Chapter 8 - Probabilistic complexity classes

- Define probabilistic complexity classes
- Including **BPP**, **RP**, and **ZPP**
- Show how **BPP** relates to the polynomial time hierarchy, i.e. $\mathbf{BPP} \subseteq \Sigma_2 \cap \Pi_2$

Probabilistic algorithms - an example

- $\mathrm{MM} := \left\{(A, B, C) \in \mathbb{Z}_2^{n\times n} \times \mathbb{Z}_2^{n\times n} \times \mathbb{Z}_2^{n\times n} \,\middle|\, n \in \mathbb{N}, A \cdot B = C\right\}$
- $\overline{\mathrm{MM}} := \left\{(A, B, C) \in \mathbb{Z}_2^{n\times n} \times \mathbb{Z}_2^{n\times n} \times \mathbb{Z}_2^{n\times n} \,\middle|\, n \in \mathbb{N}, A \cdot B \neq C\right\}$

$M_{\overline{\mathrm{MM}}} =$ "On input $A, B, C \in \mathbb{Z}_2^{n\times n}$:

1. Choose $x \in \mathbb{Z}_2^n$ uniformly at random.
2. Compute $y := B \cdot x, z := A \cdot y, w := C \cdot x$.
3. *Accept*, if $z \neq w$, otherwise *reject*."

Lemma 8.1

For all $A, B, C \in \mathbb{Z}_2^{n\times n}$:

1. *if $(A, B, C) \notin \overline{MM}$, then $M_{\overline{MM}}$ rejects the triple (A, B, C) with probability 1,*
2. *if $(A, B, C) \in \overline{MM}$, then $M_{\overline{MM}}$ accepts the triple (A, B, C) with probability at least $1/2$.*

In both cases, the probability is over the choice of x.

Balanced Turing machines

Definition 8.2

We call an NTM $N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\mathrm{accept}}, q_{\mathrm{reject}})$ *balanced, if there is a function* $f : \mathbb{N} \to \mathbb{N}$ *such that for all* $x \in \Sigma^*$ *all computation branches of* N *on input* x *have length* $f(|x|)$ *and have for every nondeterministic step exactly two possible choices. We identify computation branches with elements in* $\{0,1\}^{f(|x|)}$*.*

Properties

- Every polynomial time NTM can be simulated by a balanced polynomial time NTM.
- If N is a balanced NTM such that computation branches on input x have length $p(|x|)$ for a polynomial $p : \mathbb{N} \to \mathbb{N}$, then we call N *p-balanced*.

The classes **RP**, co-**RP**, and **ZPP**

Definition 8.3

The class **RP** *consists of all languages L for which there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a p-balanced NTM N with the following properties:*

1. *If $w \notin L$, then all computation branches of N on input w reject.*
2. *If $w \in L$, then at least half of the computation branches of N on input w accept, i.e. on input w NTM N has at least $2^{p(|w|)-1}$ accepting computation branches.*

Definition 8.4

ZPP $:=$ **RP** $\cap$ *co*-**RP**.

The class **BPP**

Definition 8.5

The class **BPP** *consists of all languages L for which there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a p-balanced NTM N with the following properties:*

1. *If $w \notin L$, then at most $1/4$ of the computation branches of N on input w accept, i.e. for $w \notin L$ the NTM has at most $2^{p(|w|)-2}$ accepting computation branches.*
2. *If $w \in L$, then at least $3/4$ of the computation branches of N on input w accept, i.e. on input w NTM N has at least $3 \cdot 2^{p(|w|)-2}$ accepting computation branches.*

Amplifying the probabilities

Theorem 8.6

For $L \in \mathbf{BPP}$ there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a p-balanced NTM N with the following properties:

1. *If $w \notin L$, then N has at most $2^{-|w|} \cdot 2^{p(|w|)}$ accepting computation branches on input w.*
2. *If $w \in L$, then N has at least $\left(1 - 2^{-|w|}\right) \cdot 2^{p(|w|)}$ accepting computation branches on input w.*

BPP and the polynomial time hierarchy

Theorem 8.7

BPP $\subseteq \Sigma_2$.

Corollary 8.8

BPP $\subseteq \Sigma_2 \cap \Pi_2$.

