Quantum Complexity Theory

Problem set 3: Entanglement and quantum communication

Show your working. Use the gates, measurements, density matrices and purification from Sheets 1–2. Tensor factors are ordered as labelled; $\mathrm{CNOT}_{A\to B}|x,y\rangle = |x, y\oplus x\rangle$. Operator products act from right to left. Kets may be given up to global phase.

1. The Bell basis

For $a, b \in \{0,1\}$, define

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad |\beta_{ab}\rangle = (I \otimes X^b Z^a)|\Phi^+\rangle.$$

(a) Write out the four $|\beta_{ab}\rangle$ and verify that they form an orthonormal basis.

(b) Let $D = (H \otimes I)\mathrm{CNOT}$, with the first qubit as control. Show that $D|\beta_{ab}\rangle = |a, b\rangle$. How can the four Bell states be distinguished with certainty?
Hint: Write $|\beta_{ab}\rangle = 2^{-1/2}\sum_{x=0}^{1}(-1)^{ax}|x, x\oplus b\rangle$, and apply CNOT first.

(c) Find both one-qubit reduced states. What can a measurement on just one qubit reveal about a, b?

2. Teleportation

Alice holds M in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. Alice and Bob also share $|\Phi^+\rangle_{AB}$: Alice holds A and Bob holds B. Alice applies $\mathrm{CNOT}_{M\to A}$, then H_M.

(a) Using the order M, A, B, show that the resulting state is

$$\frac{1}{2}\sum_{m,n=0}^{1} |m, n\rangle_{MA} \otimes X^n Z^m |\psi\rangle_B.$$

Hint: Expand the initial state, apply the two gates, and group the terms by the values of M, A.

(b) Alice measures M, A in the computational basis and sends her outcomes m, n to Bob. Find their probabilities, Bob's conditional states, and his corrections. State the order of the correction gates.

(c) Before Bob learns m, n, compute his density matrix. Explain why a classical message is needed, and why Alice has not retained a second copy. State the shared resource and the communication used.
Hint: For $\rho = |\psi\rangle\langle\psi|$, average $X^n Z^m \rho Z^m X^n$ over the four outcomes.

3. Superdense coding

Alice and Bob share $|\Phi^+\rangle_{AB}$. To send classical bits a, b, Alice applies $Z^a X^b$ to A (X^b first, then Z^a), and sends qubit A to Bob.

(a) Show that Alice's encoding produces $|\beta_{ab}\rangle$ in the order A, B.
Hint: Apply the gates to the two terms of $|\Phi^+\rangle$, or relabel the summation index x by $x \oplus b$.

(b) Give a decoding circuit and measurement that recover a, b with certainty.
Hint: Bob now holds both qubits; use Problem 1(b).

(c) Find Bob's reduced state before A arrives. Why does local encoding alone communicate no information? Compare the shared resource and communication with teleportation.

4. BB84: preparation and sifting

Assume ideal single qubits and noiseless transmission. In each round Alice chooses independent uniform bits $x, \theta \in \{0,1\}$ and sends $|\psi_{x,\theta}\rangle = H^\theta|x\rangle$ to Bob. Bob independently chooses a uniform bit ϕ and measures in the basis $\{H^\phi|0\rangle, H^\phi|1\rangle\}$, recording the label y. Here basis 0 is the computational basis and basis 1 is the Hadamard basis.

After Bob has measured, they announce their bases and retain only positions with $\theta = \phi$; these are the *sifted positions*. Their public classical channel is authenticated: Eve can read the messages but cannot alter them.

(a) List the four signal states. Compute $\Pr(y \mid x, \theta, \phi)$ when the bases agree and when they differ.
Hint: The measurement amplitude is $\langle y|H^\phi H^\theta|x\rangle$. Use $H^2 = I$.

(b) What fraction of signals is retained on average? For N signals, find the expected sifted length. Show that the sifted bits agree in the honest protocol.
Hint: Condition on Alice's basis.

(c) For fixed θ, average the signal density matrix over x. Can a measurement reveal θ before it is announced? Does this calculation also prove that x is hidden?
Hint: Use $\sum_x |x\rangle\langle x| = I$. Averaging over x and averaging over θ answer different questions.

