Problem 1: **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 $S, T \in 2^\Omega$

$$f(S) + f(T) \geq f(S \cap T) + f(S \cup T).$$

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 $H: 2^\Omega \to \mathbb{R}_+^+$ 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 2: **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

$$f: X^n \to \{0, 1\}^*$$

(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):

$$n \text{H}_b(p) \overset{(i)}{=} H(X_1, \ldots, X_n) \overset{(ii)}{=} H(Z_1, Z_2, \ldots, Z_K, K) \overset{(iii)}{=} H(K) + H(Z_1, Z_2, \ldots, Z_K|K) \overset{(iv)}{=} H(K) + E[K] \overset{(v)}{=} \mathbb{E}[K].$$

Thus, on average, no more than $n \text{H}_b(p)$ fair coin tosses can be derived from $(X_1, \ldots, X_n)$.

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

© Amos Lapidoth, 2014/2015
Problem 3

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 4

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?

Problem 5

Slackness in Kraft’s Inequality

Let $l_1, l_2, \ldots, l_m$ denote the codeword lengths of an instantaneous code of alphabet $D = \{0, 1, \ldots, D-1\}$.

a) For $D = 2$, i.e. binary codes, show that if

$$\sum_{i=1}^{m} 2^{-l_i} < 1,$$

then there exists another instantaneous binary code that is deterministically better in the sense that for each source symbol the corresponding codeword is no longer than the original code, and that for at least one symbol it is shorter.

b) For $D > 2$, (e.g. ternary codes, quaternary codes, ...) with

$$\sum_{i=1}^{m} D^{-l_i} < 1,$$

does the same conclusion hold?