Homework 11
Due Fri May 28, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

26. We defined the classes AM and MA, involving two players Arthur (a probabilistic polynomial-time verifier) and Merlin (a computationally unbounded "magical" prover who can observe Arthur's coin tosses). A formal definition of AM can be given as follows.

    Suppose $L \subseteq \{0,1\}^*$ is a language, and Merlin is trying to prove to Arthur that $x \in L$. Let $V(x,r,w) \in \{0,1\}$ denote the outcome of Arthur's verifier ($1 = \text{ACCEPT}, 0 = \text{REJECT}$) on input $x \in \{0,1\}^*$, random string $r \in \{0,1\}^*$ and witness $w \in \{0,1\}^*$ provided by Merlin. We say $L \in \mathsf{AM}$ if $\exists\, V$ such that

$$x \notin L \implies \Pr_r[\exists\, w\ (V(x,r,w)=1)] \le \frac{1}{3}\,,$$
$$x \in L \implies \Pr_r[\exists\, w\ (V(x,r,w)=1)] \ge \frac{2}{3}\,.$$

    Notice that the definition captures the nature of the interaction: Merlin provides a witness w based on both x and r. The class MA differs from this in that Merlin must provide a witness w in advance, and Arthur *then* uses a random string r to do the verification. Give an analogous formal definition of MA; use the specific constants $\frac{1}{3}$ and $\frac{2}{3}$ as above. Then, give a full formal proof that $\mathsf{MA} \subseteq \mathsf{AM}$. [2 points]

27. Prove that $\mathsf{AM} \subseteq \mathsf{PH}$. Try to find the lowest level you can within the polynomial hierarchy that contains AM. [2 points]