Homework 1

Due: September 15, 2025

CS 6832: Quantum Cryptography

Questions 2 and 3 of this problem set are based on the paper arXiv:1210.4359. You are encouraged to refer to it for guidance if you get stuck, but your answers must be in your own words.

1. **Entanglement.**

   Let $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The Z (or computational) basis for a single qubit is $\{|0\rangle, |1\rangle\}$ and the X (or Hadamard) basis is $\{|+\rangle, |-\rangle\}$.

   (a) **(2 Points)** Prove $|\Phi^+\rangle$ is the only two-qubit state such that, when both qubits are measured in the same basis (either Z or X), the measurement outcomes are always equal.

   (b) **(2 Points)** Prove there is no three-qubit state $|\psi\rangle_{\mathsf{ABC}}$ such that, when A, B, and C are measured in the same basis (either Z or X), the measurement outcomes are always equal.

   (c) **(2 Points)** Let $|\psi\rangle_{\mathsf{ABC}}$ be a three-qubit state such that, when A and B are measured in the same basis (either Z or X), the measurement outcomes are always equal. Prove that the state can be written $|\psi\rangle_{\mathsf{ABC}} = |\Phi^+\rangle_{\mathsf{AB}} \otimes |\phi\rangle_{\mathsf{C}}$ for some $|\phi\rangle$.

2. **Properties of the Operator Norm.**

Given a Hilbert space $\mathcal{H}$, we denote the set of linear operators on that space as $\mathcal{L}(\mathcal{H})$. We denote the Schatten ∞-norm (or the operator norm) as $\|X\|$. The following is a useful fact about the operator norm of diagonal block matrices.

Fact 1. *Let $X_1, X_2, \ldots, X_n \in \mathcal{L}(\mathcal{H})$ and X be the $n \times n$ diagonal block matrix*

$$X = \begin{bmatrix} X_1 & 0 & \cdots & 0 \\ 0 & X_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X_n \end{bmatrix}$$

Then $\|X\| = \max_i \|X_i\|$.

(a) **(1 Points)** Prove that $X^\dagger X \geq Y^\dagger Y$ implies $Z^\dagger X^\dagger X Z \geq Z^\dagger Y^\dagger Y Z$ for $X, Y, Z \in \mathcal{L}(\mathcal{H})$.

(b) **(2 Points)** Let $X, Y \in \mathcal{L}(\mathcal{H})$ where $X^\dagger X \geq Y^\dagger Y$. Prove that $\|XZ\| \geq \|YZ\|$ for all $Z \in \mathcal{L}(\mathcal{H})$.

(c) **(3 Points)** Let $\{P_i\}_{i=1}^n$ be projectors (i.e., $P_i^2 = P_i$). Consider the block matrix P defined as

$$P = \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{bmatrix}$$

Prove that $\|\sum_{i=1}^n P_i\| = \|P^\dagger P\| = \|PP^\dagger\|$.

(d) **(4 Points)** Let $(\mathbb{G}, \circ)$ be a group of order n. For this part, we think of the projectors P_i as being indexed by elements of $\mathbb{G}$, i.e., $\{P_i\}_{i=1}^n = \{P_i\}_{i \in \mathbb{G}}$.
Show that $PP^\dagger = \sum_{k \in \mathbb{G}} D_k$, where for each $i, j, k \in \mathbb{G}$, the (i,j)-th block of D_k is

$$(D_k)_{ij} = \begin{cases} P_i P_j & \text{if } i \circ k = j \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

Prove that for all k, $\|D_k\| = \max_i \|P_i P_{i \circ k}\|$. Conclude that $\|\sum_i P_i\| \leq \sum_k \max_i \|P_i P_{i \circ k}\|$.

3. **Monogamy of Entanglement.**

In this problem, we will prove the optimal win probability for a λ-qubit monogamy of entanglement game. The game consists of Player A's measurement projectors $\{|x^\theta\rangle\langle x^\theta|\}_{x,\theta\in\{0,1\}^\lambda}$ (where $|x^\theta\rangle = H^{\theta_1}|x_1\rangle \otimes \ldots \otimes H^{\theta_\lambda}|x_\lambda\rangle$). A strategy $\mathcal{S}$ for this game consists of a tripartite state $|\psi\rangle_{\mathsf{ABC}}$ along with Player B and C's projectors $\{B_y^\theta\}_{y,\theta\in\{0,1\}^\lambda}$ and $\{C_z^\theta\}_{z,\theta\in\{0,1\}^\lambda}$.

Our goal is to prove that for any $\lambda \in \mathbb{N} \setminus \{0\}$,

$$\max_{\mathcal{S}} \Pr[\mathcal{S} \text{ wins}] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda.$$

Recall from the lecture that for a given strategy $\mathcal{S}$,

$$\Pr[\mathcal{S} \text{ wins}] = \frac{1}{2^\lambda} \sum_{\theta\in\{0,1\}^\lambda} \langle\psi|\Pi^\theta|\psi\rangle,$$

where $\Pi^\theta = \sum_{x\in\{0,1\}^\lambda} |x^\theta\rangle\langle x^\theta| \otimes B_x^\theta \otimes C_x^\theta$.

(a) **(3 Points)** Using (2d), show that

$$\max_{\mathcal{S}} \Pr[\mathcal{S} \text{ wins}] \leq \frac{1}{2^\lambda} \sum_{k\in\{0,1\}^\lambda} \max_{\theta\in\{0,1\}^\lambda} \|\Pi^\theta \Pi^{\theta\oplus k}\|$$

where $\theta \oplus k$ indicates bitwise xor between the λ-bit strings.

(b) **(4 Points)** Let $|x_k^\theta\rangle\langle x_k^\theta|_{\mathsf{A}} = \left(\bigotimes_{i:k_i=1} |x_i^{\theta_i}\rangle\langle x_i^{\theta_i}|_{\mathsf{A}_i}\right) \otimes \left(\bigotimes_{i:k_i=0} I_{\mathsf{A}_j}\right)$ be the projector given by "ignoring" the zero indices of $k \in \{0,1\}^\lambda$. For example, if $\lambda = 4$ then

$$|x_{0101}^\theta\rangle\langle x_{0101}^\theta| = I \otimes |x_2^{\theta_2}\rangle\langle x_2^{\theta_2}| \otimes I \otimes |x_4^{\theta_4}\rangle\langle x_4^{\theta_4}|$$

Note that $|x_k^\theta\rangle\langle x_k^\theta| \geq |x^\theta\rangle\langle x^\theta|$ for all $k \in \{0,1\}^\lambda$.

For $\theta, k \in \{0,1\}^\lambda$, we define

$$\mathbf{B}_k^\theta = \sum_x |x_k^\theta\rangle\langle x_k^\theta| \otimes B_x^\theta \otimes I_{\mathsf{C}} \quad \text{and} \quad \mathbf{C}_k^\theta = \sum_x |x_k^{\theta\oplus k}\rangle\langle x_k^{\theta\oplus k}| \otimes I_{\mathsf{B}} \otimes C_x^\theta$$

Prove that $\|\Pi^\theta \Pi^{\theta\oplus k}\|^2 \leq \|\mathbf{B}_k^\theta \mathbf{C}_k^\theta \mathbf{B}_k^\theta\| = 2^{-|k|}$ where $|k| = |\{i : k_i \neq 0\}|$ is the Hamming weight of k.

(c) **(2 Points)** Using (3a) and (3b), show that $\max_{\mathcal{S}} \Pr[\mathcal{S} \text{ wins}] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda$.