St. Francis Xavier University
Department of Computer Science

CSCI 541: Theory of Computing
Assignment 2
Due March 13, 2025 at 1:30pm

Assignment Regulations.

- This assignment may be completed individually or in a group of two people. If you are collaborating on an assignment as a group, your group must submit exactly one joint set of answers.
- Please include your full name and email address on your submission. For groups, every member must include their full name and email address on the joint submission.
- You may either handwrite or typeset your submission. If your submission is handwritten, please ensure that the handwriting is neat and legible.

[8 marks] 1. Let $\mathsf{LINSPACE} = \mathsf{DSPACE}(n)$ denote the class of decision problems solvable in deterministic linear space (i.e., $O(n)$ space). Prove that $\mathsf{P} \neq \mathsf{LINSPACE}$.

Hint. Use the space hierarchy theorem.

[8 marks] 2. Prove that the complexity class coNP is closed under polynomial-time reductions. That is, show that if $A \leq_m^P B$ and $B \in \mathsf{coNP}$, then $A \in \mathsf{coNP}$.

[10 marks] 3. Suppose you have a Las Vegas randomized algorithm solving a given problem in expected polynomial time. Show that you can always convert this to a Monte Carlo randomized algorithm solving the same problem with one-sided error in polynomial time.

Hint 1. Remember that your Monte Carlo algorithm must produce a correct answer with probability $\geq 1/2$. This probability can be modelled by the expression $\mathbb{P}[T_{\mathrm{LV}}(n) < T_{\mathrm{MC}}(n)]$, where $T_{\mathrm{LV}}(n)$ is the runtime of the Las Vegas algorithm and $T_{\mathrm{MC}}(n)$ is the runtime of the Monte Carlo algorithm.

Hint 2. Building on the previous hint, you may find *Markov's inequality* useful: given a nonnegative random variable X and a value $a > 0$, we have that $\mathbb{P}[X \geq a] \leq \mathbb{E}[X]/a$.

[8 marks] 4. Recall the definition of the class coRP:

$$\mathsf{coRP} = \{\Sigma^* \setminus L \mid L \subseteq \Sigma^*, L \in \mathsf{RP}\}.$$

Prove that if $\mathsf{coRP} \subseteq \mathsf{RP}$, then $\mathsf{RP} = \mathsf{coRP}$.

[6 marks] 5. Say that a language L belongs to the complexity class $\mathsf{IP}[k]$ for $k \geq 1$ if L has an interactive protocol where at most k rounds of communications are exchanged between the prover and the verifier.

(a) Prove that $\mathsf{NP} \subseteq \mathsf{IP}[1]$.

(b) Explain why it seems likely that there exists some constant k such that $\mathsf{IP}[k] \neq \mathsf{NP}$.