COMP 590: Computational Complexity **Spring 2026**

Problem Set 2

Instructions: You **must** typeset your solution in LaTeX using the provided template. Please submit your problem set via Canvas. Include your name and the names of any collaborators at the top of your submission.

Name:
Collaborators:

Acknowledgment: Most problems come from the Arora Barak textbook and are reproduced here for convenience and typo fixes.

Problem 1: Primes. Let $\mathsf{PRIMES} = \{n : n \text{ is prime}\}$. Note that in fact $\mathsf{PRIMES} \in \mathbf{P}$, but we will not prove that. Instead, we will prove that $\mathsf{PRIMES} \in \mathbf{NP} \cap \mathbf{coNP}$.

(a) Show that $\mathsf{PRIMES} \in \mathbf{coNP}$.

Hint: show that the complement of the language is in **NP**. Argue that this means the language itself is in **coNP**.

(b) Show that $\mathsf{PRIMES} \in \mathbf{NP}$. You can use the following math fact: a number n is prime if and only if for every prime factor q of $n-1$, there exists a number $a \in \{2, ..., n-1\}$ satisfying $a^{n-1} = 1 \pmod{n}$ but $a^{(n-1)/q} \neq 1 \pmod{n}$.

Hint: the certificate that n is prime is the list of prime factors $q_1, ... q_\ell$ of $n-1$ along with the corresponding numbers $a_1, ..., a_\ell$ and (recursive) primality certificates for $q_1, ..., q_\ell$. You will need to show that this is indeed a polynomial-sized certificate and describe the machine M that verifies it.

(c) Suppose someone were to prove that PRIMES is **coNP**-complete (we do not think this is the case). What would be the consequence for the relationship between **NP** and **coNP**?

Problem 2: Same but Bigger. Recall that we defined **NEXP** as $\cup_{c \geq 1} \mathbf{NTIME}(2^{n^c})$. We say that a language is **NEXP**-complete if it is in **NEXP** and every language in **NEXP** is polynomial-time reducible to it.

(a) Give a witness-style definition of **NEXP**, akin to the one we have for **NP**, and prove that it is equivalent to our original definition.

(b) Describe a **NEXP**-complete language L.

Hint: consider the following **NP**-complete language, which is proven to be **NP**-complete in Section 2.2 of the textbook. Here M_α refers to the deterministic Turing machine described by the string α.

$$\mathsf{TMSAT} = \left\{(\alpha, x, 1^n, 1^t) : \exists u \in \{0,1\}^n \text{ s.t. } M_\alpha \text{ outputs 1 on input } (x, u) \text{ within } t \text{ steps}\right\}$$

(c) Prove that if $L \in \mathbf{EXP}$, then $\mathbf{NEXP} = \mathbf{EXP}$.

Problem 3: Quantified Formulas.

(a) Prove that if **P** = **NP**, then **NP** = **coNP**.

(b) Consider the decision problem Σ_2^{SAT}: given a quantified formula ψ of the form

$$\psi = \exists_{x \in \{0,1\}^n} \forall_{y \in \{0,1\}^m} \varphi(x, y) = 1,$$

where φ is a CNF formula, decide whether ψ is true. That is, decide whether there exists an x such that for every y, $\varphi(x, y)$ is true.

Prove that if **P** = **NP**, then $\Sigma_2^{\mathsf{SAT}} \in$ **P**. Do this without using generic results about the polynomial hierarchy collapsing to the first level if **P** = **NP**.

(c) Theorem 5.4 in the Arora-Barak textbook states the following:

1. For every $i \geq 1$, if $\Sigma_i^p = \Pi_i^p$, then **PH** = Σ_i^p, i.e., the polynomial hierarchy collapses to the ith level.
2. If **P** = **NP**, then **PH** = **P**; that is, the hierarchy collapses to **P**.

The book proves the second part of the theorem. Complete the proof of the theorem by proving the first part.

Optional Feedback. Please answer the following questions to help design future problem sets. You are not required to answer these questions, and if you would prefer to answer anonymously, please use the anonymous feedback form. However, we do encourage you to provide feedback on how to improve the course experience.

(a) Roughly how long did you spend on this problem set?

(b) What was your favorite problem on this problem set?

(c) What was your least favorite problem on this problem set?

(d) Any other feedback for this problem set? Was it too easy/difficult?

(e) Any other feedback on the course so far?