



Exercise 3 of October 5, 2016

<http://www.isi.ee.ethz.ch/teaching/courses/it1/>

Problem 1

Csiszár's Identity

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

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

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

Problem 2

Entropy is Submodular

Let Ω be a set, and denote by 2^Ω the power set of Ω . A set function $f: 2^\Omega \rightarrow \mathbb{R}$ is called *submodular* if it satisfies for all $\mathcal{S}, \mathcal{T} \in 2^\Omega$

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

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

Problem 3

Pure Randomness and Bent Coins

Let X_1, X_2, \dots, X_n denote the outcomes of independent flips of a *bent* coin. Thus, for $i = 1, \dots, n$,

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

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

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

(where $\{0, 1\}^* = \{\Lambda, 0, 1, 00, 01, \dots\}$ is the set of all finite length binary sequences and where Λ denotes the *null string*) be a mapping $f(X_1, X_2, \dots, X_n) = (Z_1, Z_2, \dots, Z_K)$, such that $Z_i \sim \text{Bernoulli}(1/2)$, where K possibly depends on (X_1, \dots, X_n) . For the sequence Z_1, Z_2, \dots, 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, \dots, Z_k) of a given length k ($k = 1, 2, \dots$) 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):

$$\begin{aligned} nH_b(p) &\stackrel{\text{i)}}{=} H(X_1, \dots, X_n) \stackrel{\text{ii)}}{\geq} H(Z_1, Z_2, \dots, Z_K, K) \stackrel{\text{iii)}}{=} H(K) + H(Z_1, Z_2, \dots, Z_K|K) \\ &\stackrel{\text{iv)}}{=} H(K) + \mathbb{E}[K] \stackrel{\text{v)}}{\geq} \mathbb{E}[K]. \end{aligned}$$

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

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

Problem 4

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

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 6

Slackness in Kraft's Inequality

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

- 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?