University of Maryland
CMSC652 — Complexity Theory
Professor Jonathan Katz

Problem Set 4

Due at the *beginning* of class on Oct. 20

1. In class we gave two different definitions of co$\mathcal{RP}$ (see lecture 5). Show that they are equivalent.

2. (a) Prove that $\mathcal{RP}$ is closed under union and intersection. (A complexity class $\mathcal{C}$ is *closed* under some operation $\circ$ if $L_1, L_2 \in \mathcal{C}$ implies $L_1 \circ L_2 \in \mathcal{C}$.)

   (b) Extend your proof from above to show that $\mathcal{BPP}$ is closed under union and intersection

   (c) We will discuss complexity class $\mathcal{PP}$ in a subsequent lecture, but for now the definition alone will suffice: Say $L \in \mathcal{PP}$ if there exists a PPT machine M such that

   $$x \in L \Rightarrow \Pr[M(x) = 1] > 1/2 \quad \text{and} \quad x \notin L \Rightarrow \Pr[M(x) = 1] < 1/2.$$

   Does your proof technique from the previous two parts extend to show that $\mathcal{PP}$ is closed under union and intersection? If so, fill in the details and complete the proof that $\mathcal{PP}$ is closed under union and intersection. If not, describe in 1–2 sentences what goes wrong.

3. Consider the following language L:

   $$L \stackrel{\text{def}}{=} \left\{ \langle M, x, 1^t \rangle \mid \begin{array}{c} M \text{ is a probabilistic T.M.} \\ \text{which accepts } x \text{ with probability at least } 2/3 \text{ within } t \text{ steps} \end{array} \right\}.$$

   (a) Show that L is $\mathcal{BPP}$-hard, where this is defined in the natural way.

   (b) Consider the following algorithm for deciding L: on input $\langle M, x, 1^t \rangle$, choose a random tape ω uniformly at random and run $M(x; \omega)$ for at most t steps. Accept iff this results in acceptance. Does this prove that $L \in \mathcal{BPP}$? Why or why not?

4. Extending what we showed in class for $\mathcal{RP}$, show how to perform error reduction for $\mathcal{BPP}$ using pairwise-independent random sources. Specifically, given a PPT algorithm M which uses m random bits and errs with probability at most $1/3$, **describe** and **analyze** a PPT algorithm that errs with probability at most $2^{-q(|x|)}$ (for some given $q = O(\log |x|)$) but uses only $O(\max\{q, m\})$ random bits.

5. Given a language B, let

$$[x \in B] \stackrel{\text{def}}{=} \begin{cases} 1 & x \in B \\ 0 & x \notin B \end{cases}.$$

Say that A is $1-tt$-reducible to B if there are two poly-time functions f, g such that

$$x \in A \Leftrightarrow [f(x) \in B] = g(x).$$

(An easier way of expressing the above is that this is just a Turing reduction from A to B, but where the machine is only allowed *one* query to the oracle for B.) Show by modifying the proof of Mahaney's theorem that if an $\mathcal{NP}$-complete language is $1-tt$ reducible to a sparse set, then $\mathcal{P} = \mathcal{NP}$.

6. Show that if $\mathsf{PH} = \mathsf{PSPACE}$ then the polynomial hierarchy collapses to some level. (*Hint*: use the fact that PSPACE has complete languages.)