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

**Due date: Sep 20, 2024** **Total marks: 40**

1. (**9 marks**)
   (a) (**3 marks**) Let QUADEQ be the language of all satisfiable sets of quadratic equations over 0/1 variables (a quadratic equation over $u_1, ..., u_n$ 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 $\mathsf{NP}$-complete.
   (b) (**6 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. (**7 marks**) Let PARTITION $= \{(x_1, \ldots, x_n) \in \mathbb{Z}^n$ : there exists $S \subset [n]$ such that $\sum_{i\in S} x_i = \sum_{i\neq S} x_i\}$. Prove that PARTITION is $\mathsf{NP}$-complete.
3. (**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 $L_f := \{(x, y) : f^{-1}(x) < y\} \in \mathsf{NP} \cap \mathsf{co\text{-}NP}$, but $L_f$ is not in $\mathsf{P}$.
4. (**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 $\mathsf{NP}$-complete.
5. (**12 points**) Two languages $L_1, L_2 \subseteq \{0, 1\}^*$ are said to be *p-isomorphic* if there is a bijection $f : \{0, 1\}^* \to \{0, 1\}^*$ such that $x \in L_1 \iff f(x) \in L_2$ and $f$ and $f^{-1}$ are polynomial-time computable. A language $L$ is *sparse* if there exists a constant $c$ such that for every integer $n \geq 1$, the number of strings of length $n$ belonging to $L$ is bounded by $n^c$.
   (a) (**4 points**) Show that if $\mathsf{NP}$-complete languages are p-isomorphic to each other, then $\mathsf{P} \neq \mathsf{NP}$.
   (b) (**8 points**) Show that if a sparse language is $\mathsf{NP}$-complete, then $\mathsf{P} = \mathsf{NP}$.