Homework 12
Due Fri May 30, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

Recall the complexity class AM from the lectures. It is the class of languages L for which there exists an Arthur-Merlin protocol, i.e., a protocol of the following form. An input $x \in \{0,1\}^*$ is given to both parties. Arthur selects a random string $r \in \{0,1\}^*$, which is visible to Merlin, who then sends Arthur a message $a \in \{0,1\}^*$. Arthur then computes an accept/reject verdict in polymomial time. The required properties of this verdict are:

$$x \in L \implies \Pr_r[\exists\, a\; V(x,r,a) = 1] \;\geq\; 2/3\,,$$
$$x \notin L \implies \Pr_r[\exists\, a\; V(x,r,a) = 1] \;\leq\; 1/3\,.$$

Here $V(x,r,a) = 1$ if the verdict is accept and 0 if the verdict is reject. Of course, V must be computable in time $\text{poly}(|x|)$ and we must have $|r| \leq \text{poly}(|x|)$ and $|a| \leq \text{poly}(|x|)$.

The complexity class MA is like AM, except that Merlin speaks first. In the above notation, both parties receive x, then Merlin provides Arthur with a "proof" a, and finally, Arthur uses a random string r, along with x and a, to compute his verdict. The required properties of this verdict are:

$$x \in L \implies \exists\, a\; \Pr_r[V(x,a,r) = 1] \;\geq\; 2/3\,,$$
$$x \notin L \implies \forall\, a\; \Pr_r[V(x,a,r) = 1] \;\leq\; 1/3\,.$$

25. How does MA relate to NP and to BPP? Prove your answers. Also, explain why the specific choice of error probability (which is $1/3$ in the above definitions) is not crucial in the above definition of MA.
[2 points]

26. Give a full formal proof that MA $\subseteq$ AM. [2 points]