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

Due date: Sep 16, 2022 **Total marks: 50**

1. (**6 marks**)
   (a) (**2 marks**) Let $L_1, L_2 \in \mathsf{NP}$. Are $L_1 \cup L_2$ and $L_1 \cap L_2$ also in NP?
   (b) (**4 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 $\sum_{i,j\in[n]} a_{i,j} u_i u_j + \sum_{i\in[n]} a_i u_i = b$) where addition is modulo 2. Show that QUADEQ is NP-complete.
2. (**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).
3. (**6 marks**) Let PRIMES $= \{n \ : \ n \text{ is a prime}\}$. Show that PRIMES $\in \mathsf{NP}$. 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 $L_f := \{(x, y) \ : \ f^{-1}(x) < y\} \in \mathsf{NP} \cap \mathsf{co\text{-}NP}$, but L_f is not in P.
5. (**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.
6. (**9 marks**) Prove that there exists a language B such that $\mathsf{NP}^B \neq \mathsf{co\text{-}NP}^B$.
7. (**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 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 NP-complete, then $\mathsf{P} = \mathsf{NP}$.