Introduction to Computational Complexity - Assignment 1

To be submitted by 2/3/2008

Reading Assignment

1. Make sure you are familiar with the following probabilistic inequalities: Markov inequality, Chebyshev inequality and Chernoff inequality. You do *not* have to know the proofs of those inequalities, but you have to know *how to use them*.
   A possible source for learning about those inequalities is Section D.1 of Appendix D, which is posted on the course's website (`http://www.wisdom.weizmann.ac.il/~orm/complexity08`).
2. Read Section D.2 of Appendix D, which is posted on the course's website. You may stop just before Theorem D.5. You may want to read the document "Introduction to pairwise independent hashing", posted on the website, first.

Question

Warm up (Not to be submitted)

For any function $\alpha : \mathbb{N} \to (0,1)$, we define the complexity class $\mathcal{RP}_\alpha$ as follows: A set S is in $\mathcal{RP}_\alpha$ if and only if there exists an probabilistic polynomial time algorithm that satisfies the following:

1. For every $x \in S$, it holds that $\Pr[M(x) \text{ accepts}] \geq \alpha(|x|)$, where the probability is over the coin tosses of M.
2. For every $x \notin S$, it holds that $\Pr[M(x) \text{ rejects}] = 1$, where the probability is over the coin tosses of M.

The purpose of this question is to show that to a great extent the choice of $\alpha(n)$ is not essential for the definition of $\mathcal{RP}$. Specifically, let $p(n)$ be any polynomial, and let $\alpha_1(n) = \frac{1}{p(n)}$ and $\alpha_2(n) = 1 - 2^{-p(n)}$. Show that $\mathcal{RP}_{\alpha_1} = \mathcal{RP}_{\alpha_2}$.

To be submitted

For any function $\alpha : \mathbb{N} \to (0,1)$, we define the complexity class $\mathcal{BPP}_\alpha$ as follows: A set S is in $\mathcal{BPP}_\alpha$ if and only if there exists an probabilistic polynomial time algorithm that satisfies the following:

1. For every $x \in S$, it holds that $\Pr[M(x) \text{ accepts}] \geq \alpha(|x|)$, where the probability is over the coin tosses of M.
2. For every $x \notin S$, it holds that $\Pr[M(x) \text{ rejects}] \geq \alpha(|x|)$, where the probability is over the coin tosses of M.

The purpose of this question is to show that to a great extent the choice of $\alpha(n)$ is not essential for the definition of $\mathcal{BPP}$. Specifically, let $p(n)$ be any polynomial, and let $\alpha_1(n) = \frac{1}{2} + \frac{1}{p(n)}$ and $\alpha_2(n) = 1 - 2^{-p(n)}$. Show that $\mathcal{BPP}_{\alpha_1} = \mathcal{BPP}_{\alpha_2}$.

Hint: Use Chernoff's inequality.