QII Exercise sheet 7

Notations. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. " $+$ " corresponds to the $\{|0\rangle, |1\rangle\}$ basis and " $\times$ " corresponds to the $\{|+\rangle, |-\rangle\}$ basis. We have $|b\rangle^{+} = |b\rangle$ and $|b\rangle^{\times} = H|b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{b}|1\rangle\right)$. Recall the main steps of the BB84 protocol

1. Alice picks a random initial raw key $K = k_1, \ldots, k_n$ uniformly at random.
2. For each $i \in \{1, \ldots, n\}$, Alice picks a random $b_i \in \{+, \times\}$, constructs $|\psi_i\rangle = |k_i\rangle^{b_i}$ and sends $|\psi_i\rangle$ to Bob.
3. Bob picks some random basis $b'_1, \ldots, b'_n \in \{+, \times\}$ and measures each qubit $|\psi_i\rangle$ in the b'_i basis. Let c_i be the outcome of this measurement.
4. Bob sends to Alice the basis $\mathbf{b'} = b'_1, \ldots, b'_n$ he used for his measurements using a public channel. Alice sends back the subset $I = \{i \in [n] : b_i = b'_i\}$ to Bob.
5. Alice then picks a random subset $J \subseteq I$ of size $\frac{|I|}{2}$ which is the subset of indices for which Alice and Bob check that there wasn't any interception and sends J to Bob. For $j \in J$, Alice also sends k_j to Bob.
6. For each $j \in J$, Bob checks that $k_j = c_j$. If one of these checks fail, he aborts.
7. Let $L = I \backslash J = l_1, \ldots, l_{|L|}$ be the subset of indices used for the final raw key. Alice has $K_A = \{k_l\}_{l \in L}$ and Bob has $K_B = \{c_l\}_{l \in L}$. They perform key reconciliation and privacy amplification to obtain the final common key K_{final}.

Exercise 1. *We consider the BB84 quantum key distribution protocol seen in class. We want to analyze the information that an eavesdropper Eve can have about each k_i if she measures the qubits $|\psi_i\rangle$ at step 2. We first consider here the case $n = 1$, so there is a single k_1, b_1 and a single state $|\psi_1\rangle$ sent.*

1. *Let ρ_{k_1} be the state that Alice sends as a function of k_1. Describe the mixed states ρ_0 and ρ_1. Let $|v\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $|v^{\perp}\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$. Show that*

$$\rho_0 = \cos^2(\pi/8)|v\rangle\langle v| + \sin^2(\pi/8)|v^{\perp}\rangle\langle v^{\perp}| \quad (1)$$

$$\rho_1 = \sin^2(\pi/8)|v\rangle\langle v| + \cos^2(\pi/8)|v^{\perp}\rangle\langle v^{\perp}| \quad (2)$$

2. *Compute the statistical distance between ρ_0 and ρ_1.*
3. *Compute Eve's optimal strategy to guess k_1. What is the measurement that achieves this guessing probability? What can you say about the overall security of the scheme.*

Exercise 2. *We consider another cheating strategy. The second cheating strategy for Eve consists in intercepting and storing the states $|\psi_i\rangle$ at step 2 and wait until she sees $\mathbf{b}', I, J$ after step 5 in order to get some information about the key.*

1. *Show that with this strategy, Alice can recover all the string k.*
2. *The issue with this strategy is the test at step 6. If Eve intercepts $|\phi_i\rangle$ then Bob doesn't get any state at the end of step 2. For each i, Eve sends a state $|\xi_i\rangle$ which is independent of b_i and k_i (since Eve doesn't know them). For a index i, compute the probability that Bob outputs c_i for each choice b'_i, depending on $|\xi_i\rangle$. Show that the probability of outputting $b'_i = b_i$ and $k_i \neq c_i$ is $\frac{1}{4}$.*
3. *Conclude on the efficiency of this cheating strategy.*

Exercise 3. *We consider yet another cheating strategy in the case the classical channel is not authenticated, meaning that Eve can modify the messages sent in the classical portion. Show how can Eve can cheat in this setting (recall that she can also tamper the quantum channel).*

* * *

Exercise 4 (GHZ Game)**.** *The game involved 3 cooperating players Alice, Bob and Charlie that cannot communicate, and is defined as follows:*

- *Alice, Bob and Charlie receive respective random inputs $x, y, z \in \{0, 1\}$ containing an even number of 1. This means they get inputs $(x, y, z) = (0, 0, 0)$ or $(0, 1, 1)$ or $(1, 0, 1)$ or $(1, 1, 0)$ each wp. $\frac{1}{4}$.*
- *They each output a bit, noted respectively a, b and c.*
- *They win the GHZ game iff. $a \oplus b \oplus c = OR(x, y, z)$ meaning that $a \oplus b \oplus c = 0$ iff. $(x, y, z) = (0, 0, 0)$ and $a \oplus b \oplus c = 1$ otherwise.*

1. *Show that every deterministic classical strategy succeeds wp. at most $\frac{3}{4}$.*
2. *Suppose the players share the following entangled 3-qubit state:*

$$|\phi\rangle = \frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right).$$

Suppose each player does the following: if his/her input is 1, apply H to his/her qubit, otherwise do nothing. Describe the resulting 3-qubit superposition.

