Information theory: assignment 3

1. Let $X_1, \ldots, X_n$ be n jointly distributed random variables. Define $f : 2^{[n]} \to \mathbb{R}$ by $f(S) = I(X_S; X_{[n]\setminus S})$. Prove that f is sub-modular.

2. For a probability distribution p on $[n]$, the *min-entropy* of p is

$$H_\infty(p) = \min\{\log(1/p(x)) : x \in [n]\}.$$

Fix an integer k and let A be the set of distributions on $[n]$ with $H_\infty(p) \geq k$.

   (a) Show that A is a convex body in $\mathbb{R}^n$, that is, if $p, p' \in A$ and $a, a' \geq 0$ with $a + a' = 1$ then $ap + a'p' \in A$.

   (b) A point x is an *extreme point* of the convex body A if there are no two points $y \neq y'$ in A and real numbers $a, a' > 0$, $a + a' = 1$, so that $x = ay + a'y'$. Prove that the set of extreme points of A is the set of distribution p that are uniform on a subset of $[n]$ of size 2^k.

3. Two families A, B of subsets of $[n]$ are called *encoding* if for every $a, a' \in A$ and $b, b' \in B$,

$$(a \cup b, a \cap b) = (a' \cup b', a' \cap b') \ \Rightarrow \ a = a', b = b'.$$

That is, knowledge of $(a \cup b, a \cap b)$ implies knowledge of a, b.

   (a) Prove that if A, B are encoding then $|A||B| \leq 2^{3n/2}$.

   (b) Find A, B that are encoding so that $|A||B| \geq (2.01)^n$.

4. An alternative proof of a version of Pinsker's inequality (following Benjamini, Duminil-Copin, Kozma and Yadin). For two finitely-supported distributions p, q over the same domain X, define

$$\Delta(p, q) = \sum_{x \in X} \frac{(p(x) - q(x))^2}{p(x) + q(x)}.$$

   (a) Prove the "dual" interpretation:

$$\Delta(p, q) = \max \left(\mathbb{E}_{x\sim p}[g(x)] - \mathbb{E}_{x\sim q}[g(x)]\right)^2,$$

   where the maximum is over all $g \in \mathbb{R}^X$ so that $\mathbb{E}_{x\sim p}[g^2(x)] + \mathbb{E}_{x\sim q}[g^2(x)] = 1$.

   (b) Prove $\Delta(p, q) \leq 2D(p||q)$.

   (c) Prove $|p - q|_1 \leq \sqrt{2\Delta(p||q)}$.