Q. Inf. Science 3 (8.S372 / 18.S996) — Fall 2020

Assignment 4

Due: **Friday**, *Oct 2, 2020 at* ***5pm*** on canvas.

1. **Compression with side information.**

   (a) *Conditionally typical set.* For a probability distribution p_{XY} define $J^n_{p,\delta}$ to be the jointly typical set: formally $J^n_{p,\delta} := T^n_{p,\delta} \cap (T^n_{p_X,\delta} \times T^n_{p_Y,\delta})$. Given y^n, define the conditionally typical set $J(y^n) := J^n_{p,\delta}(y^n)$ by

   $$J(y^n) = \left\{x^n \in X^n : (x^n, y^n) \in J^n_{p,\delta}\right\}. \tag{1}$$

   Observe that if $y^n \notin T^n_{p_Y,\delta}$ then $J(y^n)$ is empty. If $y^n \in T^n_{p_Y,\delta}$ then what bounds can you place on $p^n(x^n|y^n)$ for $x^n \in J(y^n)$? Prove that

   $$|J(y^n)| \leq \exp(n(H(X|Y) + 2\delta)). \tag{2}$$

   (b) Let $(X^n, Y^n) \sim p^n_{XY}$, i.e. each (X_i, Y_i) is drawn independently from p_{XY}. Suppose that Alice knows X^n and Y^n, Bob holds Y^n and Alice wishes to transmit X^n to Bob. Shannon's noiseless coding theorem tells her how to do this using $\approx nH(X)$ bits, but this would not take advantage of the correlations between X^n and Y^n. Show that she can transmit X^n to Bob using $n(H(X|Y) + \delta)$ bits and error ϵ, with $\epsilon, \delta \to 0$ as $n \to \infty$. (Note: the δ in (a) might not be the same δ as the one here.)

   (c) Now suppose that Alice knows only X^n and Bob knows Y^n. This is significantly more challenging than the situation in (b). Suppose that Alice uses a random codebook as in Shannon's noisy coding theorem. To compress to rate R, Alice uses a random function $E : X^n \to [2^{nR}] := \{1, 2, \ldots, 2^{nR}\}$, meaning that each $E(x^n)$ is chosen independently and uniformly from $[2^{nR}]$. As in the channel coding theorem, E is chosen randomly and then fixed and can be assumed to be known by both parties.

   Given message m, Bob decodes by choosing the unique x^n such that $E(x^n) = m$ and $(x^n, Y^n) \in J$, i.e. in the set $E^{-1}(m) \cap J(Y^n)$. If this x^n either doesn't exist or isn't unique, then he declares failure. Let WRONG be the event where

   $$E^{-1}(m) \cap J(Y^n) \tag{3}$$

   contains a string x^n that is not equal to the correct string X^n. Prove that $p^n(\text{WRONG}) \to 0$ if $R > H(X|Y) + 3\delta$ as $n \to \infty$.

   (d) What other errors are possible? By bounding their probabilities show that the coding strategy in (c) can work with error approaching 0 as $n \to \infty$ for any $R > H(X|Y)$.

2. **Feedback-assisted capacity** The proof in lecture of Shannon's noisy coding theorem

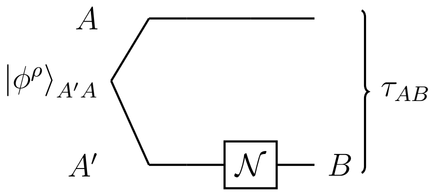
did not allow Bob to send messages back to Alice, an ability called "feedback." Suppose that after receiving each channel output Y_i, Bob can noiselessly send Alice an arbitrary message. Modify the proof in lecture to show that the same converse still holds. You do not need to repeat the parts of the proof that are unchanged. As a hint, try to show that $I(M;Y^n) \leq H(Y^n) - \sum_{i=1}^n H(Y_i|X_i)$.

3. **Entanglement-assisted capacity** For classical channels, shared randomness does not help the capacity. One way to see this is that feedback can be used to share randomness, and feedback does not help the capacity. But for quantum channels, we know that entanglement between sender and receiver can improve the classical capacity, as seen in the example of super-dense coding. In fact, free entanglement dramatically simplifies the quantum capacity. Let $C_E(\mathcal{N})$ denote the asymptotic rate that $\mathcal{N}$ can send classical bits when assisted by unlimited EPR pairs between sender and receiver. It turns out that

$$C_E(\mathcal{N}) = \max_\rho I(A:B)_\tau \tag{4}$$

where ρ is maximized over all density matrices on A, $\phi^\rho_{AA'}$ is a purification of ρ, and

$$\tau_{AB} = (\mathrm{id}_A \otimes \mathcal{N}_{A'\to B})(\phi^\rho_{AA'}) \tag{5}$$



(a) Consider the special case in which the maximum in (4) is achieved by $\rho = I/d$, where $d = |A|$. Define the generalized Paulis (also called Weyl-Heisenberg operators) by

$$\sigma_{xy} := \sum_{z=0}^{d-1} \omega^{zy} |z+x\rangle \langle z| , \tag{6}$$

where $x, y \in \{0, 1, \ldots, d-1\}$, $z + x$ is defined mod d and $\omega := e^{2\pi i/d}$. Show that

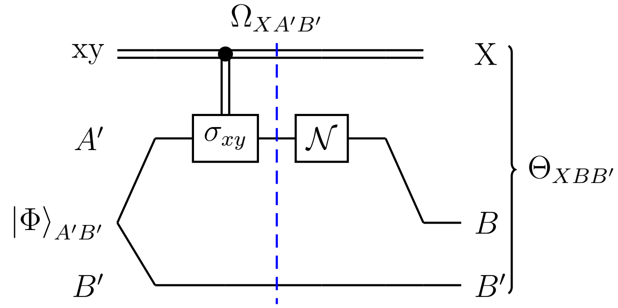
$$\mathcal{E}(M) := \frac{1}{d^2} \sum_{x,y} \sigma_{x,y} M \sigma^\dagger_{x,y} = \frac{I}{d} \mathrm{tr}[M], \tag{7}$$

for any matrix M.

Consider the following coding scheme for Alice. She chooses x, y uniformly randomly, applies σ_{xy} to her half of an entangled state

$$|\Phi\rangle_{A'B'} := \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle_{A'} \otimes |i\rangle_{B'} \tag{8}$$

$|\Phi\rangle_{A'B'}$ and then sends system A' through the channel. We can express the resulting ensemble as a single state with system X containing Alice's encoding and systems B and B' representing Bob's channel output and piece of the shared entanglement. This is depicted in the following circuit diagram.



$$\Omega_{XA'B'} := \frac{1}{d^2}\sum_{xy} |xy\rangle\langle xy|_X \otimes (\sigma_{xy}\otimes I)\Phi_{A'B'}(\sigma_{xy}\otimes I)^\dagger \tag{9}$$

$$\Theta_{XBB'} := (\mathcal{N}_{A'\to B}\otimes \mathrm{id}_{B'X})(\Omega) \tag{10}$$

Compute $I(X : BB')_\Theta$ in terms of $I(A : B)_\tau$. Using the HSW theorem, what can you then conclude about C_E? [Hint: Recall that $(X\otimes I)\,|\Phi\rangle = (I\otimes X^T)\,|\Phi\rangle$.]

(b) [Optional.] Assume now that (4) has been shown to be true. Prove that the capacity is additive, i.e. that

$$C_E(\mathcal{N}_1\otimes\mathcal{N}_2) = C_E(\mathcal{N}_1) + C_E(\mathcal{N}_2). \tag{11}$$