Tutorial 02 – The class NP (Group 2)

Exercise 1. *Boolean circuits*

Let $f_n \colon \{0,1\}^n \to \{0,1\}$ be the function defined as

$$f_n(x_1,\ldots,x_n) := \begin{cases} 1 & \text{if } x_1 + \cdots + x_n \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

1. Draw a boolean circuit that computes f_0, f_1, f_2. What can you say about f_2?
2. Show that f_n can be computed by a circuit of size and depth $O(n)$.

Exercise 2. *One-Way Functions*

Definition. A *one-way function* f is a bijection of $\{0,1\}^\star \to \{0,1\}^\star$ that satisfies the following two conditions. First, for all $n \in \mathbb{N}$, $f_{|n \text{ bits}}$ is also a bijection. Second, f can be evaluated in polynomial time in $|x|$, but f^{-1} cannot be evaluated in polynomial time.

1. Which of the following are one-way functions?
   - $f(x) := g(x)||g(x)$ where g is a one-way function.
   - $f(x) := g(g(x))$ where g is a one-way function
2. Prove that if *one-way functions* exist, then $\mathsf{P} \neq \mathsf{NP}$.

✈ The question of the reciprocal is still an open problem.

Exercise 3. NP-*Completeness*

Show that the following languages are NP-complete.

1. NDTM-T: given $\langle \alpha, x, 1^t \rangle$, does the nondeterministic Turing machine M_α accept on input x in time $\leqslant t$?
   Hint: You can admit that there exists a universal nondeterministic Turing Machine.
2. IndSet: given $\langle G = (V,E), k \rangle$, is there a set S of k independent vertices (i.e. $\forall i,j \in S, i \neq j \implies (i,j) \notin E$)?
3. 3-SAT: Does a 3CNF formula ϕ have a satisfying assignment?
   You can admit that CNF-SAT *is* NP*-complete.*

Exercise 4. *Tally Language (Berman's Theorem, 1974)*

A language is said to be *tally* (or unary), if it is included in a unary alphabet $\{a\}^*$ for a fixed symbol a.

Definition (Subset-Sum)**.** Given n numbers $v_1, \ldots, v_n \in \mathbb{Z}$, and a *target* number $T \in \mathbb{Z}$, we need to decide whether there exists a nonempty subset $S \subseteq [\![1,n]\!]$ such that $\sum_{i \in S} v_i = T$. The problem size is $|T|_2 + \sum_{i=1}^n |v_i|_2$.

1. Prove that Subset-Sum is NP-complete.
2. Let Unary-Subset-Sum be the tally variant of Subset-Sum where all numbers are represented by their unary representation. Show that Unary-Subset-Sum is in P.
3. Show that if there exists an NP-hard tally language, then $\mathsf{P} = \mathsf{NP}$.