COMP 531 - Fall 2021 - Assignment 2

Due: Oct 25, 11:59pm

- Each student must find and write their own solution. Copying solutions from any source, completely or partially, allowing others to copy your work, will not be tolerated, and will be reported to the disciplinary office. You are allowed to discuss the problems with each other without revealing your solution to each other.
- You must submit your solutions as **one readable pdf file** to mycourses.
- Your grade will be based on the mathematical correctness of your solution as well as the quality of your presentation.

---

1. Let A be an oracle such that $\mathsf{P}^A = \mathsf{NP}^A$. Prove that there is an oracle such that $\mathsf{P}^{A,B} \neq \mathsf{NP}^{A,B}$.
2. Define L to be the language, consisting of triples of polynomials (p_1, p_2, p_3) (given as arithmetic circuits) such that exactly two of the polynomials are equal. Show that $L \in \mathsf{BPP}$. It is not known whether L is in RP or coRP.
3. Prove that
$$\mathsf{NP} \subseteq \mathsf{BPP} \iff \mathsf{NP} = \mathsf{RP}.$$
4. A language $L \subseteq \{0,1\}^*$ is sparse if there is a polynomial $p(n)$ such that $|L \cap \{0,1\}^n| \leq p(n)$ for every n. Show that every sparse language is in $\mathsf{P/poly}$.
5. Prove that if there is a polynomial time oracle Turing Machine M^{SAT} that takes two CNF's ϕ_1 and ϕ_2 and outputs their satisfiability correctly using *only one* oracle query to SAT, then $\mathsf{P} = \mathsf{NP}$.
6. Prove that there are languages $A, B \in \mathsf{EXP}$ such that $A \leq_T^p B$ but $A \not\leq_p B$. (Hint: Construct A and B such that $n \in A$ if and only if either $2n \in B$ or $2n+1 \in B$, and use a diagonalization argument.)