PROBABILITY THEORY

Due: January 7, 2009, at the General Office.

Brad Baxter

1. Let $X_1, X_2, \ldots$ be independent, identically distributed Bernoulli random variables for which $\mathbb{P}(X_i = \pm 1) = 1/2$, for all i, and define the scaled average

$$A_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} X_i.$$

(a) Show that $\mathbb{E}A_n = 0$ and $\mathbb{E}(A_n^2) = 1$.

(b) State Chebyshev's inequality and apply it to show that

$$\mathbb{P}(|A_n| \ge t) \le \frac{1}{t^2},$$

for any $t > 0$.

(c) Using the Markov inequality

$$e^{ct}\mathbb{P}\left(A_n \ge t\right) \le \mathbb{E}e^{cA_n},$$

for any $c > 0$ and $t \in \mathbb{R}$, prove that

$$\mathbb{P}\left(A_n \ge t\right) \le e^{-ct}\left(\frac{e^{c/\sqrt{n}} + e^{-c/\sqrt{n}}}{2}\right)^n. \qquad (*)$$

(d) Derive the inequality

$$\frac{e^x + e^{-x}}{2} \le e^{x^2/2}, \qquad \text{for } x \in \mathbb{R},$$

using the Taylor series of the exponential function. Hence use (*) to show that

$$\mathbb{P}\left(A_n \ge t\right) \le e^{-ct + c^2/2}. \qquad (**)$$

(e) Using (**), derive the Bernstein–Azuma–Hoeffding inequality:

$$\mathbb{P}\left(|A_n| \ge t\right) \le 2e^{-t^2/2}$$

(f) Show that the characteristic function $\phi_{A_n}(z) = \mathbb{E}\exp(izA_n)$ is given by

$$\phi_{A_n}(z) = \cos^n(z/\sqrt{n}).$$

Prove that $\lim_{n\to\infty} \phi_{A_n}(z) = \exp(-z^2/2)$.

2. (a) A program generates passwords $(X_1, X_2, \ldots, X_m)$ of length m, the component characters being chosen uniformly and independently from an alphabet of N symbols: in other words, $\mathbb{P}(X_i = s_k) = 1/N$, for $1 \le k \le N$ and $1 \le i \le m$. We shall say that a password is *non-redundant* if its component characters are all different.

i. Show that the probability p_m that a password of length m is non-redundant is given by

$$p_m = \prod_{k=1}^{m-1} \left(1 - \frac{k}{N}\right).$$

ii. Prove the inequality $1 - x \le \exp(-x)$, for $x \ge 0$. Hence show that

$$p_m \le e^{-\frac{(m-1)m}{2N}}.$$

Furthermore, show that $p_m \le 10^{-q}$ if $m \ge c\sqrt{N}$, where $c = \sqrt{2q \ln 10}$.

[Hint: One possible derivation of the inequality begins with the integral $\int_0^x \exp(-s)\, ds$.]

(b) Let $X_1, X_2, \ldots$ be independent, identically distributed random variables with the exponential distribution at rate λ, that is, they share the probability density function

$$p_1(s) = \begin{cases} \lambda e^{-\lambda s}, & s \ge 0, \\ 0, & s < 0, \end{cases}$$

where λ is a positive constant.

i. Let $p_n(s)$ be the probability density function for $X_1 + X_2 + \cdots + X_n$. Show that

$$p_n(s) = \begin{cases} \frac{\lambda^n s^{n-1} e^{-\lambda s}}{(n-1)!}, & s \ge 0, \\ 0, & s < 0. \end{cases}$$

ii. Show that the characteristic function $\phi_{X_1}(z) = \mathbb{E} \exp(izX_1)$ is given by

$$\phi_{X_1}(z) = \frac{\lambda}{\lambda - iz}.$$

Hence state the characteristic function for $X_1 + X_2 + \cdots + X_n$. [You may use standard properties of characteristic functions without proof, if clearly stated.]