Theory of Computation

Solutions to Homework 5

Problem 1. Let $\mu \equiv E[X]$ and $\sigma^2 \equiv E[(X-\mu)^2]$ be finite. Show that

$$prob\,[\,|X-\mu| \geq k\sigma] \leq 1/k^2$$

for $k \geq 0$. (Hint: The Markov inequality: $prob[Y \geq m] \leq E[Y]/m$ if random variable Y takes on only nonnegative values and $m \geq 0$.)

Proof. Let $Y = (X - \mu^2)$ and $m = (k\sigma)^2$, By Markov inequality, it's easy to see that

$$\begin{aligned}
&prob[Y \geq m] \leq \frac{E[Y]}{m} \\
\Rightarrow &prob[(X-\mu)^2 \geq (k\sigma)^2] \leq \frac{\sigma^2}{(k\sigma)^2} \\
\Rightarrow &prob[\sqrt{(X-\mu)^2} \geq \sqrt{(k\sigma)^2}] \leq \frac{\sigma^2}{k^2\sigma^2} \\
\Rightarrow &prob[|X-\mu| \geq k\sigma] \leq \frac{1}{k^2}
\end{aligned}$$

still holds because $(X-\mu)^2$ is a nonnegative value and $(k\sigma)^2 \geq 0$ □

Problem 2. Show that if SAT has no polynomial circuits, then coNP≠BPP. (Hint: Adleman's theorem states that all languages in BPP have polynomial circuits.)

Proof. Assume that SAT has no polynomial circuits. As all languages in BPP have polynomial circuits by Adleman's theorem, NP $\neq$ BPP. Hence

$$\text{coNP} \neq \text{coBPP}=\text{BPP}.$$

□