Practice problem set 6

You do not have to hand in these exercises, they are for practicing only.

Problem 1: Six-state BB'84

Consider the BB'84 protocol using 6 states instead of 4. To the initial four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ we add $|\circlearrowright\rangle$ and $|\circlearrowleft\rangle$ (comprising the third basis). The protocol is executed similarly to the original one, but now Alice sends one of six states and Bob measures in one of the three bases.

(a) How many bits are left after Alice and Bob reveal the bases they have chosen.

(b) **Intercept and resend attack** Analyse an intercept-and-resend type of attack where Eve measures Alice's bits in randomly (uniformly and independently) chosen basis and then sends the outcome back to Bob. What is the error rate this attack induces?

(c) **Intercept and resend attack in the standard BB'84** What would be the error rate of the above attack in the original BB'84 protocol?

Problem 2: Entangling attack (Exercise 6.2.1)

Consider the case of a single EPR pair ($n = 1$), and suppose that Eve applies a CNOT on her qubit $|0\rangle_E$, controlled on the qubit B that Alice sends to Bob (Eve then forwards the qubit over to Bob). Compute the resulting joint state ρ_{ABE} . Compute the probability that Alice and Bob choose the same basis $\theta = \tilde{\theta}$ and obtain $x = \tilde{x}$. What is the approximate error rate they get? Is this a good attack?

Problem 3: The matching outcomes test

(a) **Exercise 6.2.2** Suppose given a tripartite state ρ_{ABE}, where A and B are each systems of a single qubit. Show that the probability that a measurement of systems A and B in the standard basis results in matching outcomes is exactly $\mathrm{Tr}\,(\Pi_1 \rho_{AB})$, where

$$\Pi_1 = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|, \text{ and } |\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \quad (1)$$

Similarly, show that if the measurement is performed in the Hadamard basis then the probability of obtaining matching outcomes is $\mathrm{Tr}\,(\Pi_2 \rho_{AB})$, with

$$\Pi_2 = |\Phi^+\rangle\langle\Phi^+| + |\Psi^+\rangle\langle\Psi^+|, \text{ and } |\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \quad (2)$$

(b) **Probability of getting matching outcomes** What is the probability of getting matching outcomes given that Alice and Bob choose the same bases p if Alice and Bob share the state ρ_{AB}.

(c) **Equation (6.6)** Prove the inequality

$$\langle\Phi^+|\rho_{AB}|\Phi^+\rangle \geqslant 2p - 1, \quad (3)$$

where p is the probability of the matching outcomes test succeeding.

(d) **Examples** What is p for the GHZ state ($|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$) and for the W state ($|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$), what are the bounds for the overlap with the Bell $|\Phi^+\rangle$ state.

(e) **Problem 3 from Quiz 6.5** Let Alice and Bob share n qubit pairs in the state $\rho_{AB}^{\otimes n}$, and suppose the matching outcomes test succeeds with probability exactly $p = 0.95$ on each of the n pairs. What is the largest value of n for which the overlap $\langle\Phi^+|^{\otimes n}\rho_{AB}^{\otimes n}|\Phi^+\rangle^{\otimes n}$ is guaranteed to exceed $1/2$?

Problem 4: Min-entropy from the matching outcomes bound

Alice and Bob can extract at most $H_{\min}(X|E)$ bits of randomness to create their key, X is the outcome of Alice's measurement on her qubit. Now we want to connect the conditional min-entropy to the probability that the matching-outcomes test succeeds. We assume that the adversary Eve prepares n identical and uncorrelated copies of the tripartite state $|\psi_{ABE}\rangle$ and sends the qubits A to Alice and B to Bob. Recall that if Alice measures her qubit in the standard basis, and the resulting

post-measurement state on her qubit and Eve's system E is a classical-quantum (cq) state

$$\rho_{XE} = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_E^{Z,0} + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_E^{Z,1}, \tag{4}$$

then the optimal guessing probability $P_{\text{guess}}(X|E)$ such that

$$H_{\min}(X|E) = -\log P_{\text{guess}}(X|E) \tag{5}$$

is given by the Helström measurement, for which

$$P_{\text{guess}}(X|E) = \frac{1}{2} + \frac{1}{4}\|\rho_E^{Z,0} - \rho_E^{Z,1}\|_1. \tag{6}$$

