COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 5

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. (*, ♦) *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 as an inequality in terms of the guessing probabilities $P_{\text{guess}}(X|E)$, $P_{\text{guess}}(X)$, and $|E|$, 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 $\text{Tr}(AB) \leq \lambda_{\max}(B)\text{Tr}(A)$, 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 $\text{Tr}(M_x\rho_x^E) \leq \text{Tr}(M_x)$.

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

2. (*) *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

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

   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 1 in Exercise 3. Consider the map

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

   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 Exercise 3, Problem 1).

(f) Write the dual problem 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 last part of this problem we use the first part (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 $\sigma \geq \rho_x$ for all $x \in \mathcal{X}$ we have $P_{\mathrm{guess}}(X|E) \leq \mathrm{Tr}(\sigma)$.

(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.]*