CR09 – Homework 1
Due date: October 11

Recall that BPP_α is the class of languages $\mathscr{L}$ for which there is a probabilistic polynomial-time Turing machine M such that:

- If $x \in \mathscr{L}$, $\Pr[M(x) = 1] \geq \alpha(|x|)$, and
- If $x \notin \mathscr{L}$, $\Pr[M(x) = 0] \geq \alpha(|x|)$

In class, we defined $\mathsf{BPP} := \mathsf{BPP}_{2/3}$

Question 0 (1 points). Given a function f, the class P^f (resp. NP^f) is the class of languages decided by a polynomial time oracle Turing machine M (resp. nondeterministic polytime oracle Turing machine) with oracle access to f (that is, M can compute in 1 step the evaluation of f on any input written on the tapes). The class E (resp. EXP) is the class of languages decided by Turing machines running in time $2^{O|x|}$ (resp. $2^{O(|x|^c}$ for some constant $c > 0$). Show the following:

$$\forall f \in \mathsf{P}, \mathsf{P}^f = \mathsf{P} \qquad\qquad \mathsf{P}^\mathsf{E} = \mathsf{NP}^\mathsf{E} = \mathsf{EXP}$$

Hint: show $\mathsf{P}^\mathsf{E} = \mathsf{EXP}$, using a padding argument (cf. the simplified proof of Ladner's theorem in the first course).

Question 1 (1 points). Show that for any polynomial p,

$$\mathsf{BPP} = \mathsf{BPP}_{1/2+1/p(|x|)}$$

Question 2 (1 points). Show that

$$\mathsf{BPP} = \mathsf{BPP}_{1-2^{-|x|^2}}$$

Question 3 (1 points). Recall that $\mathsf{AM}[k]$ is the class of languages $\mathscr{L}$ that admit a public coin $k(|x|)$-round interactive proof system. As for BPP, we denote by $\mathsf{AM}_\alpha[k]$ the class of languages with an $\mathsf{AM}[k]$ protocol with completeness and soundness error bounded by $\alpha(|x|)$. Again, using the latter notation, in class, we defined $\mathsf{AM} = \mathsf{AM}_{2/3}$. Show that for any polynomial k,

$$\mathsf{AM}[k] = \mathsf{AM}_{1-2^{-|x|^2}}[k]$$

Question 4 (3 points). Let $\ell : \mathbb{N} \to \mathbb{N}$. A *Turing machine with advice of length* ℓ is a Turing machine M together with an infinite sequence $(a_n)_{n\in\mathbb{N}}$ with $a_n \in \{0,1\}^{\ell(n)}$ for every $n \in \mathbb{N}$. The *evaluation* of a TM M with advice $(a_n)_{n\in\mathbb{N}}$ on input x is the output of $M(x, a_{|x|})$. Let $\mathsf{P}(\ell)$ denote the class of languages decided by a polynomial-time Turing machine M with advice of size ℓ, and let $\mathsf{P}(\mathsf{poly}) = \cup_{\text{polynomial } p}\mathsf{P}(p)$. Show that

$$\mathsf{P}/\mathsf{poly} = \mathsf{P}(\mathsf{poly})$$

Question 5 (3 points). Define $\mathsf{NP}/\mathsf{poly} = \mathsf{NP}(\mathsf{poly})$ to be the class of languages decided by a *nondeterministic* Turing machine M with advice of polynomial size: $\mathscr{L} \subseteq \mathsf{NP}/\mathsf{poly}$ if there exists a (deterministic) polytime TM M and infinite polysize advice sequence $(a_n)_{n\in\mathbb{N}}$ such that $\mathscr{L} = \{x \mid \exists w, |w| = \mathsf{poly}(|x|) \wedge M(x, w, a_{|x|}) = 1\}$. Show that

$$\mathsf{AM}[2] \subseteq \mathsf{NP}/\mathsf{poly}$$

Hint: use an averaging argument, similar to the proof of $\mathsf{BPP} \subseteq \mathsf{P}/\mathsf{poly}$ seen in class, and use the non-determinism in the same spirit as in the proof of $\mathsf{IP} \subseteq \mathsf{NPSPACE}$ seen in class.