C&O 781 Topics in Quantum Information

Quantum Information Theory, Error-correction, and Cryptography

University of Waterloo

Fall 2006

Instructors: Debbie Leung and Ashwin Nayak

Assignment 3

Due: Dec. 8, 2006

Question 1. Recall the test performed by Alice and Bob on a $4n$-qubit state ρ shared equally by the two in the Lo-Chau type protocol of Shor and Preskill (PRL, 2000). They choose a random subset of n of the $2n$ pairs of qubits and then Alice and Bob both measure each of the n test pairs of qubits in the $|0\rangle, |1\rangle$ basis (the Z-basis) or in the $|+\rangle, |-\rangle$ basis (the X-basis), where the basis is chosen independently, and uniformly at random for each test pair. Alice and Bob abort the protocol when they find more than $\delta - \epsilon$ fraction of disagreements in their measurement outcomes, for either measurement basis.

Recall that the states $\Psi+$ and $\Psi-$ correspond to bit errors, and $\Phi-$ and $\Psi-$ correspond to phase errors.

For parts (a–c), suppose ρ is a tensor product of $2n$ Bell states, with one half of each Bell state held by Alice and the other half by Bob. You may state, without proof, any "tail bound" from probability theory.

(a) [2 marks] Argue that close to $n/2$ Bell states are measured in each of the two bases: the Z-basis and the X-basis.

(b) [2 marks] Show that with probability exponentially close to 1, Alice and Bob can determine if the fraction of bit or phase errors in ρ is more than δ.

(c) [2 marks] Show that with probability exponentially close to 1, the **remaining** qubits in ρ have fewer than δ fraction of bit and phase errors.

Suppose now that ρ is an arbitrary $4n$-qubit state shared by Alice and Bob. Let Π be the projector on the subspace of $\mathbb{C}^{2^{4n}}$ spanned by tensor products of Bell states with fewer than δn errors, and ρ' the *unnormalized* state of the qubits remaining after the test.

(d) [4 marks] Argue that $\|\rho' - \Pi\rho'\Pi\|_{\mathrm{tr}}$ is exponentially small. In other words, the residual state when the test passes is close to a state in which there are fewer than δn bit and phase errors.

Question 2. [5 marks] Suppose Alice has as input a (classical) random variable X, and engages in a quantum communication protocol with Bob. Suppose Q denotes Bob's part of the joint quantum state held by Alice and Bob at some point in the protocol.

(a) If at this point, Alice sends a qubit, and Q' denotes Bob's new state, show that $I(X : Q') \leq I(X : Q) + 2$.

(b) Next, if Bob sends one qubit to Alice, and Q'' denotes his new state, show that $I(X : Q'') \leq I(X : Q')$.

Question 3. (a) [2 marks] Verify that $I(X : YZ) = I(XY : Z) + I(X : Y) - I(Y : Z)$.

(b) [3 marks] Suppose Q is a quantum encoding of n uniformly random bits $X = X_1 X_2 \cdots X_n$. Show that

$$I(X:Q) \quad \geq \quad \sum_{i=1}^{n} I(X_i:Q).$$

Question 4. [8 marks] Exercise 11.19 in Nielsen and Chuang, 4 marks for each part.

Question 5. [12 marks]

Consider a quantum channel $\mathcal{N}$ from Alice to Bob, and its isometric extension U (the isometry mapping each input of the channel to a bipartite state shared by Bob and Eve). Let A, B, E label their respective systems. Appending the isometric extension U with a partial trace of B results in some "conjugate channel" $\mathcal{N}^c$ from Alice to Eve (this is unique up to a final unitary on E).

$\mathcal{N}$ is called degradable if $\exists \mathcal{D}$ a TCP map (the degrading map) such that $\mathcal{D} \circ \mathcal{N} = \mathcal{N}^c$. $\mathcal{N}$ is called anti-degradable if $\exists \mathcal{A}$ a TCP map such that $\mathcal{A} \circ \mathcal{N}^c = \mathcal{N}$.

(a) [4 marks] Prove that if $\mathcal{N}$ is antidegradable, $Q(\mathcal{N}) = 0$.

(b) [4 marks] Show that the amplitude damping channel (eqs. (8.107)-(8.108) in Nielsen and Chuang) is degradable and antidegradable for $\gamma \leq 0.5$ and $\gamma \geq 0.5$.

(c) [4 marks extra credit] Show that degradable channels have single letter expression for quantum capacity.

(d) [4 marks] Find the quantum capacity of the amplitude damping channel as a function of γ. (Hint, the optimal input in the single letter optimization has Schmidt basis being the computation basis.)