18.S996 Problem Set #5
(due December 9)

Five problems would be sufficient.
1. Let $A$ be an $n \times m$ matrix over $\mathbb{R}$. Prove that there is a unique $m \times n$ real matrix $A^+$ (called the pseudoinverse) such that $AA^+A = A$, $A^+AA^+ = A^+$, and both $AA^+$ and $A^+A$ are symmetric.

2. Suppose $X$ is a Poisson random variable with mean $\lambda$. Prove that if $f$ is a function on $\mathbb{N}$ for which the expected value $E(f(X))$ exists, then

$$E(Xf(X - 1)) = \lambda E(f(X)).$$

(When $X$ takes the value 0, we interpret $0f(-1)$ as 0, although $f(-1)$ is not defined.)

3. Let $X$ be a random variable whose moment generating function $M(t) = E(e^{tX})$ exists for all $t$. The cumulant generating function for $X$ is $\log M(t)$. Prove that it is a convex and $C^\infty$ function of $t$.

4. Let $X$ be a random variable whose moment generating function $M(t) = E(e^{tX})$ exists for all $t$. Let $f(t) = \log M(t)$ be the cumulant generating function. The $n$-th cumulant $\kappa_n(X)$ is $f^{(n)}(0)$; in other words, the Taylor series of $f(t)$ is

$$f(t) = \sum_{n=1}^{\infty} \kappa_n(X) \frac{t^n}{n!}.$$

Prove that $\kappa_1(X) = E(X)$ and $\kappa_2(X) = \text{Var}(X)$. Prove that if $X$ and $Y$ are independent, then $\kappa_n(X + Y) = \kappa_n(X) + \kappa_n(Y)$ for all $n$ (a generalization the additivity of variance for independent random variables).

5. Suppose $f : \mathbb{R} \to \mathbb{R} \cup \{\infty\}$ is a convex function (i.e., $\{ (x, y) \in \mathbb{R}^2 : y \geq f(x) \}$ is a convex set) that is not identically equal to $\infty$. Its Legendre transform $f^* : \mathbb{R} \to \mathbb{R} \cup \{\infty\}$ is defined by

$$f^*(u) = \sup_v (uv - f(v)).$$

Prove that $f^*$ is convex, that $f \leq g$ implies $g^* \leq f^*$, and that $f^{**} \leq f$. Under the assumption that $f(v) = \sup\{ \ell(v) : \ell$ is an affine function satisfying $\ell \leq f$ everywhere$\}$, prove that $f^{**} = f$. (This assumption is very mild; for example, it is equivalent to lower semicontinuity.)

[For intuition regarding the Legendre transform, note that the tangent line to $f$ at $v$ is $x \mapsto f'(v)(x - v) + f(v)$ when $f$ is differentiable. If we choose $v$ so $f'(v) = u$, then the tangent line is $x \mapsto ux - f^*(u)$. Thus, taking the Legendre transform amounts to describing the tangent lines of a convex function in terms of their slope, and we can reconstruct the function as the envelope of those lines.]

6. Let $X$ be a random variable whose moment generating function $M(t) = E(e^{tX})$ exists for all $t$, and let $X_1, X_2, \ldots$ be i.i.d. copies of $X$. Prove that if $x \geq E(X)$, then

$$\text{Prob}\left( \frac{\sum_{i=1}^{n} X_i}{n} \geq x \right) \leq e^{-nf^*(x)},$$

where $f^*$ is the Legendre transform of the cumulant generating function $f(y) = \log M(y)$.

In fact, this bound is essentially sharp, in the sense that

$$\lim_{n \to \infty} \frac{1}{n} \log \text{Prob}\left( \frac{\sum_{i=1}^{n} X_i}{n} \geq x \right) = -f^*(x),$$

but you needn’t prove that.

7. You have intercepted an encrypted message, located at this URL:

http://research.microsoft.com/~cohn/Courses/18.S996F14/encrypted.txt

It consists of English text without punctuation or spacing, with each letter shifted by some quantity modulo 26. The intent was to choose the shift randomly and independently for each letter, which would have been an unbreakable “one-time pad.” However, a mistake was made, and the shifts repeat with some period. What was the original English text?