Homework-3 (Computational Complexity)

**Due date: Dec 11 (in class)**
Collaboration is encouraged. However the writeup should be your own. You should cite all collaborators and any other references that you might be using.

1. Let ZPP be the class of languages $L$ that can be decided by a probabilistic Turing machine $M$ that halts on each input in expected polynomial time, and for each input $x$, $\Pr[M(x) = L(x)] = 1$. Prove that $ZPP = RP \cap \text{co-RP}$.

2. Show that if $NP \subseteq PCP(r(n),1)$, for $r(n) = o(\log n)$ then $P = NP$. [Exercise 11.8 in Arora-Barak].

3. Show that the class IP with soundness 0 (i.e. for all $x$ not in the language $L$, the verifier $V$ always rejects) equals NP. [Exercise 8.1(d) in Arora-Barak].

4. Prove that there exists a perfectly complete $AM[O(1)]$ protocol for proving a lower bound on set size. In other words modify the Goldwasser-Sipser set lower bound protocol we gave in class to make it have completeness 1. [Exercise 8.5 in Arora-Barak]

5. Let $k \leq n$, and let $\mathcal{H}_{n,k}$ be the following collection of functions from $\{0,1\}^n \rightarrow \{0,1\}^k$. Identify $\{0,1\}$ with the field $GF(2)$ (i.e. integers mod 2). For every $k \times n$ matrix $A$ with entries in $\{0,1\}$ and for every vector $b \in \{0,1\}^k$, let $h_{A,b} : \{0,1\}^n \rightarrow \{0,1\}^k$ be the function such that $h_{A,b}(x) = Ax + b$. Let $\mathcal{H}_{n,k}$ be the set of all such $h_{A,b}$. Prove that $\mathcal{H}_{n,k}$ is a pair-wise independent family of functions. [Exercise 8.4 in Arora-Barak]