Problem 1  

Csiszár’s Identity

Show that for any pair of random vectors \( (A_1, \ldots, A_n), (B_1, \ldots, B_n) \)

\[
\sum_{i=1}^{n} \left( I(A_{i+1}^n; B_i | B^{i-1}) - I(B^{i-1}; A_i | A_{i+1}^n) \right) = 0,
\]

where we use the shorthand notation \( A_j = (A_1, \ldots, A_j), A_k^j = (A_j, A_{j+1}, \ldots, A_k) \) for \( j \leq k \), and \( B^0 \) and \( A_{n+1}^n \) are defined to be deterministic.

Problem 2

Entropy is Submodular

Let \( \Omega \) be a set, and denote by \( 2^\Omega \) the power set of \( \Omega \). A set function \( f : 2^\Omega \to \mathbb{R} \) is called submodular if it satisfies for all \( S, T \subseteq \Omega \)

\[
f(S) + f(T) \geq f(S \cap T) + f(S \cup T).
\]

For a given \( n \in \mathbb{N} \), let \( \Omega = \{X_1, X_2, \ldots, X_n\} \) be a set of chance variables. In this case, \( 2^\Omega \) contains all collections of chance variables from the set \( \Omega \). Let \( H : 2^\Omega \to \mathbb{R}^+_0 \) be the set function \( W \mapsto H(W) \), where \( H(W) \) is the entropy of the collection \( W \) of chance variables. Show that \( H \) is submodular.

Problem 3

Pure Randomness and Bent Coins

Let \( X_1, X_2, \ldots, X_n \) denote the outcomes of independent flips of a bent coin. Thus, for \( i = 1, \ldots, n \),

\[
\Pr[X_i = 1] = p \quad \text{and} \quad \Pr[X_i = 0] = 1 - p,
\]

where \( p \) is unknown. We wish to obtain a sequence \( Z_1, Z_2, \ldots, Z_K \) of fair coin flips from \( X_1, X_2, \ldots, X_n \). Toward this end let

\[
f : \mathbb{X}^n \to \{0, 1\}^*
\]

(where \( \{0, 1\}^* = \{\Lambda, 0, 1, 00, 01, \ldots\} \) is the set of all finite length binary sequences and where \( \Lambda \) denotes the null string) be a mapping \( f(X_1, X_2, \ldots, X_n) = (Z_1, Z_2, \ldots, Z_K) \), such that \( Z_i \sim \text{Bernoulli}(1/2) \), where \( K \) possibly depends on \( (X_1, \ldots, X_n) \). For the sequence \( Z_1, Z_2, \ldots, Z_K \) to correspond to fair coin flips, the map \( f \) from bent coin flips to fair flips must have the property that all \( 2^k \) sequences \( (Z_1, Z_2, \ldots, Z_k) \) of a given length \( k (k = 1, 2, \ldots) \) have equal probability (possibly 0). For example, for \( n = 2 \), the map \( f(01) = 0, f(10) = 1, f(00) = f(11) = \Lambda \) (the null string), has the property that \( \Pr[Z_1 = 1 | K = 1] = \Pr[Z_1 = 0 | K = 1] = \frac{1}{2} \).
a) Justify why the following (in)equalities hold for every such \( f \) (the used units are bits):

\[
\begin{align*}
nH_b(p) & \overset{\text{i)}}{=} H(X_1, \ldots, X_n) \overset{\text{ii)}}{\geq} H(Z_1, Z_2, \ldots, Z_K, K) \overset{\text{iii)}}{=} H(K) + H(Z_1, Z_2, \ldots, Z_K | K) \\
& \overset{\text{iv)}}{=} H(K) + E[K] \overset{\text{v)}}{\geq} E[K].
\end{align*}
\]

Thus, on average, no more than \( nH_b(p) \) fair coin tosses can be derived from \((X_1, \ldots, X_n)\).

b) Exhibit a good map \( f \) on sequences of length \( n = 4 \).

Problem 4

\textit{Conditional vs. Unconditional Mutual Information}

Give examples of joint random variables \( X, Y, \) and \( Z \) such that

a) \( I(X; Y | Z) < I(X; Y) \),

b) \( I(X; Y | Z) > I(X; Y) \).

Problem 5

\textit{Classes of Codes}

Consider the code \( \{0, 01\} \). Justify your answers to the following questions.

a) Is it instantaneous?

b) Is it uniquely decodable?

c) Is it nonsingular?