McGill University COMP531 Winter 2010 **Instructor: Phuong Nguyen**

Assignment 5

Due 12pm April 19 in MC303

The work you submit must be your own. You may discuss problems with each others; however, you should prepare written solutions alone. Copying assignments is a serious academic offense, and will be dealt with accordingly.

(It is helpful to give a high level description of a proof or an algorithm before giving the details.)

Question 1 (10pt) For this question, recall $\mathbf{NP}/poly$ is the class of languages computable by a polytime nondeterministic Turing machine with advice. In other words, $L \in \mathbf{NP}/poly$ if there is a polynomial $p(n)$ and a polytime relation $R(x, y, z)$ so that for all n, there is an advice string z of length $p(n)$ such that

$$x \in L \Leftrightarrow \exists y, |y| \leq p(n) \wedge R(x, y, z)$$

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

Question 2 (10pt) Let $R(x, y, r)$ be a polynomial time relation, $p(n)$ a polynomial, and c a constant, $0 < c < 1/10$. Suppose that L is a language such that for all x of length n:

$$x \in L \Rightarrow Pr_{r \in \{0,1\}^{p(n)}} \big[\exists y, |y| \leq p(n) \wedge R(x, y, r)\big] \geq c$$

$$x \notin L \Rightarrow Pr_{r \in \{0,1\}^{p(n)}} \big[\exists y, |y| \leq p(n) \wedge R(x, y, r)\big] \leq c/2$$

Prove that $L \in \mathbf{AM}[2]$.

Question 3 (10pt) Show that if $\mathbf{NP} = \mathbf{RP}$ then $\mathbf{AM}[2] = \mathbf{BPP}$.