Problem Set 1

Due on Thursday, April 22, 2010

1. [30/100] Prove that $\text{NP} \neq \text{E}$.

Recall that $\text{E} := \text{DTIME}(2^{O(n)})$ is the class of problems solvable by deterministic turing machine in time $2^{O(n)}$, where $n$ is the length of the input. Also, recall that a language $A$ has a many-to-one polynomial time reduction to a language $B$, written $A \leq^p_m B$ if there is a polynomial time computable function $f(\cdot)$ such that for every instance $x$ we have $x \in A \iff f(x) \in B$. In your proof, show that $\text{NP}$ is closed under polynomial many-to-one reductions, that is $A \leq^p_m B$ and $B \in \text{NP}$ implies $A \in \text{NP}$, and that if $\text{E}$ were closed under many-to-one reductions, we would have a contradiction to the time hierarchy theorem.

2. [30/100] Prove that if $\text{NP} \subseteq \text{BPP}$ then $\text{NP} = \text{RP}$.

3. [40/100] Prove that if $\text{P} = \text{NP}$, then there is a problem in $\text{EXP}$ that requires circuits of size $2^{O(n)}$.

Hint: you may want to use the fact that if $\text{P} = \text{NP}$ then $\Sigma_k = \text{P}$ for every $k$; if so, you should prove it first. Recall that $\text{EXP} := \text{DTIME}(2^{n^{O(1)}})$.

Note that the theorem in Problem 3 implies that a proof of the existence of sub-exponential size circuits for all problems in $\text{EXP}$, which is a result of an algorithmic flavor, would give $\text{P} \neq \text{NP}$, a lower bound result.

Not for credit, think about the following question. Suppose that SAT is solvable in polynomial time, then it is easy to show that $\Sigma_3 = \text{P}$. This means that every problem in $\Sigma_3$ is solvable in polynomial time given an oracle for SAT. But the class of problems solvable in polynomial time with oracle access to SAT is contained in $\Sigma_2$ (prove it), and so $\Sigma_3 \subseteq \Sigma_2$ and the polynomial hierarchy collapses. Where does the above argument go wrong?