Advanced Complexity Theory Dan Spielman
18.405/6.841
Due: Tuesday, May 1st, 2001

Problem Set 3

1. Prove that $PCP(poly, poly) \subseteq NEXP$ and $PCP(log, log) \subseteq NP$.

2. **(Re-using random bits)** In this problem, we'll see a simpler but less efficient way to recycle random bits than that which we covered in class. Let A be a BPP algorithm (i.e. it either accepts with prob $> 2/3$ or $< 1/3$) that uses $f(n)$ random bits on words of length n. Let H be a pairwise-independent family of hash functions from $\{0,1\}^{f(n)}$ to $\{0,1\}^{f(n)}$. Rather than running A many times with new random bits to reduce the error-probability, we will run A many times with pseudo-random bits generated using the hash functions.

   To run A $k(n)$ times, we will first choose a random $h \in H$. We then associate each number between 1 and $k(n)$ with it's binary representation of length $p(n)$ (i.e., pad with 0's). We then run A $k(n)$ times, using the $f(n)$ bits given by $h(i)$ on the i-th run. Accept if A accepts on the majority of its runs.

   Prove that the probability of error of this algorithm is at most $8/k$. (Hint: use Chebyshev's inequality.)

   (Note that if we used the smallest known families of hash functions, then we would only use $2f(n)$ random bits, whereas $k(n)f(n)$ random bits would usually be required to run A $k(n)$ times. However, the error-probability we obtain is not as good as that which we would get by running A with independently chosen random bits.)

3. **(Hitting sets for combinatorial rectangles)** Let H be a pairwise independent family of hash functions from $\{0,1\}^n$ to $\{0,1\}^n$. Let $\epsilon = 2^{-n/3}$. Show that for all $A, B \subseteq \{0,1\}^n$, for all but an ϵ fraction of $h \in H$,

$$\left| \operatorname*{Prob}_{y \in \{0,1\}^n}[y \in A \text{ and } h(y) \in B] - \operatorname*{Prob}_{y,z \in \{0,1\}^n}[y \in A \text{ and } z \in B] \right| \leq \epsilon.$$

   Hint: use Chebyshev's inequality.

4. For a complexity class $\mathcal{C}$, define the operator "coR$\cdot$" by $L \in \text{coR} \cdot \mathcal{C}$ if there exists an $L' \in \mathcal{C}$ and a polynomial $p(n)$ such that for all $x \in \{0,1\}^n$,

   (a) if $x \in L$ then for all strings y of length $p(n)$, $(x,y) \in L'$, and
   (b) if $x \notin L$ then for at least two-thirds of strings y of length $p(n)$, $(x,y) \notin L'$.

   Show that $\text{BP} \cdot \Sigma \cdot P = \text{coR} \cdot \Sigma \cdot P$. (that is, we can assume that AM proofs have one-sided error) If you cannot prove this, try to prove that graph-nonisomorphism is in $AM(k)$ with one-sided error, for some constant k.

Homework policy:

Same as before.