CSC 2401F 2007, Assignment r32

Due: December 21 (suggested); December 28 (last day accepted)

1. The definition a language L being accepted by an IP = IP(2/3,2/3) specified a 2/3 probability of correctness for both the completeness and soundness conditions. Show that if the soundness condition is changed to be probability 1 (i.e. the verifier never accepts an input $x \notin L$, then IP(2/3,1) = NP.

   [10 points]

2. Problem 1 of chapter 9. That is show that $\#P \subseteq FP^{PP}$ [10 points]

3. Suppose we have a "black box" $B(x_1, ..., x_n)$ that "efficiently" computes a polynomial $P \in Z_p[x_1, ..., x_n]$ of degree d for "most" inputs. Namely, say $prob[B(a_1, ..., a_n) \neq P(a_1, ..., a_n)] \leq 1/3d$. Here the probability is over a uniform random choice of the $a_i \in Z_p$. Assuming $p > d + 1$, show how to use the black box to "efficiently" compute P for all inputs $(a_1, ..., a_n) \in Z_p^n$ with high probability, say probability $\geq 1 - 2^{-n}$.
   Hint: Look at a similar result for the permanent in chapter 8 of the text.

   [10 points]