3. *Use the above to derive a strategy that wins the GHZ game wp. 1 when the players share the state* $|\phi\rangle$.

Exercise 5. *The goal of this exercice is to prove the optimality of the entangled strategy for the CHSH game that succeeds wp.* $\cos^2(\pi/8)$. *Recall that the CHSH game is the following game between Alice and Bob:*

- *Alice receives a random bit* $x \in \{0,1\}$ *and outputs a bit* a.
- *Bob receives a random bit* $y \in \{0,1\}$ *and outputs a bit* b.
- *They win the game iff.* $a \oplus b = x \wedge y$.

1. *We will first present another strategy for the CHSH game, which is easier to analyze than the one in class. Consider the following strategy for Alice and Bob:*

   - *Alice and Bob share the state* $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.
   - *For some parameters,* $\theta_0^A, \theta_1^A, \theta_0^B, \theta_1^B$, *Alice performs* $R_{\theta_x^A}$ *on her qubit and Bob performs* $R_{\theta_y^B}$ *on his qubit, where*

   $$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

   Then they measure their qubit in the computational basis to get their respective outputs a, b.

   (a) *Show that if Alice applies* R_{θ^A} *and Bob applies* R_{θ^B} *on the joint state* $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, *the resulting state is*

   $$|\phi_1\rangle = \frac{1}{\sqrt{2}}\left(\cos(\theta^A + \theta^B)(|00\rangle - |11\rangle) + \sin(\theta^A + \theta^B)(|01\rangle + |10\rangle)\right).$$

   (b) *Show that the described strategy wins the game wp.* $\cos^2(\pi/8)$ *by taking* $\theta_0^A = \theta_0^B = -\frac{\pi}{16}$ *and* $\theta_1^A = \theta_1^B = \frac{3\pi}{16}$.

2. *We now want to show that this strategy is optimal. We first change the formulation of the CHSH game to the following equivalent formulation:*

   - *Alice receives a random bit* $x \in \{0,1\}$ *and outputs a value* $a \in \{-1,1\}$.
   - *Bob receives a random bit* $y \in \{0,1\}$ *and outputs a value* $b \in \{-1,1\}$.
   - *They win the game iff.* $ab = (-1)^{x \wedge y}$.

We consider an entangled strategy where Alice and Bob share a state $|\psi\rangle$. On input x, Alice performs the projective measurement $\{A_1^x, A_{-1}^x\}$ and Bob performs the projective measurement $\{B_1^y, B_{-1}^y\}$. The subscripts correspond to the outputs of the measurement. We also define the unitaries $A^x = A_1^x - A_{-1}^x$ and $B^y = B_1^y - B_{-1}^y$.

(a) Recall that the probability for Alice and Bob of outputting a specific output pair $a, b \in \{-1, 1\}$ is $\langle\psi| A_a^x \otimes B_b^y |\psi\rangle$. Show that the expected value of $[ab]$ for this strategy for a fixed input pair (x, y) is

$$\langle\psi| A^x \otimes B^y |\psi\rangle .$$

One can use the identity for tensor products

$$M \otimes (N + P) = M \otimes N + M \otimes P.$$

for any operators M, N, P.

(b) Show that for a fixed input pair (x, y), the probability of outputting a, b st. $ab = s$ is $\frac{1}{2} + \frac{s}{2} \langle\psi| A^x \otimes B^y |\psi\rangle$.

(c) Define the $2k$-qubit operator $C = A^0 \otimes B^0 + A^0 \otimes B^1 + A^1 \otimes B^0 - A^1 \otimes B^1$. Show that the winning probability of the protocol (averaged over all 4 inputs pairs x, y) is $\frac{1}{2} + \frac{1}{8} \langle\psi| C |\psi\rangle$.

(d) Show that

$$C^2 = 4I + (A^0 A^1 - A^1 A^0) \otimes (B^1 B^0 - B^0 B^1)$$

where I is the $2k$-qubit identity matrix and C^2 here is the square of C. Use the fact that the A^x and B^y are unitaries with ± 1 eigenvalues so the squared matrices $(A^x)^2$ and $(B^y)^2$ are equal to the identity. One can use the identity

$$(M \otimes N)(M' \otimes N') = MM' \otimes NN'.$$

for any operators M, N, M', N'.

(e) For any bits x_0, x_1, y_0, y_1, and any quantum state ψ, we have

$$\langle\psi| A^{x_0} A^{x_1} \otimes B^{y_0} B^{y_1} |\psi\rangle \leq 1 \tag{3}$$

Show that $\langle\psi| C^2 |\psi\rangle \leq 8$. You can use Equation 3 without proof. If you can, try to argue or prove this equation.

