CS 262: Computational Complexity **Due: February 26, 2010**

Homework 5

Instructor: Sandy Irani

Do three of the following five problems:

1. Show that the class $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{co} - \mathbf{RP}$.

2. Describe a *decidable* language that is in $\mathbf{P/poly}$ but not in $\mathbf{P}$.

3. We have been careful to have gates with bounded *fan-in* (that is, they each take at most two inputs). However, we have allowed unbounded *fan-out* in that each gate can feed into an arbitrary number of gates. Show that any circuit can be transformed into another with fan-out two with only a linear increase in the size.

4. The language **USAT** is the set of boolean formulae that have a unique satisfying assignment. In class we proved the Valiant-Vazirani theorem which says that that there exists a polynomial-time algorithm f such that for every n-variable boolean formula, ϕ
$$\phi \in \ SAT \ \Rightarrow Pr[f(\phi) \in \ USAT \ ] \geq \frac{1}{8n}$$
$$\phi \notin \ SAT \ \Rightarrow Pr[f(\phi) \in \ USAT \ ] = 0.$$
Now suppose we have a polynomial time algorithm that given a boolean formula ϕ, will answer "yes" if $\phi \in \ USAT$, will answer "no" if $\phi \notin \ SAT$ and will answer arbitrarily otherwise. Prove that this would imply that $\mathbf{RP} = \mathbf{NP}$.

5. A language $L \subseteq \{0,1\}^*$ is *sparse* if there is a polynomial p such that $|L \cap \{0,1\}^n| \leq p(n)$ for all n. Show that every sparse language is in $\mathbf{P/poly}$.