Honors Theory of Computation, Spring'00
HOMEWORK 5:
Out: April 5, 2000
Due: April 17, 2000

==
IMPORTANT:
1) Answer each question within the page limitation specified (use reasonable size handwriting, and leaving a 1-inch margin for grading). If necessary, summarize your method or arguments.
2) Be precise in your use of mathematical notations. Every sentence must be an English sentence, even if formulas are involved.
==

(Q1) Problem 10.4.6 (p.237). LIMIT: 1 page

This problem concerns $NP \cap co - NP$ and a notion called "strong nondeterministic TM".

(Q2) Certificates for primes. LIMIT: 0.5 page

Let $n = 65521$. Give a certificate $C(n)$ (as in the text) for the fact that n is prime. Summarize what you did to find $C(n)$ (computer programs or hand calculators are allowed).

(Q4) Chernoff bound. LIMIT: 1 page

(a) Chernoff bounds are really a family of bounds based on the following method. Show for any r.v. X and real number c, and any $t > 0$,

$$Pr(X \geq c) \leq E[e^{t(X-c)}]$$

HINT: Use exactly the same argument as in beginning of of the proof of Lemma 11.9.
(b) The trick in Chernoff bounds if to choose the t which minimizes the expression $E[e^{t(X-c}]$. Let us define

$$m_X(c) = \min_{t>0} E[e^{t(X-c}].$$

Determine $m_X(c)$ in case X is a sum of n Bernoulli r.v.s $X_1, X_2, ..., X_n$ where $Pr(X_i = 1) = p$ $(0 < p < 1)$.
HINT: Use calculus to determine $m_X(c)$. Differentiate the expression $f(t) = E[e^{t(X-c}]$ and equate to zero.
(c) Conclude that

$$Pr(X \geq (1-\epsilon)np) \leq \left(\frac{1}{1-\epsilon}\right)^{(1-\epsilon)np} \left(\frac{1-p}{1-(1-\epsilon)p}\right)^{n-(1+\epsilon)np}$$

(Q4) Problems 11.5.14 and 11.5.15 (page 274). LIMIT: 3 pages

(a) BPP closed under union and intersection (1 page)
(b) RP closed under union and intersection (1 page)
(c) PP closed under complement and symmetric difference (1 page)
HINT: Use the (relaxed) definition of these computations in which a path of a computation tree of a BPP-, RP- or PP-machine is AT MOST (not EXACTLY EQUAL to) a polynomial of the input length. Also do Problem 11.5.13, but do not hand these in for grading.