COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 3

1. **Semidefinite programming**

   (a) We first prove a lemma: If $X, Y \in \mathbb{C}^{d\times d}$, $X \geq 0$, $Y \geq 0$, then $\mathrm{Tr}(XY) \geq 0$.

   This is because for $X \geq 0$, we can find eigenvalue decomposition of X: $X = \sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle\phi_i|$ where the eigenvalues $\lambda_i \geq 0$.

   Then $\mathrm{Tr}(XY) = \mathrm{Tr}(\sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle\phi_i| Y) = \sum_{i=1}^{d} \lambda_i \langle\phi_i| Y |\phi_i\rangle \geq 0$ because since $Y \geq 0$, we have that $\langle\phi_i| Y |\phi_i\rangle \geq 0$ for each i.

   Let $\Omega_1 = \{X \in \mathbb{C}^{d\times d} : X \geq 0,\ \Phi(X) = B\}$, and $\Omega_2 = \{Y \in \mathbb{C}^{d'\times d'} : \Phi^*(Y) \geq A,\ Y = Y^\dagger\}$ be the set of X and the set of Y satisfying the constraints in the primal problem and the dual problem. Now, for any $X \in \Omega_1$ and $Y \in \Omega_2$, we have

   $$\begin{aligned}
   \mathrm{Tr}(BY) =& \mathrm{Tr}(\Phi(X)Y) \\
   =& \mathrm{Tr}(X\Phi^*(Y)) \\
   =& \mathrm{Tr}(X(\Phi^*(Y) - A)) + \mathrm{Tr}(XA) \\
   \geq& \mathrm{Tr}(XA) \qquad \text{(apply the lemma on } X \geq 0, \Phi^*(Y) - A \geq 0) \\
   =& \mathrm{Tr}(AX).
   \end{aligned}$$

   Therefore, $\beta = \inf_{Y\in\Omega_2} \mathrm{Tr}(BY) \geq \sup_{X\in\Omega_1} \mathrm{Tr}(AX) = \alpha$.

   (b) For a Hermitian matrix $M \in \mathbb{C}^{d\times d}$, we can find the eigenvalue decomposition of M: $M = \sum_{i=1}^{d} \mu_i |\phi_i\rangle\langle\phi_i|$.

   Since $\{|\phi_i\rangle\}$ forms a basis of $\mathbb{C}^d$, we have that $\lambda\mathbb{I} - M = \sum_{i=1}^{d}(\lambda - \mu_i) |\phi_i\rangle\langle\phi_i|$.

   Therefore, $M \leq \lambda\mathbb{I} \Leftrightarrow \lambda\mathbb{I} - M \geq 0 \Leftrightarrow \forall i, \lambda - \mu_i \geq 0 \Leftrightarrow \forall i, \lambda \geq \mu_i$, which means all eigenvalues of M are less than or equal to λ.

   (c) We want Y to act as λ in (b), $\Phi^*(\lambda) = \lambda\mathbb{I}$ and $A = M$ in order to put the condition $\lambda\mathbb{I} \geq M$ in the dual problem.

   So we choose $d' = 1$, $K_i = (0\ 0\ \cdots\ 1\ 0\cdots 0) = \langle i-1|$ be the $1 \times d$ matrix that has 0 on every entry except the i^{th} entry, and $\nu_i = 1$. Then it is easy to see that $\Phi^*(Y) = \sum_{i=0}^{d-1} |i\rangle Y \langle i| = Y \sum_{i=0}^{d-1} |i\rangle\langle i| = Y\mathbb{I}$ and $\Phi(X) = \sum_{i=1}^{d} \langle i| X |i\rangle = \mathrm{Tr}(X)$. We choose $A = M$ and $B = 1$, then the dual problem is just

   $$\begin{aligned}
   & \beta := \inf Y \\
   s.t.\quad & Y\mathbb{I} \geq M, \\
   & Y \in \mathbb{R}.
   \end{aligned}$$

   Using the result of (b), it's easy to see that $\beta = \lambda_1(M)$.

With this choice of Φ, A and B, the primal problem is

$$\begin{aligned} & \alpha := \sup \operatorname{Tr}(MX) \\ s.t. \quad & \operatorname{Tr}(X) = 1, \\ & X \geq 0. \end{aligned}$$

Recall that from (a), we have that $\alpha \leq \beta$. It remains to prove that $\alpha \geq \beta = \lambda_1(M)$. So we only need to find a feasible X such that $\operatorname{Tr}(MX) = \lambda_1(M)$.

Let's do the eigenvalue decomposition of M: $M = \sum_{i=1}^{d} \mu_i |\phi_i\rangle\langle\phi_i|$. Without loss of generality, we assume μ_1 is the largest and thus $\mu_1 = \lambda_1(M)$.

We set $X = |\phi_1\rangle\langle\phi_1|$. This is a feasible X since it is easy to see that $\operatorname{Tr}(X) = 1$ and $X \geq 0$. Moreover, $\operatorname{Tr}(MX) = \langle\phi_1| M |\phi_1\rangle = \mu_1 = \lambda_1(M)$.

Therefore, in this case, its optimum $\alpha = \beta$.

