CS401 - Problem Set 9

1. Show that there is a language $\mathsf{B} \in \mathbf{EXP}$ such that $\mathbf{NP}^{\mathsf{B}} \neq \mathbf{P}^{\mathsf{B}}$.

2. The class **ZPP** (zero-error probabilistic polynomial time) is another variant on **BPP**:

   Definition. $L \in \mathbf{ZPP}$ if there exists a probabilistic TM (PTM) M such that if

   $$x \in L \leftrightarrow \Pr[(M(x) = 1)] = 1 \tag{1}$$
   $$x \notin L \leftrightarrow \Pr[(M(x) = 1)] = 0 \tag{2}$$

   and for all x, $M(x)$ terminates in polynomial time ***on average***.

   The idea with **ZPP** is that it always outputs the right answer, and usually it takes polynomial time, but it can sometimes take much longer. However, the likelihood of it taking a long time is small.

   Another way of defining **ZPP**, which we'll call $\mathbf{ZPP}_2$ is as follows:

   Definition. $L \in \mathbf{ZPP}$ if there exists a probabilistic TM (PTM) M that can output the symbols $\{0, 1, ?\}$, where if

   $$x \in L \rightarrow M(x) \in \{1, ?\} \tag{3}$$
   $$x \notin L \rightarrow M(x) \in \{0, ?\} \tag{4}$$
   $$\tag{5}$$

   and for all x, the probability that $M(x)$ outputs '?' is less than $1/2$, and M runs in polynomial time.

   (a) Prove that $\mathsf{ZPP} = \mathsf{ZPP}_2$

   (b) Explain the significance of part (a).

   (c) Prove $\mathbf{ZPP} \in \mathbf{RP} \cap \mathbf{coRP}$. Note that **RP** always terminates in polynomial time.