Q. Inf. Science 3 (8.372 / 18.S996) — Fall 2022

Assignment 6

Due: **Friday***, Oct 22, 2022 at* ***5pm*** on gradescope.

1. **Fano's inequality**

   Let M and $\hat{M}$ be two random variables defined over an alphabet of size d such that $\Pr\left[M \neq \hat{M}\right] \leq \epsilon$. Prove that

$$H(\hat{M}|M) \leq H_2(\epsilon) + \epsilon \log(d). \tag{1}$$

   As a hint, you may want to define a random variable E that is 1 if $M = \hat{M}$ and is 0 if $M \neq \hat{M}$, and then expand the conditional entropy $H(EM|\hat{M})$ in two ways as

$$\begin{aligned} H(E\hat{M}|M) &= H(\hat{M}|M) + H(E|M\hat{M}) &(2)\\ &= H(E|M) + H(\hat{M}|EM) &(3) \end{aligned}$$

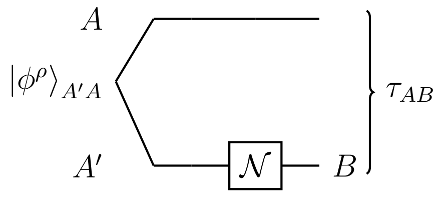
2. **Feedback-assisted capacity** The proof in lecture of Shannon's noisy coding theorem did not allow Bob to send messages back to Alice, an ability called "feedback." Suppose that after receiving each channel output Y_i, Bob can noiselessly send Alice an arbitrary message. Modify the proof in lecture 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 $\mathcal{N} : A' \to B$ can send classical bits when assisted by unlimited EPR pairs between sender and receiver. It turns out that

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

   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

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

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

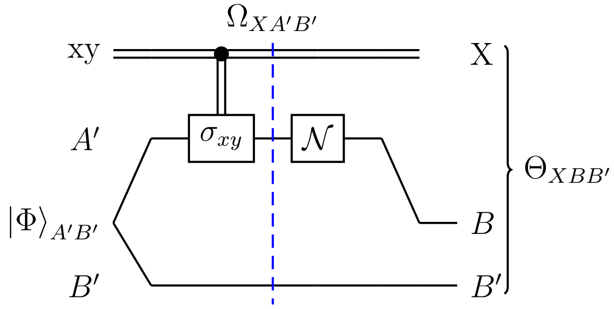
$$\mathcal{E}(M) := \frac{1}{d^2} \sum_{x,y} \sigma_{x,y} M \sigma_{x,y}^\dagger = \frac{I}{d} \operatorname{tr}[M], \tag{7}$$

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

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

$\left|\Phi\right\rangle_{A'B'}$ 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 $(X \otimes I) \left|\Phi\right\rangle = (I \otimes X^T) \left|\Phi\right\rangle$.]

(b) *Input concavity.* Show that $C_E(\mathcal{N}, \rho)$ is independent of the choice of purification ϕ^ρ. Show that $C_E(\mathcal{N}, \rho)$ is concave in the input ρ. [Hint: purify $\sum_x p(x) \left|x\right\rangle \left\langle x\right| \otimes \phi^{\rho_x}$.]

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

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