5. BB84: intercept-resend

Eve intercepts every signal in Problem 4. Independently in each round, she chooses a uniform basis $\varepsilon \in \{0,1\}$, measures in that basis, and resends the state corresponding to her outcome. Alice and Bob sift as before.

(a) Condition on a sifted position. Find Bob's error probability when $\varepsilon = \theta$, and when $\varepsilon \neq \theta$.
Hint: In the second case, Bob measures a state from the other basis.

(b) Deduce the error rate among sifted bits. What is the rate if Eve instead attacks each signal independently with probability f, forwarding the others unchanged?
Hint: Apply the law of total probability, conditional on sifting.

(c) Alice and Bob choose m sifted positions uniformly for testing, reveal both bits there, and abort if any tested pair disagrees. Find the probability that the attack on every signal escapes this test. Why must the disclosed test positions be discarded?
Hint: Errors on different rounds are independent in this attack model; the sample is chosen without using the bit values.

Scope. Problem 5 analyses the specified attack. General BB84 security requires further arguments and classical post-processing, including error correction and privacy amplification.

6. Monogamy of a Bell pair

Let A, B be qubits and E any finite-dimensional system. Suppose the reduced state on AB is the perfect Bell pair $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$.

(a) If the joint state $|\Omega\rangle_{ABE}$ is pure, show that $|\Omega\rangle_{ABE} = |\Phi^+\rangle_{AB} \otimes |e\rangle_E$ for some unit vector $|e\rangle$.

Hint: Expand $|\Omega\rangle = \sum_{a,b} |\beta_{ab}\rangle|e_{ab}\rangle$, where the vectors $|e_{ab}\rangle$ need not be normalised. Compute the diagonal Bell-basis entries of ρ_{AB}.

(b) Now allow ρ_{ABE} to be mixed. Prove that

$$\rho_{ABE} = |\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \rho_E.$$

Hint: Purify ρ_{ABE} using a further system R, and apply (a) with ER in place of E.

(c) Find ρ_{AE}. If A is measured in the computational or Hadamard basis, find each outcome probability and the conditional state of E. Explain why A cannot simultaneously form another Bell pair with a qubit in E.

Hint: Trace out B first. For a rank-one measurement projector P_x on A, use the unnormalised conditional state $\mathrm{Tr}_A[(P_x \otimes I_E)\rho_{AE}(P_x \otimes I_E)]$.

7. Shared correlations and BB84 (extension)

(a) Consider the GHZ state $|G\rangle_{ABE} = (|000\rangle + |111\rangle)/\sqrt{2}$. Find ρ_{AB} and the expectations of $Z \otimes Z$ and $X \otimes X$ on AB. Are A, B entangled? How can Eve nevertheless learn Alice's computational-basis outcome perfectly?

Hint: A mixed bipartite state is *separable* (not entangled) if it is a mixture of product states. Trace out E, then compare what happens when all three qubits are measured in the computational basis.

(b) Let τ_{AB} be any two-qubit density matrix satisfying

$$\mathrm{Tr}[(Z \otimes Z)\tau_{AB}] = \mathrm{Tr}[(X \otimes X)\tau_{AB}] = 1.$$

Show that $\tau_{AB} = |\Phi^+\rangle\langle\Phi^+|$.

Hint: Find the joint eigenvalues of $Z \otimes Z$ and $X \otimes X$ in the Bell basis. Why does expectation 1 for a ± 1-valued observable force support in its $+1$ eigenspace? Use the spectral theorem also when τ_{AB} is mixed.

(c) Alice and Bob share $|\Phi^+\rangle$. Alice chooses a uniform bit θ and measures in $\{H^\theta|0\rangle, H^\theta|1\rangle\}$. Show that her uniform outcome x prepares Bob's qubit in $H^\theta|x\rangle$, a BB84 signal state. Combine (b) with Problem 6 to explain why perfect correlations in both bases leave Eve uncorrelated with x, even after θ is announced. Why is a finite error-free test sample insufficient to establish the exact premise of (b)?

Hint: Compute $(\langle x|H^\theta \otimes I)|\Phi^+\rangle$. For the last question, revisit Problem 5(c).