(f) Since for any $|\phi\rangle$, $\langle\phi| C^2 |\phi\rangle \leq 8$, *this implies that for* $|\psi\rangle$,

$$\langle\psi| C |\psi\rangle \leq \sqrt{8}. \tag{4}$$

Show that the value of the CHSH game is at most $\cos^2(\pi/8)$. *You can prove Equation 4 without proof. If you want, try to prove Equation 4.*

Exercise 6. *We consider the 2-fold parallel repetition of the CHSH game, that we denote CHSH*^{2}. *This corresponds to the following game*

- *Alice receives two random bits* $x_1, x_1 \in \{0,1\}$ *and outputs two bits* a_1, a_2.
- *Bob receives two random bits* $y_1, y_2 \in \{0,1\}$ *and outputs two bits* b_1, b_2.
- *They win the game iff.* $a_1 \oplus b_1 = x_1 \wedge y_1$, *and* $a_2 \oplus b_2 = x_2 \wedge y_2$

1. *Give a quantum strategy that wins the game CHSH*^{2} *wp.* $\cos^4(\pi/8)$.
2. *Recall that the best classical strategy wins CHSH wp.* $\frac{3}{4}$ *so we expect the best classical strategy for CHSH*^{2} *to win wp.* $\frac{9}{16}$. *Show that there exists a strategy that wins CHSH*^{2} *wp* $\frac{10}{16}$.

Exercise 7. *Consider 2 discrete probability function* $p = (p_1, \ldots, p_n)$ *and* $q = (q_1, \ldots, q_m)$. *So we have* $p_i \geq 0, \sum_i p_i = 1$, *and* $q_i \geq 0, \sum_i q_i = 1$. *Consider the direct product distribution* $r = (r_{1,1}, \ldots, r_{n,m})$ *where* $r_{i,j} = p_i q_j$. *Show that*

$$H(r) = H(p) + H(q).$$

Exercise 8. *For each state* $|\psi_{AB}\rangle$, *give the reduced density matrices* $\rho_A = tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$ *and* $\rho_B = tr_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$. *You can write your answers in Dirac's "ket,bra" notation or in matrix form. Compute also* $H(\rho_A)$ *in each case. You can use* $\log_2(3) \approx 1.585$.

1. $|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0-\rangle + |1+\rangle)$.
2. $|\psi_{AB}\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$.
3. $|\psi_{AB}\rangle = \sqrt{\frac{3}{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle - \sqrt{\frac{1}{8}}|10\rangle + \sqrt{\frac{1}{8}}|11\rangle$.

Exercise 9. *Consider 2 quantum mixed states* ρ *and* σ *which are orthogonal. This means we can write* ρ *and* σ *in their spectral decomposition*

$$\rho = \sum_i p_i |e_i\rangle\langle e_i|$$

$$\sigma = \sum_j q_j |f_j\rangle\langle f_j|$$

where each $p_i, q_j > 0$ *and* $\sum_i p_i = \sum_j q_j = 1$*, and the orthogonality constraint gives* $\forall i, j \ \langle e_i | f_j \rangle = 0$ *(or equivalently* $|e_i\rangle \perp |f_j\rangle$*). Let also* $I_\rho = \sum_i |e_i\rangle\langle e_i|$ *and* $I_\sigma = \sum_j |f_j\rangle\langle f_j|$

1. *Show that* $\rho \cdot \log(\sigma) = \rho \cdot I_\sigma = \mathbf{0}$ *where* $\mathbf{0}$ *is the all* 0 *matrix.*
2. *Let* $\xi = r\rho + (1-r)\sigma$ *with* $r \in [0,1]$*. Show that* $\log(\xi) = \log(r\rho) + \log((1-r)\sigma)$*.*
3. *Let* $r \geq 0$*. Show that* $\log(r\rho) = \log(\rho) + \log(r) I_\rho$*.*
4. *Let* $\xi = r\rho + (1-r)\sigma$ *with* $r \in [0,1]$*. Show that*

$$H(\xi) = H_2(r) + rH(\rho) + (1-r)H(\sigma)$$

where $H_2(r) = -r\log(r) - (1-r)\log(1-r)$*.*

Exercise 10. *Let* $\sigma_{AB} = r|0\rangle\langle 0|_A \otimes \rho_B^0 + (1-r)|1\rangle\langle 1|_A \otimes \rho_B^1$ *be a quantum mixed state on* 2 *registers. Using the previous question, show that*

$$I(A:B)_\sigma = H(r\rho_B^0 + (1-r)\rho_B^1) - \big(rH(\rho_B^0) + (1-r)H(\rho_B^1)\big)$$

Find matrices ρ_B^0, ρ_B^1 *st.* $I(A:B)_\sigma = 0$*. Find others st.* $I(A:B)_\sigma = H_2(r)$*.*