COMP 590: Computational Complexity **Spring 2026**

Problem Set 1

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: Machine with Concrete. The MIT museum contains a sculpture by Arthur Green called *Machine with Concrete* (see book for a photo). It consists of 13 gears connected to one another in a series such that each gear moves 50 times slower than the previous one. The fastest gear is constantly rotated by an engine at a rate of 212 rotations per minute. The slowest gear is fixed to a block of concrete and so apparently cannot move at all. Explain why this machine does not break apart.

Problem 2: Unary Factoring. Recall that normally we assume that numbers are represented as a string using the *binary* basis. That is, a number n is represented by the sequence $x_0, x_1, ..., x_{\log n}$ such that $n = \Sigma_{i=0}^{\log n} x_i 2^i$. However, we could have used other encoding schemes. If $n \in \mathbb{N}$ and $b \geq 2$, then *the representation of n in base b*, denoted by $\llcorner n \lrcorner_b$, is obtained as follows: first, represent n as a sequence of digits in $\{0, ..., b-1\}$, and then replace replace each digit d by its binary representation. The *unary* representation of n, denoted by $\llcorner n \lrcorner_1$, is the string 1^n, i.e., a sequence of n ones.

(a) Show that choosing a different base of representation will make no difference to the class **P**. That is, show that for every subset S of the natural numbers, if we define $L_S^b = \{\llcorner n \lrcorner_b : n \in S\}$, then for every $b \geq 2$, $L_b^s \in \mathbf{P}$ if and only if $L_2^S \in \mathbf{P}$.

(b) Show that choosing the unary representation may make a difference by showing that the following language, is in **P**.

$$\mathsf{UNARYFACTORING} = \left\{\llcorner n \lrcorner_1, \llcorner \ell \lrcorner_1, \llcorner k \lrcorner_1, : \text{ there is a prime } j \in (\ell, k) \text{ dividing } n.\right\}$$

This problem is not known to be in **P** if we choose the binary representation, and in fact some well-known cryptographic algorithms rely on the assumption that it is not in **P** for the binary representation. Later

Problem 3: Asymmetric Relations. We have defined a relation $\leq_p$ among languages. This relation is *reflexive*, i.e., $L \leq_p L$ for all languages L, and *transitive*, i.e., if $L \leq_p L'$ and $L' \leq_p L''$, then $L \leq_p L''$. Show that it is not *symmetric*, namely $L \leq_p L'$ does not imply that $L' \leq_p L$.

Problem 4: Quadratic Equations

(a) Let QUADEQ be the language consisting of all sets of satisfiable *quadratic equations* over 0/1 variables where addition is modulo 2. A quadratic equation over variables $u_1, ..., u_n$ has the form $\Sigma_{i,j \in [n]} a_{i,j} u_i u_j = b$. Show that QUADEQ is **NP**-complete.

Hint: reduce from 3SAT. Start by showing this for *cubic* equations. Then show that you can introduce an intermediate variable to replace each cubic equation with two quadratic equations.

(b) Let REALQUADEQ be the language of all satisfiable sets of quadratic equations over *real* variables. Show that REALQUADEQ is **NP**-hard.

Hint: you can express the constraint $x \in \{0, 1\}$ using the equation $x^2 = x$.

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?