School of Mathematical and Computational Sciences Indian Association for the Cultivation of Science

Master's/Integrated Master's-PhD Program/ Integrated Bachelor's-Master's Program/PhD Course

Theory of Computation II: COM 5108

Tutorial IV (07 September 2023)

Instructor: Goutam Biswas

Autumn Semester 2023

- 1. An *enumerator* Turing machine (ETM) is one that enumerates strings of a language. It does not take any input. Prove that a language is Turing recognizable if and only if it is enumerable by some ETM.
- 2. Let $L_1, L_2 \subseteq \Sigma^*$ be Turing recognizable languages.
 - (a) Show that $L_1 \cap L_2$ is Turing recognizable.
 - (b) Show that $L_1L_2 = \{x \in \Sigma^* : \exists u, v, x = uv, u \in L_1, v \in L_2\}$ is Turing recognizable.

What is your conclusion?

- 3. Let $L_1, L_2 \subseteq \Sigma^*$ be in **P**.
 - (a) Show that $L_1 \cup L_2$ is in **P**.
 - (b) Show that L_1L_2 is in **P**.

What is your conclusion?

- 4. Let $L_1, L_2 \subseteq \Sigma^*$ be in **NP**.
 - (a) Show that $L_1 \cup L_2$ is in **NP**.
 - (b) Show that L_1L_2 is in **NP**.

What is your conclusion?

5. Consider the following algorithm where $a \in \mathbb{Z}_n$, n and E are positive integers. The binary representation of E is $(e_{k-1}e_{k-2}\cdots e_1e_0)$.

 $\begin{array}{ll} \operatorname{what}(a,e,n) \\ 1 & v \leftarrow 1 \\ & s \leftarrow a \bmod n \\ & \operatorname{while} e \geq 1 \\ & \operatorname{if} (e \bmod 2) = 1 \operatorname{then} v \leftarrow (v \times s) \bmod n \\ & s \leftarrow s^2 \bmod n \\ & e \leftarrow e \div 2 \\ & \operatorname{return} v \end{array}$

- (a) What is the length of the input?
- (b) Compute what (10, 10, 7).
- (c) What does it compute?
- (d) Analyze the time complexity.