COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 3

This exercise sheet is designed to help you review the concepts discussed in the lecture and explore some additional interesting results that were not covered in the lecture. Exercises marked with * will have solutions provided after the exercise session, while those marked with ♦ will be the main focus during the exercise session. You are encouraged to discuss with other students, and ask for help if you get stuck for too long.

1. **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	
	$\alpha := \max \mathrm{Tr}(AX)$		$\beta := \min \mathrm{Tr}(BY)$
s.t.	$\Phi(X) = B,$	*s.t.*	$\Phi^*(Y) \geq A,$
	$X \geq 0.$		$Y = Y^\dagger.$

   (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 $\alpha = \|M\|_{tr}$. 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 express this problem as an optimization problem, and then show that it can be written in the form of a primal or dual semidefinite program.

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".