Theory of Computation

Final-Term Examination on January 10, 2012

Fall Semester, 2011

Note: You may use any results proved in class.

Problem 1 (25 points)**.** Prove that L is **NP**-complete if and only if its complement $\bar{L}$ is **coNP**-complete.

Solution.

$\Rightarrow$ Let L be an **NP**-complete language; thus $L \in \mathbf{NP}$. For all $L' \in \mathbf{NP}$, let R be a reduction form L' to L. Problem instance $x \in L' \Leftrightarrow R(x) \in L$. Equivalently, $x \notin L' \Leftrightarrow R(x) \notin L$ (the law of transposition). So $x \in \bar{L}' \Leftrightarrow R(x) \in \bar{L}$. R is a reduction from $\bar{L}'$ to $\bar{L}$. Hence $\bar{L}$ is **coNP**-complete.

$\Leftarrow$ Let $\bar{L}$ be a **coNP**-complete language; thus $\bar{L} \in \mathbf{coNP}$. For all $\bar{L}' \in \mathbf{coNP}$, let R be a reduction form $\bar{L}'$ to $\bar{L}$. Problem instance $x \in \bar{L}' \Leftrightarrow R(x) \in \bar{L}$. Equivalently, $x \notin \bar{L}' \Leftrightarrow R(x) \notin \bar{L}$ (the law of transposition). So $x \in L' \Leftrightarrow R(x) \in L$. R is a reduction from L' to L. Hence L is **NP**-complete.

$\square$

Problem 2 (25 points)**.** The Jacobi symbol $(a \mid m)$ is the extension of the Legendre symbol $(a \mid p)$, where p is an odd prime, and

$$(a \mid p) = \begin{cases} 0 & \text{if } (p \mid a)\,, \\ 1 & \text{if } a \text{ is a quadratic residue module } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue module } p. \end{cases}$$

Recall that when $m > 1$ is odd and $\gcd(a, m) = 1$, then $(a \mid m) = \prod_{i=1}^{k} (a \mid p_i)$. Please calculate $(1234 \mid 99)$. Please write down the steps leading to your answer.

Solution.

$$(1234 \mid 99) = (46 \mid 99) = (46 \mid 9)\,(46 \mid 11) = (1 \mid 9)\,(2 \mid 11) = 1{\cdot}(-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$$

□

Problem 3 (25 points)**.** Let $\mu \equiv E[X]$ and $\sigma^2 \equiv E[(X-\mu)^2]$ be finite. Show that

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

for $k \geq 0$.
(Hints: The Markov inequality says: $\text{prob}[Y \ \geq \ m] \leq E[Y]/m$ if random variable Y takes on only nonnegative values and $m \geq 0$. Try $Y = (X-\mu)^2$.)

Solution. Let $Y = (X-\mu)^2$ and $m = (k\sigma)^2$. Then

$$\text{prob}[Y \ \geq \ m] \leq \frac{E[Y]}{m}$$

$$\begin{aligned}
&\Leftrightarrow \text{prob}[(X-\mu)^2 \geq (k\sigma)^2] \leq \frac{\sigma^2}{(k\sigma)^2} \\
&\Leftrightarrow \text{prob}[\sqrt{(X-\mu)^2} \geq \sqrt{(k\sigma)^2}] \leq \frac{\cancel{\sigma}^2}{k^2\ \cancel{\sigma}^2} \\
&\Leftrightarrow \text{prob}[|X-\mu| \geq k\sigma] \leq \frac{1}{k^2}.
\end{aligned}$$

The last line is due to Markov's inequality because $(X-\mu)^2$ is a nonnegative value and $(k\sigma)^2 \geq 0$. □

Problem 4 (25 points)**.** Please define RP and prove that RP $\subseteq$ NP.

Solution. RP is the class of all languages L with a (precise) polynomial-time Monte Carlo TM M such that

$$\text{If } x \in L, \text{ then } \text{Prob}[M(x) = \text{“Yes”}] \geq \frac{1}{2}. \tag{1}$$

$$\text{If } x \notin L, \text{ then } \text{Prob}[M(x) = \text{“No”}] = 1.$$

If L in RP and $x \in L$, then there exists a sequence of coin flips f such that M accepts x with f as the nondeterministic choices by (1). If $x \notin L$, the $\text{Prob}[M(x) = \text{“Yes”}] = 0$. So M rejects x. So $L \in$ NP. □