Complexity Theory 2010
(Home work 3)

August 2, 2010

- Due on Monday, August 16, before 10 a.m.
- Late home works will not be accepted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.
- Collaboration is discouraged, but not prohibited. It is recommended that you try to solve the problems on your own. You can discuss the questions with your colleagues but you should not copy solutions. Always write down your own answers. If copying is detected that may immediately lead to a grade less than 7. (**This would be followed strictly**)
- Credits would be given to partial solutions also.
- The answers should be typed or written clearly and a hard copy is to be submitted.

1. (**10 points**) Prove that the number of languages in $\mathbf{P}/poly$ are not countable.

2. (**10 points**) A language $L \subseteq \{0,1\}^*$ is said to be sparse if there exist a polynomial p such that for every n, $|L \cap \{0,1\}^n| \leq p(n)$. Show that every sparse language is in $\mathbf{P}/poly$.

3. (**10 points**) A theorem due to Ravi Kanan says the following:

   For every polynomial p there is a language $L \in \Sigma_3^p$ such that $L \notin \mathbf{SIZE}(p(n))$.

   Using the above result, prove the following:
   For every polynomial p there is a language $L \in \Sigma_2^p$ such that $L \notin \mathbf{SIZE}(p(n))$.
   (Hint: If $\mathsf{3SAT} \notin \mathbf{SIZE}(p(n))$ then we are done as $\mathsf{3SAT} \in \Sigma_2^p$, then argue what happens if $\mathsf{3SAT} \in \mathbf{SIZE}(p(n))$).

4. (**20 points**) Prove the following.

   (a) **ZPP** = **RP** $\cap$ **coRP**.

   (b) If **NP** $\subseteq$ **BPP** then **NP** = **RP**.

5. (**20 points**) For $\rho : \mathbb{N} \to [0,1]$, we define the class of languages $\mathbf{ZPP}_\rho$, such that it contains a language L if there exist a poly-time randomized algorithm A such that

$$\forall x \Pr[A(x) = \chi_L(x)] \geq \rho(|x|),$$

   and $\Pr[A(x) \in \{\chi_L(x), ?\}] = 1$, where $\chi_L(x) = 1$ if $x \in L$ and $\chi_L(x) = 0$ otherwise. Prove that

   (a) For every positive polynomial p, the class $\mathbf{ZPP}_{\frac{1}{p}}$ equals **ZPP**.

   (b) For every positive polynomial p, the class **ZPP** equals $\mathbf{ZPP}_\rho$, where $\rho(n) = 1 - 2^{-p(n)}$.

6. (**30 points**) In class we saw the sketch of the proof of the following theorem:

   > Suppose there is a polynomial time algorithm that on input a CNF formula having exactly one satisfying assignment finds that assignment, then **NP** = **RP**.

   Write a complete proof of the above theorem. You should prove all results that you require.