(d) We first show that $\|\rho - \sigma\|_{tr} = \max_{0 \leq E \leq \mathbb{I}} \operatorname{Tr}((\rho - \sigma)E)$. This is because we can do eigenvalue decomposition of $\rho - \sigma$ to get $\rho - \sigma = \sum_{i=1}^{d} \mu_i |\phi_i\rangle\langle\phi_i|$, and then $\max_{0 \leq E \leq \mathbb{I}} \operatorname{Tr}((\rho - \sigma)E) = \max_{0 \leq E \leq \mathbb{I}} \sum_{i=1}^{d} \mu_i \langle\phi_i| E |\phi_i\rangle$ which is at most $\sum_{i:\mu_i > 0} \mu_i$ since $0 \leq \langle\phi_i| E |\phi_i\rangle \leq 1$ for each i (and it is easy to see that there exists E to achieve this). Notice that $\operatorname{Tr}(\rho - \sigma) = 0$ and thus $\sum_i \mu_i = 0$. Therefore, $\max_{0 \leq E \leq \mathbb{I}} \operatorname{Tr}((\rho - \sigma)E) = \sum_{i:\mu_i > 0} \mu_i = \frac{1}{2} \sum_i |\mu_i| = \|\rho - \sigma\|_{tr}$.

In order to write it in the primal problem, we need to rewrite the condition that $E \leq \mathbb{I}$. We let $X_1 = E$ and $X_2 = \mathbb{I} - E$, then we have that

$$\begin{aligned} \|\rho - \sigma\|_{tr} = & \max_{X_1, X_2} \operatorname{Tr}((\rho - \sigma)X_1) \\ \text{s.t.} \quad & X_1 \geq 0,\ X_2 \geq 0,\ X_1 + X_2 = \mathbb{I}. \end{aligned} \tag{1}$$

We group X_1 and X_2 into the diagonal of a single matrix

$$X = \begin{pmatrix} X_1 & X_3 \\ X_3^\dagger & X_2 \end{pmatrix},$$

and use the linear map

$$\Phi\left(\begin{pmatrix} X_1 & X_3 \\ X_3^\dagger & X_2 \end{pmatrix}\right) = X_1 + X_2,$$

which can be also expressed as $\Phi(X) = \nu_1 K_1 X K_1^\dagger + \nu_2 K_2 X K_2^\dagger$ for $K_1 = (\mathbb{I}\ 0) \in \mathbb{C}^{d \times 2d}$, $K_2 = (0\ \mathbb{I}) \in \mathbb{C}^{d \times 2d}$ and $\nu_1 = \nu_2 = 1$.

This allows us to express the conditions $X_1 \geq 0,\ X_2 \geq 0,\ X_1 + X_2 = \mathbb{I}$ as the standard form condition $X \geq 0$ and $\Phi(X) = B$ where $B = \mathbb{I}$.

To write the object $\operatorname{Tr}((\rho - \sigma)X_1)$ in terms of X, we set

$$A = \begin{pmatrix} \rho - \sigma & 0 \\ 0 & 0 \end{pmatrix},$$

and it is clear that $\mathrm{Tr}((\rho-\sigma)X_1) = \mathrm{Tr}(AX)$.
We write the primal problem as

$$\begin{aligned} & \alpha := \sup \mathrm{Tr}(AX) \\ s.t. \quad & \Phi(X) = B, \\ & X \geq 0, \end{aligned}$$

for the above matrices

$$A = \begin{pmatrix} \rho-\sigma & 0 \\ 0 & 0 \end{pmatrix},$$

and $B = \mathbb{I}$, and the Hermitian preserving linear map

$$\Phi\left(\begin{pmatrix} X_1 & X_3 \\ X_3^\dagger & X_2 \end{pmatrix}\right) = X_1 + X_2.$$

With some effort, we can show (X_1, X_2) satisfying Equation (1) can be mapped to

$$X = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix},$$

which satisfies the condition for the primal problem. Moreover, any matrix $X = \begin{pmatrix} X_1 & X_3 \\ X_3^\dagger & X_2 \end{pmatrix}$ such that $\Phi(X) = B$ and $X \geq 0$ can be mapped to (X_1, X_2) satisfying Equation (1). Therefore, the above primal problem computes $\|\rho-\sigma\|_{tr}$.
The dual problem is

$$\begin{aligned} & \beta := \inf \mathrm{Tr}(Y) \\ s.t. \quad & \Phi^*(Y) \geq A, \\ & Y = Y^\dagger, \end{aligned}$$

where $\Phi^*(Y) = \nu_1 K_1^\dagger Y K_1 + \nu_2 K_2^\dagger Y K_2 = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix}$ and $A = \begin{pmatrix} \rho-\sigma & 0 \\ 0 & 0 \end{pmatrix}$.
Just as in (c), to prove $\beta = \alpha$, we only need to find a feasible Y such that $\mathrm{Tr}(Y) = \|\rho-\sigma\|_{tr}$.
Recall that $\rho-\sigma$ can be decomposed as $\rho-\sigma = \sum_{i=1}^d \mu_i |\phi_i\rangle\langle\phi_i|$. We set $Y = \sum_{i:\mu_i\geq 0} \mu_i |\phi_i\rangle\langle\phi_i|$. Then it is easy to see that $\mathrm{Tr}(Y) = \sum_{i:\mu_i\geq 0} \mu_i = \|\rho-\sigma\|_{tr}$, and $Y = Y^\dagger$. Furthermore, $Y = \sum_{i:\mu_i\geq 0} \mu_i |\phi_i\rangle\langle\phi_i| \geq \sum_{i=1}^d \mu_i |\phi_i\rangle\langle\phi_i| = \rho-\sigma$ and thus $\Phi^*(Y) \geq A$, which concludes the proof of part (d).