EE/Stats 376A: Homework 6

Due on **Friday March 3, 5 pm**

1. **Erasure channels.**
   Problem 7.27 of CT.

2. **Random questions.**
   Problem 7.32 of CT.

3. **Linear Random Codes.**
   As discussed in Lecture 11, random linear codes are obtained by randomly choosing the generator matrix such that each entry of the matrix is equally likely to be 0 or 1 and the entries are chosen independently. Show that linear random codes can achieve the capacity of the binary symmetric channel BSC. (Hint: Make sure you first understand the argument for (completely) random codes used in Lecture 11. What are the differences and similarities between (completely) random codes and linear random codes?)

4. **Optimal Broadcasting.**

   (a) Suppose X is a real-valued discrete random variable. Argue that there exists a value a such that $Pr(X = a) \neq 0$ and $a \leq E[X]$.

   (b) Consider a discrete memoryless channel with transition probability $p(y|x)$. In class, we showed that for a fixed input distribution $p(x)$, one can construct for each n a random code $\mathbf{C_n}$ of block length n and rate R such that

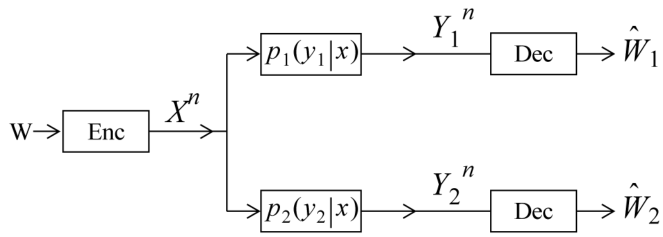
   $$\mathrm{E}[P_e^{(n)}(\mathbf{C_n})] \to 0$$

   as $n \to \infty$ as long as $R < I(X;Y)$. Here $P_e^{(n)}(C_n)$ is the probability of error using the code C_n and jointly typical decoding, and the expectation is over the random choice of the code. Using part (a)or otherwise, show that this result implies that there exists a sequence of (non-random) codes $\{C_n^*\}$ of rate R such that $P_e^{(n)}(C_n^*) \to 0$ as $n \to 0$.

   (c) Now suppose one wants to broadcast a message W to two receivers, as shown in the figure below. The transmitter sends X^n. Receiver i sees the output Y_i^n after passing X^n through a discrete memoryless channel $p_i(y_i|x)$, $i = 1, 2$. Each receiver decodes the message W based on its own received signal only . Show that as long as

   $$R < \max_{p(x)} \min(I(X;Y_1), I(X;Y_2)),$$

   there exists a sequence of rate R, block length n (non-random) codes $\{C_n^*\}$ such that each receiver can decode the message reliably, i.e. the probability of error for each receiver goes to zero as the block length n grows.



(d) Prove that if

$$R > \max_{p(x)} \min(I(X;Y_1), I(X;Y_2)),$$

then for any code at least one of the receivers will have a probability of error that is bounded away from zero no matter how large the block length n is.

5. **Polar code: encoding.**
Recall that for a polar code of block length $n = 2^k$, the matrix A_k is the transformation from $\mathbf{U} = [U_1, \dots, U_n]^t$ to the channel inputs $\mathbf{X} = [X_1, \dots, X_n]^t$. Here, $U_1, U_2, \dots, U_n$ is the decoding order.

   (a) Compute A_k for $k = 1, 2, 3$.

   (b) Prove that for $k \geq 2$:

$$A_k = \begin{bmatrix} A_{k-1} & A_{k-1} \\ 0 & A_{k-1} \end{bmatrix}.$$

6. **Polar codes: polarization.**
Consider the use of a polar code on a binary erasure channel P of erasure probability p.

   (a) Let $n = 8$ be the block length. Compute the capacities of the 8 transformed channels P^{+++}, P^{++-}, etc.

   (b) For each $n = 2^k$, F_n is the empirical cumulative distribution function of the transformed channel capacities, i.e. for $x \in [0, 1]$,

   $F_n(x) :=$ fraction of transformed channels with capacity less than or equal to x.

   What does the polarization theorem say about the function F_n as $n \to \infty$? Compute F_n numerically for large enough n to see the polarization effect, and plot F_n for several representative values of n to demonstrate the effect.