Complexity Theory 2012
(Home work 3)

August 3, 2012

- Due on Monday, August 17, 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. Prove that the number of languages in $\mathbf{P}/poly$ are not countable.
2. 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. 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. Prove the following.

(a) $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$.

(b) If $\mathbf{NP} \subseteq \mathbf{BPP}$ then $\mathbf{NP} = \mathbf{RP}$.

5. Let A be a probabilistic algorithm and L the language which it decides, define g_A^L as the gap of A for L as

$$g_A^L = \min_{x \in L} \Pr[A(x) = 1] - \max_{x \notin L} \Pr[A(x) = 1].$$

Also let ϵ_A^L be the error of A for L, defined as

$$\epsilon_A^L = \max_x \Pr[A(x) \neq \chi_L(x)],$$

where $\chi_L(x) = 1$ if $x \in L$ and $\chi_L(x) = 0$ if $x \notin L$.

(a) Let A_1 be a **BPP** algorithm for a language L_1, find the values of $g_{A_1}^{L_1}$ and $\epsilon_{A_1}^{L_1}$.

(b) Let A_2 be a **RP** algorithm for a language L_2, find the values of $g_{A_2}^{L_2}$ and $\epsilon_{A_2}^{L_2}$.

(c) Let A be any probabilistic algorithm for the language L, show that

$$\epsilon_A^L \leq 1 - g_A^L$$

6. 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 $\rho(n) = 1 - 2^{-p(n)}$.