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

Due date: Nov 15, 2020   **Total marks: 50**

1. (**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. (**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 for every prime factor r of $n-1$, there exists a number $a \in \{2, ..., n-1\}$ satisfying $a^{n-1} = 1 \mod n$ but $a^{\frac{n-1}{r}} \neq 1 \mod n$.

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 $L_f := \{(x, y) \ : \ f^{-1}(x) < y\} \in$ NP $\cap$ co-NP, but L_f is not in P.

4. (**7 marks**) In the SUBSET SUM problem, we are given a list of numbers $a_1, ..., a_n$ and a number T and need to decide whether there exists a subset $S \subseteq [n]$ such that $\sum_{i \in S} a_i = T$. Prove that SUBSET SUM is NP-complete.

5. (**10 marks**) Prove that there exists a language B such that NP$^B \neq$ co-NP^B.

6. (**8 marks**) A directed graph $G = (V, E)$ is *strongly connected* if for every two nodes $u, v \in V$, there are paths from u to v and from v to u in G. Show that the following language is NL-complete,

$$\{G \ : \ G \text{ is a strongly connected directed graph}\}.$$

7. (**8 marks**) Prove that in the read-once certificate definition of NL, if we allow the verifier machine to move its head back and forth on the certificate then the class being defined changes to NP.