CS 262: Computational Complexity *Instructor: Sandy Irani*

Homework 3

Due: May 13, 2013

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. 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

$$\phi \in \ SAT \ \Rightarrow Pr[f(\phi) \in \ USAT \ ] \geq \frac{1}{8n}$$
$$\phi \notin \ SAT \ \Rightarrow Pr[f(\phi) \in \ SAT \ ] = 0.$$

   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 $\mathbf{RP} = \mathbf{NP}$.

4. 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 $\mathbf{P/poly}$.

5. Define $\mathbf{ZPP'}$ to be the class of all languages decided by a probabilistic Turing Machine running in expected polynomial time. That is, for every language L in $\mathbf{ZPP'}$ there is a probabilistic Turing Machine M (with two read-only tapes the first tape containing the input, and the second tape containing a random bit in every tape square) with the following behavior: on input $x \in L$, M always accepts, on input $x \notin L$, M always rejects, and for every input x,

$$E[\#\text{ steps before M halts}] = |x|^{O(1)}.$$

   Show that $\mathbf{ZPP'} = \mathbf{ZPP}$.

6. The class $\mathbf{P/log}$ is the class of languages decidable by a Turing Machines running in polynomial time that take O(log n) bits of advice. Show that $SAT \in \mathbf{P/log}$ implies $\mathbf{P} = \mathbf{NP}$.