COMP 598 Winter 2011
Homework 5

Due by 5pm on Monday 11 April 2011.

First part: Exercises 15.5.4, 19.3.1, 19.3.2, 19.4.2, 19.4.5, 20.2.1, 20.7.1, 21.1.1, 21.4.1 in *From Classical to Quantum Shannon Theory*

Second part: The below exercises

1. There is a famous classical protocol known as Slepian-Wolf compression. The protocol involves two spatially separated senders, who are given the sequences x^n and y^n, respectively, chosen according to many realizations of the joint distribution $p_{X,Y}(x,y)$. A noiseless classical channel connects each sender to a common receiver. The goal of the compression protocol is for the two spatially separated senders to compress their sequences and transmit them over as few uses of the two noiseless classical channels as possible.

   (a) Describe a scheme for them to compress their sequences down to a rate equal to the Shannon entropies $H(X)$ and $H(Y)$, such that the common receiver can recover the sequences x^n and y^n that the two senders transmit. That is, determine a scheme such that the sum rate $R_1 + R_2 = H(X) + H(Y)$.

   (b) Surprisingly, it turns out that they can do quite a bit better than the scheme in part (a). The famous Slepian-Wolf protocol shows how they can compress down to the joint entropy $H(X,Y)$. That is, there exists a scheme such that the sum rate $R_1 + R_2 = H(X,Y)$. Describe how the Slepian-Wolf protocol works. You are welcome to consult pages 11-1 to 11-19 of `arXiv:1001.3404`. (It might be good to exploit the hashing technique presented in el Gamal's notes because we will be extending this to the quantum domain.)

   (c) We will now consider a particular quantum generalization of the above setting. Alice and Bob share a classical-quantum state of the following form:

   $$\sum_{x^n \in \mathcal{X}^n} p_{X^n}(x^n) |x^n\rangle \langle x^n|^{X^n} \otimes \rho_{x^n}^{B^n}, \tag{1}$$

   where Alice holds the X^n system and Bob holds the B^n system. The above state is equivalent to many copies of the c-q state

   $$\rho^{XB} \equiv \sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|^X \otimes \rho_x^B.$$

   Determine a scheme where Alice can send $nH(X)_\rho$ classical bits to a receiver Charlie, and Bob can send $nH(B)_\rho$ qubits to Charlie, such that Charlie can recover the state in (1) with high fidelity in the limit of large block length.

   (d) We will show that it is possible to do better than the scheme suggested above. Suppose that Bob first sends his system to Charlie with $nH(B)_\rho$ qubits, using the scheme suggested in the previous part. The state shared between Alice and Charlie

is then close in trace distance to the state in (1). Devise a coding scheme similar to the random hashing method outlined on page 11-12 of `arXiv:1001.3404`, in which Alice hashes the sequences in her system with some hash function. Alice then passes the hashed value along to Charlie. Along with the hashing scheme, construct a POVM, conditional on the value of the hash, for Charlie to decode the sequence x^n corresponding to the hashed value. You might find the ideas of conditionally typical projectors and the proof of Lemma 3 of arXiv:1008.0452 to be helpful here.

(e) Show that your scheme in the previous section works well, in the sense that the error probability is small. You can do this by taking the expectation of the error probability with respect to the hash function and the choice of the sequence x^n. What is the minimum number of bits that Alice can hash her sequences x^n down to, such that Bob can still reliably recover the sequences?

(f) Using the POVM, construct a quantum instrument that acts on Alice's transmitted hash and Charlie's system, such that the state after the instrument acts is close in trace distance to the state in (1).

2. You will prove the HSW coding theorem without the use of conditionally typical projectors. The method will be akin to the way that we proved the entanglement-assisted classical capacity theorem in Section 20.4.

(a) Consider the maximally correlated state $\overline{\Phi}^{AB}$:

$$\overline{\Phi}^{AB} \equiv \frac{1}{D} \sum_{i=0}^{D-1} |i\rangle \langle i|^A \otimes |i\rangle \langle i|^B .$$

Show that the generalized shift operator $X(j)$ acting on Alice's system is the same as the opposite shift acting on Bob's system:

$$X^A(j)\, \overline{\Phi}^{AB} \left(X^A(j)\right)^\dagger = X^B(-j)\, \overline{\Phi}^{AB} \left(X^B(-j)\right)^\dagger .$$

This is the classical analog of the transpose trick that holds for Bell states: $M^A |\Phi\rangle^{AB} = \left(M^T\right)^B |\Phi\rangle^{AB}$.

(b) Consider an arbitrary common randomness state:

$$\overline{\varphi}^{AB} \equiv \sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|^A \otimes |x\rangle \langle x|^B .$$

Taking many copies of the above common randomness state gives the following IID state:

$$\left(\overline{\varphi}^{AB}\right)^{\otimes n} \equiv \sum_{x^n \in \mathcal{X}^n} p_{X^n}(x^n) |x^n\rangle \langle x^n|^{A^n} \otimes |x^n\rangle \langle x^n|^{B^n} .$$

Show that each local Hilbert space of Alice and Bob naturally decomposes into a direct sum of type class subspaces, similar to the decomposition in Section 20.4. Find an operator $X^{A^n}(s)$ acting on system A^n, with the property that Alice acting on $\left(\overline{\varphi}^{AB}\right)^{\otimes n}$ with $X^{A^n}(s)$ is the same as Bob acting on $\left(\overline{\varphi}^{AB}\right)^{\otimes n}$ with $\left(X^{B^n}(s)\right)^\dagger$:

$$X^{A^n}(s) \left(\overline{\varphi}^{AB}\right)^{\otimes n} \left(X^{A^n}(s)\right)^\dagger = \left(X^{B^n}(s)\right)^\dagger \left(\overline{\varphi}^{AB}\right)^{\otimes n} \left(X^{B^n}(s)\right) .$$

(c) Alice and Bob can exploit the above common randomness state to make an HSW code for sending classical information over a classical-quantum channel. Suppose that the following classical-quantum channel connects Alice to Bob:

$$x \rightarrow \rho_x.$$

The channel takes a classical input x and prepares a quantum output ρ_x for Bob. Thus, if Alice inputs her half of the common randomness state $\overline{\varphi}^{AB}$, Bob holds both systems of the following state:

$$\sum_{x \in \mathcal{X}} p_X(x) \rho_x \otimes |x\rangle \langle x|^B.$$

Devise an ensemble from which Alice and Bob can select a random code, and devise a decoding POVM for Bob to detect the codewords. The scheme should exploit the shifting operators in the previous part and typical projectors of the above state (the code should be similar to that in the direct coding part of the entanglement-assisted classical capacity theorem in Section 20.4).

(d) Show that the four conditions of the Packing Lemma hold for your ensemble and the projectors that form your decoding POVM. Conclude that there exists a good code that can achieve the Holevo information $I(X;B)$ with respect to the following state:

$$\sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|^X \otimes \rho_x^B.$$

(e) Is the common randomness really necessary? Argue that it is not. Also, show how they can use the above coding scheme in order to achieve the Holevo information $\chi(\mathcal{N})$ of an arbitrary quantum channel $\mathcal{N}$, where

$$\chi(\mathcal{N}) = \max I(X;B)_\sigma,$$

where

$$\sigma^{XB} \equiv \sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|^X \otimes \mathcal{N}(\rho_x).$$