Problem Set 10

This problem set is due on **Wednesday May 2, by 5:00pm.**

Use the CS172 drop box.

Write **your name and your student ID number** on your solution. Write legibly. The description of your proofs should be as *clear* as possible (which does not mean *long* – in fact, typically, good clear explanations are also short.) Be sure to be familiar with the collaboration policy, and read the overview in the class homepage `www.cs.berkeley.edu/~luca/cs172`.

1. (a) Show that TQBF is complete for **PSPACE** also under logspace reductions.
   (*Hint:* The solution is not lengthy or tedious. Do not try to give the full logspace reduction. Instead, take a second look at the reduction done in class.)

   (b) Show that $TQBF \notin \mathbf{NL}$.

2. Consider the function $pad : \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ defined as $pad(s, l) = s\#^j$, where $j = \min(0, l - |s|)$. Thus, $pad(s, l)$ just adds enough copies of the new symbol $\#$ to the end of the string s so that the length of the new string is at least l. For a language A and a function $f : \mathbb{N} \to \mathbb{N}$, define the language $pad(A, f(n))$ to be

$$pad(A, f(n)) = \{pad(s, f(|s|)) \mid s \in A\}$$

   (a) Prove that if $A \in \mathbf{TIME}(n^6)$, then $pad(A, n^2) \in \mathbf{TIME}(n^3)$.
   (*Note:* This part will not be graded as we proved this in section. You need not submit the solution to this, but you can attempt this part to understand the definition.)

   (b) (Sipser 9.14) Define $\mathbf{EXPTIME} = \mathbf{TIME}(2^{n^{O(1)}})$ and $\mathbf{NEXPTIME} = \mathbf{NTIME}(2^{n^{O(1)}})$. Use the function pad to prove that

$$\mathbf{NEXPTIME} \neq \mathbf{EXPTIME} \Rightarrow \mathbf{P} \neq \mathbf{NP}$$

3. Recall that we defined **IP** as the class of languages A, such that for a polynomial time verifier V and provers P

$$w \in A \Rightarrow \exists P \ \mathbf{Pr}[V \leftrightarrow P \text{ accepts } w] = 1$$
$$w \notin A \Rightarrow \forall P \ \mathbf{Pr}[V \leftrightarrow P \text{ accepts } w] \leq 1/2$$

   (a) Let $\mathbf{IP}'$ be the class of languages where we allow the prover to be probabilistic i.e. the prover can use randomness. Show that $\mathbf{IP}' = \mathbf{IP}$.

   (b) Let $\mathbf{IP}'$ be the class of languages where we replace the 1/2 in the definition above by 0 i.e. the verifier must surely reject in case $w \notin A$. Show that $\mathbf{IP}' = \mathbf{NP}$.