University of Maryland
CMSC652 — Complexity Theory
Professor Jonathan Katz

Problem Set 5

Due at the *beginning* of class on Dec. 8

1. What complexity class that we have seen previously is equal to $\mathcal{IP}[0]$?

2. Consider the following definition of the class $\mathcal{IP}^*$: a language L is in $\mathcal{IP}^*$ if there exist (P, V) with V running in probabilistic polynomial time such that:

   - If $x \in L$ then $\Pr[\langle P, V\rangle(x) = 1] \geq 3/4$.
   - If $x \notin L$ then $\Pr[\langle P, V\rangle(x) = 1] = 0$.

   Prove that $\mathcal{IP}^* = \mathcal{NP}$.

3. Show an **AM** protocol for the following promise problem:

$$\begin{aligned} \Pi_Y &= \{(\phi, k) \mid \#SAT(\phi) > 8k\} \\ \Pi_N &= \{(\phi, k) \mid \#SAT(\phi) < k/8\}. \end{aligned}$$

   I.e., when $x \in \Pi_Y$ then the prover should be able to convince the verifier with probability 1 while if $x \in \Pi_N$ then the prover should be unable to convince the verifier with probability better than 1/2. (*Hint*: it will be easier to construct an **AM** protocol with non-zero completeness error first....) Why doesn't this show that $\#\mathcal{P} \subseteq$ **AM**?

4. Sketch an interactive proof system for $\Sigma_2 = \mathcal{NP}^{\mathcal{NP}}$ *without* relying on the $\mathsf{PSPACE} \subseteq \mathcal{IP}$ result. *Hint*: use the proof system for co$\mathcal{NP}$ that we showed in class as a black box...

5. Work out *in full* an execution of the interactive proof system for PSPACE that we showed in class (assuming an honest prover), for the true statement:

$$\phi = \forall x_1 \exists x_2 : (x_1 \vee \bar{x}_2) \bigwedge (\bar{x}_1 \vee x_2).$$

   What is the smallest prime q that the parties can use for this ϕ to guarantee soundness error at most 1/2 (recall that the verifier can compute the arithmetization of ϕ, too...)?