COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 5

1. **Computing the min-entropy.**

   (a) By definition of the min-entropy, $H_{\min}(X|E) = -\log P_{\text{guess}}(X|E)$, $H_{\min}(X) = -\log P_{\text{guess}}(X)$. So the desired inequality $H_{\min}(X|E) \geq H_{\min}(X) - \log |E|$ is equivalent to the inequality $-\log P_{\text{guess}}(X|E) \geq -\log(|E| \cdot P_{\text{guess}}(X))$.

   Since $-\log x$ is monotonically decreasing, it suffices to prove that

$$P_{\text{guess}}(X|E) \leq |E| \cdot P_{\text{guess}}(X) \ .$$

   (b) Suppose $A \geq 0$ and $B \geq 0$. Write the eigenvalue decomposition of B: $B = \sum_i \lambda_i(B) \ket{u_i}\bra{u_i}$. Using the linearity and cyclicity of the trace,

$$\begin{aligned}
\mathrm{Tr}(AB) &= \mathrm{Tr}\Big(A \sum_i \lambda_i(B) \ket{u_i}\bra{u_i}\Big) = \sum_i \lambda_i(B) \mathrm{Tr}\big(A \ket{u_i}\bra{u_i}\big) \\
&\leq \lambda_{\max}(B) \sum_i \mathrm{Tr}\big(A \ket{u_i}\bra{u_i}\big) = \lambda_{\max}(B) \mathrm{Tr}\Big(A \sum_i \ket{u_i}\bra{u_i}\Big) \\
&= \lambda_{\max}(B) \cdot \mathrm{Tr}(A \cdot \mathbb{I}) = \lambda_{\max}(B) \cdot \mathrm{Tr}(A),
\end{aligned}$$

   where the inequality uses $\mathrm{Tr}\big(A \ket{u_i}\bra{u_i}\big) = \bra{u_i} A \ket{u_i} \geq 0$ since $A \geq 0$.

   (c) Let $\{M_x\}$ be a POVM and ρ_x^E be a quantum state on E. Then $M_x \geq 0$ and $\rho_x^E \geq 0$ with $\mathrm{Tr}(\rho_x^E) \leq 1$, which implies $\lambda_{\max}(\rho_x^E) \leq 1$. Applying part (b) to $A = M_x$, $B = \rho_x^E$ gives

$$\mathrm{Tr}\big(M_x \rho_x^E\big) \ \leq \ \lambda_{\max}(\rho_x^E) \cdot \mathrm{Tr}(M_x) \ \leq \ \mathrm{Tr}(M_x) \ .$$

   (d) Let $\rho_{XE} = \sum_x p_x \ket{x}\bra{x}_X \otimes \rho_x^E$. Then by definition of the guessing probability,

$$P_{\text{guess}}(X|E) = \max_{\{M_x\} \text{ is a POVM}} \big(p_x \mathrm{Tr}(M_x \rho_x^E)\big) \ .$$

   Applying part (c) to the above equation gives

$$\begin{aligned}
P_{\text{guess}}(X|E) \leq& \max_{\{M_x\} \text{ is a POVM}} (p_x \mathrm{Tr}(M_x)) \\
&\leq \max_x p_x \max_{\{M_x\} \text{ is a POVM}} \left(\sum_x \mathrm{Tr}(M_x)\right) \\
&= P_{\text{guess}}(X) \max_{\{M_x\} \text{ is a POVM}} \mathrm{Tr}(\sum_x M_x) \\
&= P_{\text{guess}}(X) \max_{\{M_x\} \text{ is a POVM}} \mathrm{Tr}(\mathbb{I}_E) \\
&= P_{\text{guess}}(X) \cdot |E| \ .
\end{aligned}$$

   By part(a), this implies the desired inequality $H_{\min}(X|E) \geq H_{\min}(X) - \log |E|$.

2. **A dual formulation for the conditional min-entropy.**

(a) Z is block-diagonalized. Therefore, $Z \geq 0$ is equivalent to $\forall\, x, N_x \geq 0$, which holds because $\{N_x\}$ is a valid POVM.

Moreover, by definition of the POVM, we have

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

(b)

$$\begin{aligned}
\mathrm{Tr}(Z\rho_{XE}) &= \mathrm{Tr}\Big(\sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes N_x \sum_{x'\in\mathcal{X}} |x'\rangle\langle x'| \otimes \rho^E_{x'}\Big) \\
&= \sum_{x,x'\in\mathcal{X}} \mathrm{Tr}\big(\,|x\rangle\langle x|\,|x'\rangle\langle x'|\,\big)\mathrm{Tr}\big(N_x\rho^E_{x'}\big) \\
&= \sum_{x\in\mathcal{X}} \mathrm{Tr}\big(N_x\rho^E_x\big).
\end{aligned}$$

(c) Since $Z \geq 0$, it is easy to see that $N_x = (\langle x|\otimes\mathbb{I}_E)Z(|x\rangle\otimes\mathbb{I}_E) \geq 0$ for all x. Besides, it is easy to verify that$\sum_{x\in\mathcal{X}} N_x = \sum_{x\in\mathcal{X}}(\langle x|\otimes\mathbb{I}_E)Z(|x\rangle\otimes\mathbb{I}_E) = \mathrm{Tr}_X(Z) = \mathbb{I}_E$. Therefore, $\{N_x\}$ is a valid POVM.

