Theory of Computation

Homework 4

Due: 2012/12/11

Problem 1 Show that BPP is closed under reductions. (For simplicity, we assume a reduction runs in polynomial time instead of log space.)

Proof: Let $L \in$ BPP and $\epsilon = 1/4$ such that there exists a polynomial-time NTM M which decides L with $\mathbf{Pr}[M(x) = 1 \mid x \in L] > 1 - \epsilon$ and $\mathbf{Pr}[M(x) = 0 \mid x \notin L] > 1 - \epsilon$ for every input x. Suppose that L' is reducible to L via a reduction R, which runs in polynomial time. Note that for all x, $x \in L'$ iff $R(x) \in L$. Then consider a polynomial-time NTM N which decides L' as follows: on input x, N runs $M(R(x))$ for $k = \frac{4 \ln 2}{\epsilon^2}$ times to obtain k outputs y_1, y_2,...,$y_k \in \{0, 1\}$. If the strict majority of these outputs is 1, then $N(x) = 1$; otherwise, $N(x) = 0$.

For the i-th run of $M(R(x))$, define the random variable $X_i = 1$ if $y_i = I(x \in L')$, where I is the indicator function; otherwise, $X_i = 0$. In other words, $X_i = 1$ if and only if y_i is correct. Note that X_is are independent random variables with $\mathbf{Pr}[X_i = 1] > 1 - \epsilon$. By Corollary 69 (p. 550 in the slide), $\mathbf{Pr}[\sum_{i=1}^{k} X_i \leq \frac{k}{2}] \leq e^{-\frac{\epsilon^2 k}{2}} = 1/4$. This guarantees that $N(x)$ will output the correct answer with error probability $\leq 1/4$. Thus, $L' \in$ BPP, and BPP is closed under reductions.

■

Problem 2 Show that RP is closed under intersection. (This means that $L_1 \cap L_2 \in$ RP if $L_1 \in$ RP and $L_2 \in$ RP.)

Proof: Let L_1 and $L_2 \in$ RP be decided by polynomial-time Monte Carlo TMs N_1 and N_2, respectively. Note that for $i = 1, 2$, and $\epsilon_i = 1/2$, $\mathbf{Pr}[N_i(x) = 1 \mid x \in L_i] > 1 - \epsilon_i$ and $\mathbf{Pr}[N_i(x) = 1 \mid x \notin L_i] = 0$.

To show that RP is closed under intersection, let TM $N_\cap$ simulate N_1 and N_2 with independent coin flips on input x such that $N_\cap(x) = 1$ if both machines N_1 and N_2 accept x; otherwise, $N_\cap(x) = 0$. Now we prove that $N_\cap$ decides $L_1 \cap L_2$ with one-sided error probability $\epsilon = 1 - (1 - \epsilon_1)(1 - \epsilon_2)$. Note that $0 < \epsilon \leq 1$. Assume $x \in L_1 \cap L_2$. We have $\mathbf{Pr}[N_\cap(x) = 1] = \mathbf{Pr}[N_1(x) = 1] \times \mathbf{Pr}[N_2(x) = 1] > (1 - \epsilon_1) \times (1 - \epsilon_2) = 1 - \epsilon = 1/4$ (recall that any constant probability will work for RP). Now assume $x \notin L_1 \cap L_2$. This implies either $\mathbf{Pr}[N_1(x) = 1] = 0$ or $\mathbf{Pr}[N_2(x) = 1] = 0$ because $x \notin L_1$ or $x \notin L_2$. Thus $\mathbf{Pr}[N_\cap(x) = 1] = 1 - \mathbf{Pr}[N_\cap(x) = 0] = 1 - \mathbf{Pr}[N_1(x) = 0$ or $N_2(x) = 0] = 1 - (1 - \mathbf{Pr}[N_1(x) = 1] \times \mathbf{Pr}[N_2(x) = 1])) = 0$. Clearly, $L_1 \cap L_2 \in$ RP, and we have shown that RP is closed under intersection.

■