The same reasoning holds for any other choice of Alice's basis, notably the Hadamard basis $\{|+\rangle, |-\rangle\}$. In the BB'84 protocol Alice chooses with probability $1/2$ one of the two bases in which to measure her qubit. If we denote by $P_{\text{guess}}(X|E, \Theta = 0)$ and $P_{\text{guess}}(X|E, \Theta = 1)$ the optimal guessing probabilities for Alice measuring in the standard ($\Theta = 0$) and Hadamard ($\Theta = 1$) bases respectively, the desired lower bound is given by

$$H_{\min}(X|E) = -\log\left[\frac{1}{2}P_{\text{guess}}(X|E, \Theta = 0) + \frac{1}{2}P_{\text{guess}}(X|E, \Theta = 1)\right]. \tag{7}$$

(a) **Problem 1** Suppose Alice and Bob share a pure Bell pair $|\Phi^+\rangle$, uncorrelated with Eve's system: $\rho_{ABE} = |\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_E$. What is $H_{\min}(X|E)$?

(b) **Problem 2** Now consider the general case, where $|\psi_{ABE}\rangle$ is an arbitrary state prepared by Eve. Let p be the probability that this state succeeds in the matching outcomes test, when Alice and Bob both measure in the same basis Θ chosen at random. Give coefficients a, b, c such that

$$p = a\langle\psi_{ABE}|X_A \otimes X_B \otimes \mathbb{1}_E|\psi_{ABE}\rangle + b\langle\psi_{ABE}|Z_A \otimes Z_B \otimes \mathbb{1}_E|\psi_{ABE}\rangle + c, \tag{8}$$

where X,Z are the Pauli observables $X = |+\rangle\langle+| - |-\rangle\langle-|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

(c) **Problem 3** Let p_X (resp. p_Z) be the probability that the state $|\psi_{ABE}\rangle$ passes the matching outcomes test in the Hadamard (resp. computational) basis, so that $p = \frac{1}{2}(p_X + p_Z)$.

By expanding the qubit A in the computational basis, the state $|\psi_{ABE}\rangle$ can be expressed as $|\psi_{ABE}\rangle = |0\rangle_A \otimes |u_0)_{BE} + |1\rangle_A \otimes |u_1)_{BE}$ ($|u)_{BE}$ signifies a not normalized vector in $\mathcal{H}_{BE}$), with $\||u_0)_{BE}\|^2 + \||u_1)_{BE}\|^2 = 1$. Give coefficients a',b' such that

$$\langle\psi_{ABE}|X_A \otimes X_B \otimes \mathbb{1}_E|\psi_{ABE}\rangle = a'\,\mathfrak{Re}((u_0|X_B \otimes \mathbb{1}_E|u_1)) + b'. \tag{9}$$

(d) **Problem 4** Suppose Alice measures her qubit in the computational basis: the post-measurement state on A and E (tracing out B) can be written as $\rho_{AE}^Z = |0\rangle\langle 0|_A \otimes \sigma_E^{Z,0} + |1\rangle\langle 1|_A \otimes \sigma_E^{Z,1}$. Similarly, if Alice measures in the Hadamard basis we may write the post-measurement state as $\rho_{AE}^X = |+\rangle\langle+|_A \otimes \sigma_E^{X,+} + |-\rangle\langle-|_A \otimes \sigma_E^{X,-}$.

Use the previous two questions to determine coefficients α ,β such that

$$2p - 1 \leqslant \alpha F(\sigma_E^{X,+}, \sigma_E^{X,-}) + \beta F(\sigma_E^{Z,0}, \sigma_E^{Z,1}). \tag{10}$$

where F denotes the fidelity.

[Hint: observe that $|u_0\rangle_{BE}$ and $|u_1\rangle_{BE}$ considered in the previous question are purifications of $\sigma_E^{Z,0}$ and $\sigma_E^{Z,1}$ respectively, and use Uhlmann's theorem]

(e) **Problem 5** Recall the inequality $D(\rho, \sigma) \leqslant \sqrt{1 - F(\rho, \sigma)^2}$. Using also the definition of $H_{\min}(X|E)$, what is the best lower bound on $H_{\min}(X|E)$ as a function of p that you can get?