(d) By the previous results, $\{M_x\}$ can be grouped together into the diagonal of a single matrix Z, and the constraint that $\{M_x\}$ is a POVM can be equivalently written as $Z \geq 0$ and $\Phi(Z) = \mathbb{I}_E$. Besides, the objective function $P_{\text{guess}}(X|E) = \sup_{\{M_x\}} \sum_{x\in\mathcal{X}} \mathrm{Tr}\big(M_x\rho_x\big)$ can also be written in terms of Z as shown in part (b). Therefore the primal problem that gives $P_{\text{guess}}(X|E)$ is

$$\begin{aligned}
P_{\text{guess}}(X|E) = \sup_Z\, &\mathrm{Tr}(Z\rho_{XE}) \\
\text{s.t. }\, &\Phi(Z) = \mathbb{I}_E, \\
&Z \geq 0.
\end{aligned}$$

In the language of Problem 1 in Exercise 3, we are using $A = \rho_{XE}$ and $B = \mathbb{I}_E$, and the map

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

(e) By Exercise 3, for any matrix Y defined over system E,

$$\Phi^*(Y) = \sum_{x\in\mathcal{X}} \big(\,|x\rangle \otimes \mathbb{I}_E\big)Y\big(\,\langle x| \otimes \mathbb{I}_E\big) = \left(\sum_{x\in\mathcal{X}} |x\rangle\langle x|\right) \otimes Y = \mathbb{I}_X \otimes Y.$$

(f) By part (d) and part (e), the dual problem is

$$\begin{aligned} P_{\text{guess}}(X|E) = \inf_{Y} \ & \operatorname{Tr}(Y) \\ \text{s.t.} \ & \mathbb{I}_X \otimes Y \geq \rho_{XE}, \\ & Y = Y^{\dagger}. \end{aligned}$$

(g) We will show that $\mathbb{I}_X \otimes Y \geq \rho_{XE}$ is equivalent to $\forall x \in \mathcal{X}, Y \geq \rho_x$.
$\Leftarrow$: if $Y \geq \rho_x$, then $|x\rangle\langle x| \otimes Y \geq |x\rangle\langle x| \otimes \rho_x$. We can do a summation over x and we will get $\mathbb{I}_X \otimes Y \geq \rho_{XE}$.
$\Rightarrow$: by definition, we have that for all $x \in \mathcal{X}$, $\langle x| \mathbb{I}_X \otimes Y |x\rangle \geq \langle x| \rho_{XE} |x\rangle$, which is $Y \geq \rho_x$ for each x.
Therefore, we can replace the constraint in the dual problem in part (f) with $\sigma \geq \rho_x$ for all $x \in \mathcal{X}$, which concludes the proof of part (g).

(h) Such σ is a feasible solution to the problem in part (g). Therefore, by the definition of infimum, we have $P_{\text{guess}}(X|E) \leq \operatorname{Tr}(\sigma)$.

(i) Set the feasible solution sets for τ and ρ as follows:

$$\begin{aligned} P_1 &= \big\{\{M_{x_1}\} \,:\, \{M_{x_1}\} \text{ a POVM on } \mathcal{H}_{E_1}\big\}, \qquad & \Omega_1 &= \big\{\sigma_1 :\ \sigma_1 \geq \tau_{x_1}^{E_1},\ \forall x_1 \in \mathcal{X}_1\big\}, \\ P &= \big\{\{M_x\} \,:\, \{M_x\} \text{ a POVM on } \mathcal{H}_E\big\}, & \Omega &= \big\{\sigma :\ \sigma \geq \rho_x^E,\ \forall x \in \mathcal{X}^n\big\}. \end{aligned}$$

Define the product-restricted sets

$$\tilde{P} := \Big\{\{M_x\} :\ M_x = M_{x_1} \otimes \cdots \otimes M_{x_n},\ \{M_{x_i}\} \in P_1\Big\}, \qquad \tilde{\Omega} := \Big\{\sigma = \sigma_1 \otimes \cdots \otimes \sigma_n \,:\ \sigma_i \in \Omega_1\Big\}.$$

It is clear that $\tilde{P} \subseteq P$ and $\tilde{\Omega} \subseteq \Omega$.
From previous results, we have that

$$P_{\text{guess}}(X|E) = \sup_{\{M_x\} \in P} \sum_{x \in \mathcal{X}^n} \operatorname{Tr}(M_x \rho_x^E) \ \geq \ \sup_{\{M_x\} \in \tilde{P}} \sum_{x \in \mathcal{X}^n} \operatorname{Tr}(M_x \rho_x^E),$$

and

$$P_{\text{guess}}(X|E) = \inf_{\sigma \in \Omega} \operatorname{Tr}(\sigma) \ \leq \ \inf_{\sigma \in \tilde{\Omega}} \operatorname{Tr}(\sigma).$$

It is not hard to verify that

$$\sup_{\{M_x\} \in \tilde{P}} \sum_{x \in \mathcal{X}^n} \operatorname{Tr}(M_x \rho_x^E) = \Big(\sup_{\{M_{x_1}\} \in P_1} \sum_{x_1 \in \mathcal{X}} \operatorname{Tr}(M_{x_1} \tau_{x_1}^E)\Big)^n = (P_{\text{guess}}(X_1|E_1))^n \ ;$$

Moreover,

$$\inf_{\sigma \in \tilde{\Omega}} \operatorname{Tr}(\sigma) = \big(\inf_{\sigma_1 \in \Omega_1} \operatorname{Tr}(\sigma_1)\big)^n = (P_{\text{guess}}(X_1|E_1))^n \ .$$

Therefore, $P_{\text{guess}}(X|E) = (P_{\text{guess}}(X_1|E_1))^n$.
Thus $H_{\min}(X|E)_\rho = nH_{\min}(X_1|E_1)_\tau$.