HW4, CPSC 468/568, Due Mar. 31, 2016

Throughout this assignment, if a proof or step of a proof follows directly from a definition given or a theorem proven in class or in a reading assignment, then you may simply say that, *i.e.*, you need not reproduce proofs given in class or in the reading.

Problem 0 *(0 points)*:

Read Chapter 8 of your textbook.

Problem 1 *(10 points)*:

Prove that AM[2] $\subseteq$ NP/poly.

Problem 2 *(20 points)*:

Prove that $\mathrm{NP}^{\mathrm{BPP}} \subseteq \mathrm{MA}[2] \subseteq \mathrm{ZPP}^{\mathrm{NP}}$.

Problem 3 *(10 points)*:

Prove that, if NP = RP, then AM[2] = BPP.

Problem 4 *(20 points)*:

Show that there exists an oracle A such that $\mathrm{coNP}^A \not\subseteq \mathrm{AM}^A$.

Problem 5 *(20 points)*:

Prove that IP[$O(1)$] $\subseteq$ AM[$O(1)$]. That is, prove that, if there is a k-round, private-coin interactive proof system for the set S, where k is a constant, then there a k'-round, public-coin interactive proof system for S, where k' is also a constant. Note that k' may be greater than k.

(Hint: Consider the Goldwasser-Sipser lower-bound protocol given in Chapter 8.)

Problem 6 *(10 points)*:

Show that IP is contained in PSPACE.

Problem 7 *(10 points)*:

Given two $n \times n$ integer matrices A and B, their product AB can be computed in time $O(n^{2.373})$ using the best known matrix-multiplication algorithm. Provide a checker for matrix multiplication that runs in time $O(n^2)$.