We may grade a **subset of the assigned questions**, to be determined after the deadline, so that we can provide better feedback on the graded questions.
Unless otherwise stated, each question requires sufficient justification to convince the reader of the correctness of your answer.
For bonus questions, we will not provide any insight during office hours or Piazza, and we do not guarantee anything about the difficulty of these questions.
We strongly encourage you to typeset your solutions in LaTeX.
If you collaborated with someone, you must state their name(s). You must write your own solution for all problems and may not look at any other student's write-up.

0. If applicable, state the name(s) and uniqname(s) of your collaborator(s).

Solution:

1. In this question we examine the validity of verifiers and deciders for showing membership in NP or P.

   (a) Recall

   $$L_{\text{ACC}} = \{(\langle M \rangle, x) : M \text{ is a TM that accepts } x\}$$

   Is the program V a verifier for L_{ACC}, where the certificate $C \geq 1$ is an integer represented in binary? (Hint: Is V efficient?) Show why or why not.

   V = "On input $(\langle M \rangle, x, C)$:
   1. Run M on x for C steps
   2. If M accepts x in those C steps, ACCEPT. Else, REJECT."

   Solution:

   (b) Define

   $$\textsf{First-Digit-Factorial} = \{n \in \mathbb{N} : \text{the first digit of the decimal representation of } n! \text{ is } 2\},$$

   where the first digit is the most significant digit. Does F show that First-Digit-Factorial $\in$ P? Show why or why not.

   F = "On input n:
   1. $product \leftarrow 1$
   2. For i from 2 to n
   3. $\quad product \leftarrow product \cdot i$
   4. $digit \leftarrow product$
   5. While $digit \geq 10$
   6. $\quad digit \leftarrow \lfloor digit/10 \rfloor$
   7. If $digit = 2$, ACCEPT. Else REJECT."

   Solution:

2. Show that the following languages are in the class NP.

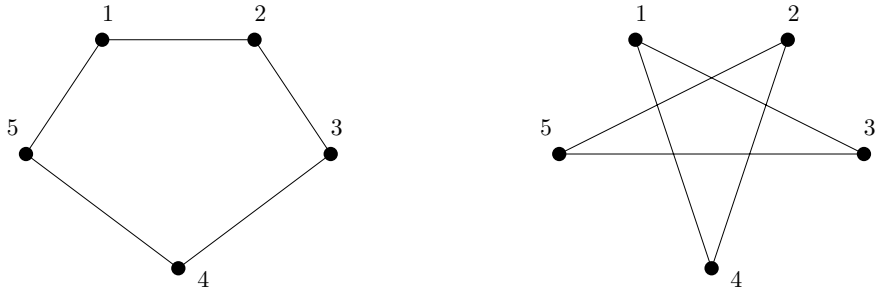
   Note: To prove that a language is in NP, you must provide a verifier and prove that your verifier satisfies correctness and efficiency.

   (a) Ham-Cycle $= \{\langle G \rangle : G$ is an undirected graph with a Hamiltonian cycle$\}$.
   Note: a Hamiltonian cycle for a graph is a path that visits each node exactly once and ends at the starting node.

   Solution:

   (b) For two graphs $G = (V, E)$, $G' = (V', E')$, an *isomorphism* between them is a bijection $\gamma \colon V \to V'$ such that $(a, b) \in E$ if and only if $(\gamma(a), \gamma(b)) \in E'$. Similarly, G and G' are said to be *isomorphic* if there exists an isomorphism between them.

   For example, the following two graphs are isomorphic, by the bijection γ where $\gamma(1) = 1, \gamma(2) = 3, \gamma(3) = 5, \gamma(4) = 2, \gamma(5) = 4$.



   Define Graph-Isomorphism $= \{(\langle G \rangle, \langle H \rangle) : G, H$ are isomorphic graphs$\}$.

   Solution:

   (c) Define Not-Prime $= \{n \in \mathbb{N} :$ n is not a prime number$\}$

   Solution:

3. (a) Let A, B be two languages in P. Then show the language $A \cup B$ is also in P.

   Solution:

   (b) Let A, B be two languages in NP. Then show the language $A \cup B$ is also in NP.

   Solution:

   (c) Let $A, B \in$ P. Define $AB = \{ab : a \in A, b \in B\}$ where ab denotes the concatenation of a and b. For example, if $a = 100111$ and $b = 0011$ are bitstrings then $ab = 1001110011$. Show that $AB \in$ P.

Solution:

4. This question explores the complexity class $\mathsf{coNP} = \left\{\overline{L} \;\middle|\; L \in \mathsf{NP}\right\}$. Conceptually, NP contains the languages whose "yes" instances can be verified efficiently, whereas coNP contains the languages whose "no" instances can be verified efficiently.

   (a) Prove that P is closed under set complement. That is, for any $L \in \mathsf{P}$, we have $\overline{L} \in \mathsf{P}$.

   Solution:

   (b) Use part (a) to prove that if $\mathsf{P} = \mathsf{NP}$, the following set inclusions hold: (i) $\mathsf{NP} \subseteq \mathsf{coNP}$ (that is, for any $L \in \mathsf{NP}$, we have $L \in \mathsf{coNP}$), and (ii) $\mathsf{coNP} \subseteq \mathsf{NP}$.

   Solution:

   (c) Conclude from part (b) that if $\mathsf{NP} \neq \mathsf{coNP}$, then $\mathsf{P} \neq \mathsf{NP}$.

   Solution: