COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 4

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. **Tsirelson's bound via sum of square decompositions.**
   In class we saw a quantum strategy that succeeds in the CHSH game with success probability $\frac{1}{2} + \frac{\sqrt{2}}{4}$. In this problem we show that this bound is optimal.

   (a) Suppose that a quantum strategy for the CHSH game is based on observables A_0 and A_1 on $\mathcal{H}_A$ for Alice, B_0 and B_1 on $\mathcal{H}_B$ for Bob, and a shared entangled state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Let $C = A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1$, where we omit the tensor product sign for convenience (this is the same as abusing notation and using e.g. A_1 to denote $A_1 \otimes I_B$, etc.). Show that this strategy succeeds with probability

   $$p_{succ} = \frac{1}{2} + \frac{\langle\psi| C |\psi\rangle}{8} \tag{1}$$

   in the CHSH game.

   (b) Let $P = A_0 - \frac{1}{\sqrt{2}}(B_0 + B_1)$ and $Q = A_0 - \frac{1}{\sqrt{2}}(B_0 - B_1)$. Using identities $A_0^2 = A_1^2 = B_0^2 = B_1^2 = I$ and $A_iB_j = B_jA_i$ for $i, j \in \{1, 2\}$, show by direct calculation that

   $$P^2 + Q^2 = 4I - \sqrt{2}C\ .$$

   (c) Recall that if X is Hermitian then $X^2 \geq 0$. Deduce from the previous questions that

   $$p_{succ} \leq \frac{1}{2} + \frac{\sqrt{2}}{4}\ .$$

2. **A monogamy bound on 2-out-of-3 CHSH.**
   Consider the following 3-player nonlocal game, where the three players are Alice, Bob and Charlie. The referee selects inputs $x, y, z \in \{0, 1\}$ uniformaly at random and sends x to Alice, y to Bob and z to Charlie. The players respond with a single bit each, $a, b, c \in \{0, 1\}$ respectively. With probability $\frac{1}{2}$ the referee checks that $a \oplus b = x \wedge y$ and accepts if and only if this is the case. With probability $\frac{1}{2}$ the referee checks that $b \oplus c = y \wedge z$ and accepts if and only if this is the case.

   (a) Since this is just two copies of the CHSH game, it may at first seem that quantum players can win with probability $\frac{1}{2} + \frac{\sqrt{2}}{4}$ overall. Take a few minutes to see if you can make this work. In particular, try to write down carefully the entangled state that the players would share.

It doesn't work so easily, right? In the remainder of the exercise we apply the same strategy as in the previous exercise to demonstrate that, for this game, there is no quantum advantage!

(b) Let A_i, B_j and C_k, for $i, j, k \in \{0, 1\}$, be the player's observables in a quantum strategy for this game, and let $|\psi\rangle_{ABC}$ be the player's shared entangled state. As before we write A_i for $A_i \otimes I_B \otimes I_C$, etc. Letting

$$C_{AB} = A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1 \quad \text{and} \quad C_{BC} = B_0C_0 + B_1C_0 + B_0C_1 - B_1C_1 \ ,$$

derive an expression similar to (1) for this strategy's success probability in the game.

(c) Let

$$\begin{aligned} Q_1 &= \frac{1}{2\sqrt{2}}\big(A_0(B_0 - B_1) + C_1(B_0 + B_1) - 2A_0C_1\big) \ , \\ Q_2 &= \frac{1}{2\sqrt{2}}\big(A_1(B_0 + B_1) + C_0(B_0 - B_1) - 2A_1C_0\big) \ . \end{aligned}$$

Show that

$$Q_1^2 + Q_2^2 = 2I - \frac{1}{2}(C_{AB} + C_{BC}) \ .$$

(d) Deduce an upper bound on the success probability of this strategy. Show that there exists a classical strategy in the game that achieves the same success probability.