Homework 11
Due Mon May 23, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

25. Recall from class the definitions of the complexity classes AM and MA. The definitions set the soundness and completeness probabilities to $\frac{1}{3}$ and $\frac{2}{3}$ respectively.

    - Give a complete formal proof that $\mathsf{MA} \subseteq \mathsf{AM}$. As mentioned in class, your proof will most likely use an error-reduction-by-repetition step somewhere to bring the error of the MA protocol down to $2^{-\Theta(m)}$, where m is the length of Merlin's message.
    - Argue how to extend your proof to show that $\mathsf{MAM} \subseteq \mathsf{AM}$. Then extend it further to prove the Babai-Moran Theorem, which states that $\mathsf{AM}[k] = \mathsf{AM}$ for every constant k.

    [2 points]

26. The AM protocol for GNI (Graph Non-Isomorphism) that we gave in class had the annoying property that its completeness was imperfect. Give an alternative AM protocol for GNI that has perfect completeness.

    [2 points]

    [Hint: Suppose we have got to a situation where Arthur has to distinguish between $|T| \le k$ and $|T| \ge ck$, for some *large* value c. The protocol in class worked with $c = 2$, which is not large, so you'll have to do some "preprocessing". Now consider applying a hash function (chosen from a suitable 2-universal hash family) mapping the universe containing T to $\{0,1\}^{k'}$, with $k' \approx ck$. Following an idea used in the proof of the Sipser-Gács Theorem, Arthur has to tell whether or not a small number of hashed images of T (corresponding to *several* hash functions) can together cover $\{0,1\}^{k'}$. Formalize this reasoning; be precise about the value of k', the necessary proability inequalities, etc. Finally, describe what interaction between Arthur and Merlin will enable Arthur to tell the two cases apart.]