Theory of Computation

Midterm Examination on December 16, 2014

Fall Semester, 2014

Problem 1 (25 points) Let $G(V, E)$ be a directed graph with vertices V and edges E, and $|V|$ be the number of vertices in G. HAMILTONIAN CYCLE asks if there is a cycle through a graph G which visits each vertex exactly once. It is known that HAMILTONIAN CYCLE is NP-complete. BIGCYCLE asks if G has a cycle of length equal or larger than $|V|/2$. Reduce HAMILTONIAN CYCLE to BIGCYCLE.

Ans: Let N be an NTM which decides BIGCYCLE. Construct an NTM M which decides HAMILTONIAN CYCLE as follows:

1: On input $G(V, E)$ with $|V|$.

2: Add exactly $|V|$ isolated vertices to G to obtain G'.

3: Run N(G').

4: If N accepts, halt and accept.

5: Otherwise, halt and reject.

Clearly $G \in$ HAMILTONIAN CYCLE if and only if $G' \in$ BIGCYCLE. M clearly runs in polynomial time. It completes the proof. ■

Problem 2 (25 points) Let a, b, n, m be any odd integers. Show that if $\gcd(ab, nm) = 1$, then $(ab^2|nm^2) = (a|n)$. (Recall that $(ab|m) = (a|m)(b|m)$ when $\gcd(ab, m) = 1$ and $(a|nm) = (a|n)(a|m)$ when $\gcd(a, nm) = 1$.)

Ans:

$$\begin{aligned}
(ab^2|nm^2) &= (a|nm^2)(b^2|nm^2) \\
&= (a|n)(a|m^2)(b|nm^2)(b|nm^2) \\
&= (a|n)(a|m)(a|m)(b|nm^2)^2 \\
&= (a|n)(a|m)^2 \\
&= (a|n).
\end{aligned}$$

■

Problem 3 (25 points) Show that if 3-SAT has uniform polynomial circuits, then NP = coNP.

Ans: By Theorem 74 (see p. 613 in the slides), 3-SAT is then in P. As 3-SAT is NP-complete, by Corollary 29 (see p. 292 in the slides) P = NP = coNP. ∎

Problem 4 (25 points) Show that RP is closed under union. (This means that $L_1 \cup L_2 \in$ RP if $L_1 \in$ RP and $L_2 \in$ RP. Recall that the error probability does not have to be exactly 1/2; any constant will do.)

Ans: 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 $\epsilon_i = 1/2$, $\mathbf{Pr}(N_i(x) = 1 \mid x \in L_i) \geq 1 - \epsilon_i$ and $\mathbf{Pr}(N_i(x) = 1 \mid x \notin L_i) = 0$.

To show that RP is closed under union, let TM $N_\cup$ simulate N_1 and N_2 with independent coin flips on input x. $N_\cup(x) = 1$ if N_1 or N_2 accepts x; otherwise, $N_\cup(x) = 0$. Now we prove that $N_\cup$ decides $L_1 \cup L_2$ with one-sided error probability $\epsilon = \epsilon_1\epsilon_2$. Note that $0 < \epsilon \leq 1$. Assume $x \in L_1 \cup L_2$. Then

$$\begin{aligned}
\mathbf{Pr}(N_\cup(x) = 1) &= 1 - \mathbf{Pr}(N_\cup(x) = 0) \\
&= 1 - \mathbf{Pr}(N_1(x) = 0) \times \mathbf{Pr}(N_2(x) = 0) \\
&\geq 1 - \epsilon_1\epsilon_2 \\
&= 1 - \epsilon.
\end{aligned}$$

Hence $\epsilon = \dfrac{1}{4}$. Now assume $x \notin L_1 \cup L_2$. This implies that $\mathbf{Pr}(N_1(x) = 1) = \mathbf{Pr}(N_2(x) = 1) = 0$. So,

$$\begin{aligned}
\mathbf{Pr}(N_\cup(x) = 1) &= 1 - \mathbf{Pr}(N_\cup(x) = 0) \\
&= 1 - \mathbf{Pr}(N_1(x) = 0) \times \mathbf{Pr}(N_2(x) = 0) \\
&= 1 - (1 - \mathbf{Pr}(N_1(x) = 1)) \times (1 - \mathbf{Pr}(N_2(x) = 1)) \\
&= 0.
\end{aligned}$$

Clearly, $L_1 \cup L_2 \in$ RP, and the claim holds. ∎