COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 4

1. **Tsirelson's bound via sum of square decompositions.**

   (a) We can observe that, for example,

   $$\begin{aligned}\langle\psi| A_0B_0 |\psi\rangle &= \langle\psi| (A_0^+ - A_0^-)(B_0^+ - B_0^-) |\psi\rangle \\ &= \mathbf{Pr}\big((a_0,b_0)=(0,0)|(x,y)=(0,0)\big) + \mathbf{Pr}\big((a_0,b_0)=(1,1)|(x,y)=(0,0)\big) \\ &\quad - \mathbf{Pr}\big((a_0,b_0)=(0,1)|(x,y)=(0,0)\big) - \mathbf{Pr}\big((a_0,b_0)=(1,0)|(x,y)=(0,0)\big) \\ &= \mathbf{Pr}\big(a_0\oplus b_0=0|(x,y)=(0,0)\big) - \mathbf{Pr}\big(a_0\oplus b_0=1|(x,y)=(0,0)\big) \\ &= 2\,\mathbf{Pr}\big(WIN|(x,y)=(0,0)\big) - 1\ ,\end{aligned}$$

   where for the last line we used

   $$\mathbf{Pr}\big(a_0\oplus b_0=0|(x,y)=(0,0)\big) + \mathbf{Pr}\big(a_0\oplus b_0=1|(x,y)=(0,0)\big) = 1\ .$$

   Performing a similar calculation for the three other terms gives the result.

   (b) By expanding the squares we get

   $$\begin{aligned}P^2 &= I + \frac{1}{2}\big(2I + B_0B_1 + B_1B_0\big) - \frac{2}{\sqrt{2}}A_0(B_0+B_1)\ , \\ Q^2 &= I + \frac{1}{2}\big(2I - B_0B_1 - B_1B_0\big) - \frac{2}{\sqrt{2}}A_1(B_0-B_1)\ .\end{aligned}$$

   Summing the two expressions, we get the desired relation.

   (c) From part (b) it then follows that

   $$0 \le \langle\psi| (P^2+Q^2) |\psi\rangle = 4\,\langle\psi|\psi\rangle - \sqrt{2}\,\langle\psi| C |\psi\rangle\ .$$

   Since $\langle\psi|\psi\rangle = 1$, using the expression for p_{succ} given in part (a) be obtain Tsirelson's bound.

2. **A monogamy bound on 2-out-of-3 CHSH.**

   (a) It doesn't work, because Bob doesn't know ahead of time if he will play CHSH with Alice or with Charlie. He can share an EPR pair with each of them, but he doesn't know which qubit to measure to return his result.

   (b) We obtain

   $$p_{succ} = \frac{1}{2} + \frac{1}{16}\big(\,\langle\psi| C_{AB} |\psi\rangle + \langle\psi| C_{BC} |\psi\rangle\,\big)\ .$$

   (c) This identity can be verified by direct calculation.

   (d) We obtain the bound $p_{succ} \le \frac{3}{4}$. This is the same success probability obtained by the classical strategy where all players answer 0 all the time.