Computational Complexity

Handout – Lecture 9

Definition 1 (Probabilistic TMs)**.** *Probabilistic Turing machines (PTMs)* are variants of (deterministic) Turing machines, where a few elements are modified.

- Instead of one halting state q_{halt}, there are two halting states q_{acc} (the *accept state*) and q_{rej} (the *reject state*).
- Instead of a single transition function δ, there are two transition functions δ_1, δ_2.
- To execute a PTM on an input x, at each step, we use the transition function δ_1 with probability 1/2 and the transition function δ_2 with probability 1/2. At each step, this choice is made independently of all previous choices.
- The TM outputs only 0 (when halting in q_{acc}) or 1 (when halting in q_{rej}). We denote by $\mathbb{M}(x)$ the random variable corresponding to the value that the machine $\mathbb{M}$ outputs when executed on x.
- Let $T : \mathbb{N} \to \mathbb{N}$. The TM runs in time $T(n)$ if for every input x the machine halts after at most $T(|x|)$ steps, regardless of the random choices that it makes.

Definition 2 (BPTIME, BPP)**.** Let $T : \mathbb{N} \to \mathbb{N}$ be a function, and $L \subseteq \{0,1\}^*$ be a language. We say that a PTM $\mathbb{M}$ decides L in time $T(n)$ if for every $x \in \{0,1\}^*$, $\mathbb{M}$ halts in $T(|x|)$ steps, regardless of its random choices, and $\Pr[\mathbb{M}(x) = L(x)] \geq 2/3$.

The class BPTIME$(T(n))$ is the set of all languages decided by PTMs in time $O(T(n))$.

The class BPP is defined as follows:

$$\text{BPP} = \bigcup_{c \geq 1} \text{BPTIME}(n^c)$$

Definition 3 (BPP, alternative definition)**.** A language $L \subseteq \{0,1\}^*$ is in BPP if there exists a polynomial-time TM $\mathbb{M}$ and a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0,1\}^*$:

$$\Pr_{r \in_R \{0,1\}^{p(|x|)}}[\mathbb{M}(x,r) = L(x)] \geq 2/3$$

Definition 4 (RTIME, RP, coRP)**.** Let $T : \mathbb{N} \to \mathbb{N}$ be a function. The class RTIME$(T(n))$ contains every language $L \subseteq \{0,1\}^*$ for which there exists a PTM $\mathbb{M}$ running in time $O(T(n))$ such that:

$$\begin{array}{ll} \text{if } x \in L, & \text{then } \Pr[\mathbb{M}(x) = 1] \geq 2/3 \\ \text{if } x \notin L, & \text{then } \Pr[\mathbb{M}(x) = 0] = 1 \end{array}$$

The class RP is defined as follows:

$$\text{RP} = \bigcup_{c \geq 1} \text{RTIME}(n^c)$$

The class coRTIME($T(n)$) contains every language $L \subseteq \{0,1\}^*$ for which there exists a PTM $\mathbb{M}$ running in time $O(T(n))$ such that:

$$\begin{array}{ll} \text{if } x \in L, & \text{then } \Pr[\mathbb{M}(x) = 1] = 1 \\ \text{if } x \notin L, & \text{then } \Pr[\mathbb{M}(x) = 0] \geq 2/3 \end{array}$$

The class coRP is defined as follows:

$$\text{coRP} = \bigcup_{c \geq 1} \text{coRTIME}(n^c)$$

Alternatively:

$$\text{coRP} = \{ \ \overline{L} \mid L \in \text{RP} \ \}$$

Definition 5 (ZTIME, ZPP)**.** Let $T : \mathbb{N} \to \mathbb{N}$ be a function. The class ZTIME($T(n)$) contains every language $L \subseteq \{0,1\}^*$ for which there exists a PTM $\mathbb{M}$ running in expected time $O(T(n))$ such that for every input $x \in \{0,1\}^*$, whenever $\mathbb{M}$ halts on x, the output of $\mathbb{M}$ is exactly $L(x)$.

The class ZPP is defined as follows:

$$\text{ZPP} = \bigcup_{c \geq 1} \text{ZTIME}(n^c)$$