Problem Set 1

Due on Thursday, April 22, 2010

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

   Recall that $\mathbf{E} := \mathbf{DTIME}(2^{O(n)})$ 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 $A \leq_m^p B$ if there is a polynomial time computable function $f(\cdot)$ such that for every instance x we have $x \in A \Leftrightarrow f(x) \in B$. In your proof, show that $\mathbf{NP}$ is *closed* under polynomial many-to-one reductions, that is $A \leq_m^p B$ and $B \in \mathbf{NP}$ implies $A \in \mathbf{NP}$, and that if $\mathbf{E}$ were closed under many-to-one reductions, we would have a contradiction to the time hierarchy theorem.

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

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

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

Note that the theorem in Problem 3 implies that a proof of the existence of subexponential size circuits for all problems in $\mathbf{EXP}$, which is a result of an algorithmic flavor, would give $\mathbf{P} \neq \mathbf{NP}$, 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 $\Sigma_3 = \mathbf{P}$. This means that every problem in Σ_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 Σ_2 (prove it), and so $\Sigma_3 \subseteq \Sigma_2$ and the polynomial hierarchy collapses. Where does the above argument go wrong?