Theory of Computation

Homework 5

Due: 2012/12/25

Problem 1 (Chernoff Bound) Suppose x_1, x_2,...,x_n are independent random variables taking values 1 and 0 with probabilities p and $1-p$, respectively. Let $X = \sum_{i=1}^{n} X_i$. Then for $0 \leq \theta \leq 1$, $\mathbf{Pr}[X \leq (1-\theta)pn] \leq e^{-\frac{\theta^2 pn}{2}}$.

Proof: Let t be any negative real number. By Markov inequality, $\mathbf{Pr}[X \leq (1-\theta)pn] = \mathbf{Pr}[e^{tX} \geq e^{t(1-\theta)pn}] \leq e^{-t(1-\theta)pn}\mathbf{E}[e^{tX}]$. Since $X = \sum_{i=1}^{n} X_i$, $\mathbf{E}[e^{tX}] = (1 + p(e^t - 1))^n$. Thus,

$$\begin{aligned} \mathbf{Pr}[X \leq (1-\theta)pn] &\leq e^{-t(1-\theta)pn}(1 + p(e^t - 1)^n) \\ &\leq e^{-t(1-\theta)pn}e^{pn(e^t-1)} \end{aligned} \tag{1}$$

Note that $(1+a)^n \leq e^{an}$ for any $a > 0$. Let $t = \ln(1-\theta)$. then

$$\mathbf{Pr}[X \leq (1-\theta)pn] \leq e^{-pn(\theta+(1-\theta)\ln(1-\theta))} \tag{2}$$

The exponent expands to $-pn(\frac{\theta^2}{2} + \frac{\theta^3}{6} + \cdots)$ for $0 \leq \theta \leq 1$. Thus $\mathbf{Pr}[X \leq (1-\theta)pn] \leq e^{\frac{-\theta^2 pn}{2}}$.

■

Problem 2 Recall that EXP = TIME(2^{n^k}). Show that BPP $\subseteq$ EXP.

Proof: It is known that PSPACE $\subseteq$ EXP (p. 220 of the slides). Thus all we need to show is BPP $\subseteq$ PSPACE. Let $L \in$ BPP, and consider a precise polynomial-time NTM N that decides L. Let $\epsilon \leq 1/4$ be the error probability, and $p(n)$ be the polynomial time complexity of N, where n is the length of the input. Without loss of generality, assume N has 2 options in each nondeterministic move. As in the textbook, in each run N makes $p(n)$ nondeterministic moves. Thus N has $2^{p(n)}$ possible computation paths each of length $p(n)$. Each computation path has the same probability of occurrence.

Construct a deterministic TM M which simulates N to generate all possible computation paths sequentially and reuses the space used by each previous path. M counts the the number n_{accept} of the accepting paths. M accepts the input if $\frac{n_{\text{accept}}}{2^{p(n)}} \geq 3/4$; otherwise, M rejects. Thus N runs in polynomial space. Clearly, BPP $\subseteq$ PSPACE and BPP $\subseteq$ EXP is proved.

■