**E0 224: Computational Complexity Theory**
**Indian Institute of Science**
**Assignment 1**

**Due date: Sep 16, 2025** **Total marks: 50**

---

**General instructions:**

- Write your solutions furnishing all relevant details. You may assume the results proved in the class.
- You are encouraged to solve the problems yourself.
- If you discuss with someone or consult material (other than course lecture notes), then please ensure that you understand the solutions completely before writing them in our own language. Please put appropriate citations stating clearly whom or what you have consulted and how it has benefited you.
- If you need any other clarification, please contact the instructor.

---

1. (**8 marks**)
   (a) (**3 marks**) Let QUADEQ be the language of all satisfiable sets of quadratic equations over $\mathbb{F}_2$. A quadratic equation in variables $u_1, ..., u_n$ has the form $\sum_{i,j\in[n]} a_{i,j}u_iu_j + \sum_{i\in[n]} a_iu_i = b$ where addition is modulo 2. Show that QUADEQ is NP-complete.
   (b) (**5 marks**) Design a deterministic polynomial-time algorithm to solve the 2SAT problem (i.e., when every clause of the input CNF formula has at most 2 literals).
2. (**8 marks**) Let PARTITION $= \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \text{there exists } S \subset [n] \text{ such that } \sum_{i\in S} x_i = \sum_{i\neq S} x_i\}$. Prove that PARTITION is NP-complete.
3. (**6 marks**) Let PRIMES $= \{n : n \text{ is a prime}\}$. Show that PRIMES $\in$ NP. You may use the following fact: A number $n$ is prime if and only if there exists a number $a \in \{2, ..., n-1\}$ satisfying $a^{n-1} = 1 \mod n$ and for every prime factor $r$ of $n-1$, $a^{\frac{n-1}{r}} \neq 1 \mod n$.
4. (**6 marks**) Let $f : \mathbb{Z} \to \mathbb{Z}$ be a bijection that maps $n$-bit integers to $n$-bit integers. Such a $f$ is a *one-way function* if $f$ is polynomial-time computable, but $f^{-1}$ is not. Show that if $f$ is a one-way function, then the language $L_f := \{(x, y) : f^{-1}(x) < y\} \in \text{NP} \cap \text{co-NP}$, but $L_f$ is not in P.
5. (**7 marks**) Assuming P $\neq$ NP $\cap$ co-NP, prove that there exist a NP verifier $M$ and a polynomial function $p$ such that $L(M) = \{x : \exists u \in \{0,1\}^{p(|x|)} \text{ such that } M(x, u) = 1\}$ is in P but the corresponding search problem cannot be solved in polynomial time.
6. (**6 marks**) Consider the following variant of the graph isomorphism problem: given two graphs $H = (U, F)$ and $G = (V, E)$ (not necessarily having the same number of vertices), check if there is a one-to-one map (i.e., an injection) $\phi : U \to V$ such that $(u_1, u_2) \in F$ if and only if $(\phi(u_1), \phi(u_2)) \in E$. Prove that this variant of the graph isomorphism problem is NP-complete.
7. (**9 marks**) Prove that there exists a language $B$ such that $\text{NP}^B \neq \text{co-NP}^B$.