6.045J/18.400J: Automata, Computability and Complexity Nancy Lynch, Nati Srebro
Homework 11 (Fake)
Due: Never — *Susan Hohenberger*

Readings: Sipser, Section 10.2 (omitting the subsection on primality).

The following table summarizes the requirements on the behavior of machines for languages in several probabilistic classes. A language L is in a specified class if and only if there exists a probabilistic polynomial time Turing machine that accepts words in L with the specified probability, and rejects words not in L with the specified probability.

Class	Probability of accepting $w \in L$	Probability of rejecting $w \notin L$
P	1	1
NP	> 0	1
coNP	1	> 0
BPP	$> \frac{2}{3}$	$> \frac{2}{3}$
RP	$> \frac{2}{3}$	1
coRP	1	$> \frac{2}{3}$
PP	$\geq \frac{1}{2}$	$> \frac{1}{2}$

Problem 1: Recall the definition of PP: A language $L \in$ PP if and only if there exists a probabilistic polynomial time Turing machine such that:

· If $w \in L$, then $\Pr[M \text{ accepts } w] \geq \frac{1}{2}$.
· If $w \notin L$, then $\Pr[M \text{ accepts } w] < \frac{1}{2}$.

Show that:

1. BPP $\subseteq$ PP.
2. NP $\subseteq$ PP.
3. PP $\subseteq$ PSPACE.

Hint for (2): Consider a nondeterministic TM for L, and replace rejections with probabilistic decisions.

Problem 2: The class RP is the class of languages L for which there is a probabilistic Turing machine M that always terminates in polynomial time, and such that for all $w \notin L$, M *always* reject w, and for all $w \in L$, M accepts w with probability at least $\frac{2}{3}$. The class coRP is the class of languages whose complement is in RP.

So far, we have only discussed machines that *always* terminate in polynomial time, but that give a correct answer only with some probability. Here we consider machines that *always* give the right answer when they terminate, but that run in time that is only polynomial on average.

Show that for any language $L \in$ RP $\cap$ coRP there is a probabilistic Turing machine M that runs in expected polynomial time (i.e., the expected number of steps until M terminates is bounded by a polynomial), and that when w terminates it accepts if and only if $w \in L$.

This class RP $\cap$ coRP is called ZPP for "zero probability polynomial".