COS 522, April 11, 2000
Due: April 25, 2000

Homework Set 3

Problem 1 Prove that $NP \neq DSPACE(n^2)$.

Problem 2 For any set $B \subseteq \{0,1\}^*$, let $L_B = \{0^n | (\exists x\ |x| = n) x1, x1^2, \cdots,\ x1^n \in B\}$.
(a) Show that $L_B \in NP^B$.
(b) Let M be any polynomial time deterministic oracle machine. Let $L(M^B)$ be the language accepted by M^B. Prove that, for a random B, the probability that $L(M^B) = L_B$ is zero.
(c) Infer that, for a random oracle B, $P^B \neq NP^B$ with probability 1.

Remarks A set B is identified with the real number with binary representation $0.x_1x_2x_3\cdots$, where $x_i = 1$ if and only if B contains the i-th lexicographically smallest element of $\{0,1\}^*$. A *random* oracle B means a random real number x uniformly chosen from the interval $[0,1]$ (in the standard Lebesgue sense) and let B be the corresponding B. (For calculational purposes, one can take each x_i to be an independently chosen unbiased coin toss.)

Problem 3 Prove that if $NP \subseteq BPP$, then $RP = NP$.

Problem 4 Prove that if $NP \subseteq BPP$, then $PH = BPP$.

Remark The above Problem shows that if we make a stronger assumption in Karp-Lipton-Sipser, then the polynomial hierarchy collapses further below Σ_2 to BPP.

Problem 5 Show that finding the lexicographically first maximal independent set of a graph is P-complete. Use reduction from CIRCUIT VALUE EVALUATION (see the notes from Spielman and from Hastad).