# 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,

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

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, we can get

$$\begin{aligned}
\langle\psi| A_0B_1 |\psi\rangle &= \mathbf{Pr}\big(a_0\oplus b_0 = 0|(x,y)=(0,1)\big) - \mathbf{Pr}\big(a_0\oplus b_0 = 1|(x,y)=(0,1)\big) \\
&= 2\,\mathbf{Pr}\big(\mathrm{WIN}|(x,y)=(0,1)\big) - 1 \;,
\end{aligned}$$

$$\begin{aligned}
\langle\psi| A_1B_0 |\psi\rangle &= \mathbf{Pr}\big(a_0\oplus b_0 = 0|(x,y)=(1,0)\big) - \mathbf{Pr}\big(a_0\oplus b_0 = 1|(x,y)=(1,0)\big) \\
&= 2\,\mathbf{Pr}\big(\mathrm{WIN}|(x,y)=(1,0)\big) - 1 \;,
\end{aligned}$$

$$\begin{aligned}
\langle\psi| A_1B_1 |\psi\rangle &= \mathbf{Pr}\big(a_0\oplus b_0 = 0|(x,y)=(1,1)\big) - \mathbf{Pr}\big(a_0\oplus b_0 = 1|(x,y)=(1,1)\big) \\
&= 1 - 2\,\mathbf{Pr}\big(\mathrm{WIN}|(x,y)=(1,1)\big) \;.
\end{aligned}$$

By total probability,

$$\begin{aligned}
p_{\mathrm{succ}} &= \sum_{x^*\in\{0,1\},y^*\in\{0,1\}} \mathbf{Pr}\big(\mathrm{WIN}|(x,y)=(x^*,y^*)\big)\,\mathbf{Pr}\big((x,y)=(x^*,y^*)\big) \\
&= \frac{1}{4}\sum_{x^*\in\{0,1\},y^*\in\{0,1\}} \mathbf{Pr}\big(\mathrm{WIN}|(x,y)=(x^*,y^*)\big) \\
&= \frac{1}{2} + \frac{\langle\psi| C |\psi\rangle}{8}
\end{aligned}$$

which is the desired equality.

(b) By expanding the squares (and using the identities $A_0^2 = A_1^2 = B_0^2 = B_1^2 = I$ and $A_iB_j = B_jA_i$), we get that

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

Summing the two expressions, we get the desired relation.

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

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

We can use the expression for $p_{\text{succ}}$ given in part (a) be obtain the desired 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) Using the same reasoning as in part (1a), we can show that, conditioned on the referee verifying that $a \oplus b = x \wedge y$, the success probability can be written as $\frac{1}{2} + \frac{\langle\psi|C_{AB}|\psi\rangle}{8}$.
And conditioned on the referee verifying that $b \oplus c = y \wedge z$, the success probability can be written as $\frac{1}{2} + \frac{\langle\psi|C_{BC}|\psi\rangle}{8}$.
Note that the referee does the above checks with equal probability, we can obtain that

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

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

$$\begin{aligned}
Q_1^2 =& \frac{1}{8}\left(A_0^2(B_0 - B_1)^2 + C_1^2(B_0 + B_1)^2 + 4A_0^2C_1^2\right)\\
&+ \frac{1}{8}A_0C_1(B_0 - B_1)(B_0 + B_1) + \frac{1}{8}A_0C_1(B_0 + B_1)(B_0 - B_1)\\
&- \frac{1}{2}A_0C_1^2(B_0 + B_1) - \frac{1}{2}A_0^2C_1(B_0 - B_1)\\
=& \frac{1}{8}\left(2B_0^2 + 2B_1^2 + 4I\right) + \frac{1}{4}A_0C_1(B_0^2 - B_1^2) - \frac{1}{2}A_0(B_0 + B_1) - \frac{1}{2}C_1(B_0 - B_1)\\
=& I - \frac{1}{2}A_0(B_0 + B_1) - \frac{1}{2}C_1(B_0 - B_1)\ .
\end{aligned}$$

Similarly, we can show that

$$Q_2^2 = I - \frac{1}{2}A_1(B_0 - B_1) - \frac{1}{2}C_0(B_0 + B_1)\ .$$

Therefore, we have that

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

(d) Using the same reasoning as in part (1c), we obtain that $\langle\psi| C_{AB} |\psi\rangle + \langle\psi| C_{BC} |\psi\rangle \leq 4$ and thus thus from the part (2b), $p_{\text{succ}} \leq \frac{3}{4}$. This is the same success probability obtained by the classical strategy where all players answer 0 all the time.