Proof of Theorem 8.7

- Language $L \in \mathbf{BPP}$
- $p : \mathbb{N} \to \mathbb{N}$ polynomial and N p-balanced NTM with $L(N) = L$
- for $x \in \{0,1\}^*$ identify elements in $\{0,1\}^{p(|x|)}$ with computation branches of N on input x
- set

$$A(x) := \{w \in \{0,1\}^{p(|x|)} \mid w \text{ describes an } \textit{accepting} \text{ computation branch of } N \text{ on input } x\}$$

- from Theorem 8.6 we obtain

$$x \in L \Rightarrow |A(x)| \geq (1 - 2^{-|x|})2^{p(|x|)}$$
$$x \notin L \Rightarrow |A(x)| \leq 2^{-|x|}2^{p(|x|)}$$

Proof of Theorem 8.7

- for $S \subseteq \{0,1\}^{p(|x|)}$ and $t \in \{0,1\}^{p(|x|)}$ set

$$t \oplus S := \{t \oplus z \mid z \in S\}$$

- we show

$$x \in L \Rightarrow \exists t_1 \ldots, t_{p(|x|)} \in \{0,1\}^{p(|x|)} : \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x) = \{0,1\}^{p(|x|)}$$

$$x \notin L \Rightarrow \forall t_1 \ldots, t_{p(|x|)} \in \{0,1\}^{p(|x|)} : \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x) \neq \{0,1\}^{p(|x|)}$$

Proof of Theorem 8.7 - the case $x \notin L$

- $x \notin L \Rightarrow |A(x)| \leq 2^{-|x|}2^{p(|x|)}$

$\Rightarrow$

$$\left|\bigcup_{i=1}^{p(|x|)} t_i \oplus A(x)\right| \leq p(|x|)2^{-|x|}2^{p(|x|)}$$

for all $t_1, \dots, t_{p(|x|)}$

- wlog. assume $p(|x|)2^{-|x|} < 1$ (p is a polynomial)

$\Rightarrow$

$$x \notin L \Rightarrow \forall t_1 \dots, t_{p(|x|)} \in \{0,1\}^{p(|x|)} : \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x) \neq \{0,1\}^{p(|x|)}$$

Proof of Theorem 8.7 - the case $x \in L$

Proof strategy

- Use the *probabilistic method*, i.e.
- show that for $t_1, \ldots, t_{p(|x|)}$ chosen uniformly, independently at random

$$\Pr\left(\bigcup_{i=1}^{p(|x|)} t_i \oplus A(x) = \{0,1\}^{p(|x|)}\right) > 0$$

$\Rightarrow$ $t_1, \ldots, t_{p(|x|)}$ with $\bigcup_{i=1}^{p(|x|)} t_i \oplus A(x) = \{0,1\}^{p(|x|)}$ exist

Proof of Theorem 8.7 - the probabilistic argument

- fix $x \in L$ and choose $t_1, \ldots, t_{p(|x|)}$ uniformly, independently at random, probabilities over this choice
- for all i

$$\Pr\big(y \notin t_i \oplus A(x)\big) = \Pr\big(t_i \notin y \oplus A(x)\big) \leq 2^{-|x|},$$

since $|A(x)| = |y \oplus A(x)| \geq (1 - 2^{-|x|})2^{p(|x|)}$

- the t_i's are chosen independently, hence

$$\Pr\left(y \notin \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x)\right) \leq 2^{-|x|p(|x|)},$$

Proof of Theorem 8.7 - the probabilistic argument

- by union bound

$$\Pr\left(\exists y \in \{0,1\}^{p(|x|)} : y \notin \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x)\right) \leq 2^{p(|x|)} \cdot 2^{-|x|p(|x|)}$$

- assuming $|x| \geq 2$, we have $2^{p(|x|)} \cdot 2^{-|x|p(|x|)} < 1$

$\Rightarrow$

$$\Pr\left(\bigcup_{i=1}^{p(|x|)} t_i \oplus A(x) = \{0,1\}^{p(|x|)}\right) > 0$$

Proof of Theorem 8.7 - combining both cases

- overall

$$x \in L \Leftrightarrow \exists t = (t_1, \ldots, t_{p(|x|)}) \in \{0,1\}^{p(|x|)^2} \forall y \in \{0,1\}^{p(|x|)} :$$
$$y \in \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x).$$

- define language

$$A := \{(x, y, t) \in \{0,1\}^{|x| \times p(|x|) \times p(|x|)^2} \mid t = (t_1, \ldots, t_{p(|x|)}),$$
$$y \in \bigcup_{i=1}^{p(|x|)} t_i \oplus A(x)\}$$

Proof of Theorem 8.7 - combining both cases

- using A obtain

$$x \in L \Leftrightarrow \exists t = (t_1, \ldots, t_{p(|x|)}) \in \{0,1\}^{p(|x|)^2} \forall y \in \{0,1\}^{p(|x|)} : (x, y, t) \in A$$

- using Corollary 7.6 obtain $L \in \Sigma_2$