le i \le d'$ and $0 \le j \le d$. Let $Z \in M_{d' \times d}(\mathbb{C})$. Show that a map of the form $\boldsymbol{T} : X_A \mapsto Z X_A Z^\dagger$ has Choi-Jamiolkowski representation $|\zeta\rangle\langle\zeta|$ where $|\zeta\rangle = \boldsymbol{vec}(Z)$.

(e) Show that (1) $\Rightarrow$ (2), i.e. suppose that a map $\boldsymbol{T} : M_d(\mathbb{C}) \to M_{d'}(\mathbb{C})$ has a positive semidefinite Choi-Jamiolkowski representation. Construct a set of maps $\{K_j \in M_{d' \times d}(\mathbb{C})\}$ such that $\boldsymbol{T}(X) = \sum_j K_j X K_j^\dagger$ for any $X \in M_d(\mathbb{C})$.
[Hint: You might find calculations from part (d) helpful.]

5. (10 points) **A limit on quantum attacks on Wiesner's scheme.**
Consider Wiesner's quantum money scheme for the case of a single qubit. Recall that an attack on this scheme is a CPTP map $\boldsymbol{T}$ which maps a single qubit to two qubits, and is such that the probability that the two-qubit density matrix $\boldsymbol{T}(|x\rangle\langle x|_\theta)$ succeeds in the bank's verification procedure twice in sequence is maximized, when $x, \theta \in \{0,1\}$ are chosen uniformly at random.

(a) Write out the formula which expresses the success probability of an attack specified by a CPTP map $\boldsymbol{T}$.

(b) Let $J(\boldsymbol{T}) = \sum_{i,j\in\{0,1\}} \boldsymbol{T}(|i\rangle\langle j|) \otimes |i\rangle\langle j|$ be the Choi-Jamiolkowski representation of the map $\boldsymbol{T}$. Consider the matrix $Q = \sum_{x,\theta\in\{0,1\}} |x\rangle\langle x|_\theta \otimes |x\rangle\langle x|_\theta \otimes |x\rangle\langle x|_\theta$. Write the success probability of the map $\boldsymbol{T}$ as a simple expression involving $J(\boldsymbol{T})$ and Q.

(c) Show that the condition that the CP map $\boldsymbol{T}$ is trace-preserving can be expressed as the condition that its Choi-Jamiolkowski representation $J(\boldsymbol{T})$ satisfies

$$\mathrm{Tr}_1\big(J(\boldsymbol{T})\big) = \sum_{0\le i,j\le d-1} \mathrm{Tr}\,\big(\boldsymbol{T}(|i\rangle\langle j|)\big)\ |i\rangle\langle j| = \mathbb{I}_d.$$

(d) Find a semidefinite program in primal form (see problem 2.) whose optimum is the success probability of an arbitrary attack on the single-qubit Wiesner quantum money scheme. *[Hint: recall the characterization of CP maps from their Choi-Jamiolkowski representation given in the previous problem, and use the previous question as well]* Write down the dual semidefinite program.

(e) Solve the semidefinite program! That is, give an explicit matrix which achieves the optimum, together with the value of the optimum. *[Hint: I will allow you to google — but if you do so, state your source. Serious bonus points for solving the problem yourself, either by hand (explain your reasoning) or using Matlab or any other program (print out your code).]*

(f) Give an explicit representation of the attack you found in (e) as a sequence of three operations: (i) appending some auxiliary qubits in state $|0\rangle$; (ii) applying a unitary transformation on all qubits; (iii) performing a partial trace or measurement map on some of the qubits. *[If you weren't able to solve (e), you can ignore this question. It will only count for 1 point.]*