More Exercises

Problem 1 (AEP)

In the following, we consider an i.i.d. sequence $x^n = (X_1, X_2, \ldots, X_n)$, where $X_i \sim \text{Br}(\theta)$. Furthermore, we define the function $L(x^n)$ to be the Hamming weight of x^n, i.e., the number of ones in the sequence x^n.
For every $\theta > 0$, let $A_\epsilon^{(n)}$ denote the typical set as defined in class and in the textbook.

(a) If $\theta = 1/2$, for which values of $\epsilon > 0$ is the all-zero sequence a typical sequence?

(b) For general θ, show that knowledge of the Hamming weight $L(x^n)$ of a sequence x^n is sufficient to determine whether x^n is a member of the typical set.

(c) For general θ, and n arbitrarily large, are the typical sequences "approximately equiprobable?" Note that we say that the elements of a set of sequences are approximately equiprobable if the ratio of the probabilities of the most likely and least likely sequences in the set tends to a constant as n grows.

(d) For $\theta > 0$, $0 \leq p \leq 1$, we define the following set

$$C^{(n)}(\alpha, p) = \{x^n \in \mathcal{X}^n : pn - n\alpha \leq L(x^n) \leq pn + n\alpha\},$$

where $\mathcal{X} = \{0, 1\}$. For $\theta > 1/2$, is it possible to adjust the value of α and p so that $A_\epsilon^{(n)} = C^{(n)}(\alpha, p)$?

Problem 2 (Random 20 questions)

Let X be uniformly distributed over $\{1, \ldots, m\}$. Assume that $m = 2^n$. We ask random questions: Is $X \in S_1$? is $X \in S_2$?... until only one integer remains. All 2^m subsets S of $\{1, \ldots, m\}$ are equally likely to be asked.

(a) Without loss of generality, suppose that $X = 1$ is the random object. What is the probability that object 2 yields the same answers for the k questions as does object 1?

(b) What is the expected number of objects in $\{2, \ldots, m\}$ that have the same answers to the questions as does the correct object 1?

(c) Suppose that we ask $n + \sqrt{n}$ random questions. What is the expected number of wrong objects agreeing with the answers?

(d) Use Markov's inequality $\Pr\{X \geq t\mu\} \leq \frac{1}{t}$, to show that the probability of error (one or more wrong objects remaining) goes to zero as $n \to \infty$.

Problem 3 (Secret Sharing)

For a given set of participants $\mathcal{P}$, and a collection $\mathcal{A}$ of subsets of $\mathcal{P}$, a secret sharing scheme is a random variable S and a family of random variables $\{X_p : p \in \mathcal{P}\}$ such that for all $A \in \mathcal{A}$,

$$H(S|X_A) = 0,$$

and for all $B \notin \mathcal{A}$

$$H(S|X_B) = H(S).$$

The set $\mathcal{A}$ specifies the *access structure* of the scheme: For a subset A of $\mathcal{P}$, by pooling their shares, if $A \in \mathcal{A}$, the participants in A can reconstruct S, otherwise, hey can know nothing about S.

(a) Prove that for $A, B \subset \mathcal{P}$, if $B \notin \mathcal{A}$ and $A \cup B \in \mathcal{A}$, then

$$H(X_A|X_B) = H(S) + H(X_A|X_B, S).$$

(b) Prove that if $B \in \mathcal{A}$, then

$$H(X_A|X_B) = H(X_A|X_B, S).$$

(c) Prove that for $A, B, C \subset \mathcal{P}$ such that $A \cup C \in \mathcal{A}$, $B \cup C \in \mathcal{A}$, and $C \notin \mathcal{A}$, then

$$I(X_A; X_B|X_C) \geq H(S).$$

Problem 4

In this question we find two inequalities relating probability of error and entropy.

(a) Show that if X and X' are i.i.d. with entropy $H(X)$,

$$Pr(X = X') \geq 2^{-H(X)},$$

with equality if and only if X has a uniform distribution.

(b) Show that if X and X' are independent random variables from $p(x)$ and $q(x)$ respectively, then

$$P(X = X') \geq 2^{-H(p)-D(p\|q)},$$
$$P(X = X') \geq 2^{-H(q)-D(q\|p)}.$$

Problem 5 (Entropy Rate)

(a) Consider a stationary stochastic process $X_1, \ldots, X_n$, and let $Y_1, \ldots, Y_n$ be defined by

$$Y_i = \Phi(X_i),\ i = 1, 2, \cdots$$

for some function Φ. Prove that $H(\mathcal{Y}) \leq H(\mathcal{X})$.

(b) What is the relationship between the entropy rates $H(\mathcal{Z})$ and $H(\mathcal{X})$ if

$$Z_i = \Psi(X_i, X_{i+1}),\ i = 1, 2, \cdots$$

for some function Ψ?

(c) What is the relationship between the entropy rates $H(\mathcal{Z})$ and $H(\mathcal{X})$ if

$$Z_i = \Psi(X_i, \ldots, X_{i+l}),\ i = 1, 2, \cdots$$

for a fixed l and some function Ψ?

(d) Consider a second order Markov process over alphabet $\{0, 1\}$. Note that in a second order Markov process, X_n only depends on the two previous values X_{n-1} and X_{n-2} (compare it with a Markov Chain in which X_n only depends on X_{n-1}). Specifically, assume that the process we are considering is realized as follows:

$$X_n = \begin{cases} \text{Br}(0.5) & X_{n-1} = X_{n-2} \\ \text{Br}(0.9) & \text{otherwise} \end{cases}$$

Find the entropy rate $H(\mathcal{X})$.
Hint: Define $Z_n = (X_n, X_{n+1})$ and argue that $\{Z_n\}$ makes a first order Markov process (a Markov Chain). Then find the entropy rate $H(\mathcal{Z})$ and relate it to $H(\mathcal{X})$.