Chapter 7 - The Polynomial Time Hierarchy

- Relativized complexity classes.
- The classes in the polynomial time hierarchy (**PH**).
- Characterizations of classes in **PH**.
- **PH** and **PSPACE**

Relativized complexity classes

Let **C** be a class of languages. Then

$$\mathbf{P}(\mathbf{C}) := \{L \mid L \text{ can be decided by a deterministic polynomial time OTM } M^{?} \text{ with oracle } A \in \mathbf{C}.\}$$

$$\mathbf{NP}(\mathbf{C}) := \{L \mid L \text{ can be decided by a nondeterministic polynomial time OTM } M^{?} \text{ with an oracle } A \in \mathbf{C}.\}$$

The polynomial time hierarchy (**PH**)

Definition 7.1

Set $\Delta_0 = \Sigma_0 = \Pi_0 := \mathbf{P}$*. Inductively define for all* $k \in \mathbb{N}$*:*

1. $\Sigma_k = \mathbf{NP}(\Sigma_{k-1})$
2. $\Pi_k = co\text{-}\Sigma_k$
3. $\Delta_k = \mathbf{P}(\Sigma_{k-1})$

Definition 7.2

The class

$$\mathbf{PH} := \bigcup_{k \geq 0} \Sigma_k$$

is called the polynomial time hierarchy.

P, **NP**, co-**NP** and **PH**

Observation

- $\Delta_1 = \mathbf{P}$
- $\Sigma_1 = \mathbf{NP}$
- $\Pi_1 = \text{co-}\mathbf{NP}$

Minimal Boolean formulas and **PH**

Equivalence and minimality of Boolean formulas

- We call two Boolean formulas *equivalent*, if
  1. they have the same set of variables and
  2. they are true on the same set of assignments to those variables.
- A Boolean formula is called *minimal* if no shorter Boolean formula is equivalent to it.

Two languages

$\mathrm{MF} := \{\langle\phi\rangle \mid \phi \text{ is a minimal Boolean formula}\}$
$\overline{\mathrm{MF}} = \{\langle\phi\rangle \mid \phi \text{ is a not minimal Boolean formula}\}$

Observation

$\overline{\mathrm{MF}} \in \mathbf{NP}^{SAT}$, i.e. $\overline{\mathrm{MF}} \in \Sigma_2$ and $\mathrm{MF} \in \Pi_2$.

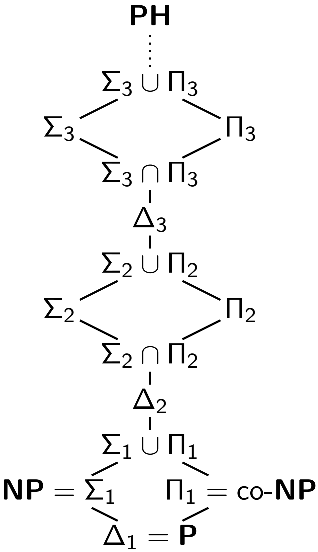
Inclusions inside of **PH**

Lemma 7.3

For all $k \in \mathbb{N}$

1. $\Delta_k = co\text{-}\Delta_k \subseteq \Sigma_k \cap \Pi_k \subseteq \Sigma_k \cup \Pi_k \subseteq \Sigma_{k+1}$
2. $\Sigma_k \cup \Pi_k \subseteq \Delta_{k+1}$

Illustration of inclusions



Alternative characterizations

Theorem 7.4

$L \in \Sigma_k$ if and only if there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a language $A \in \Pi_{k-1}$ with

$$L = \{x \mid \exists w \in \{0,1\}^{p(|x|)} : (x, w) \in A\}.$$

Corollary 7.5

$L \in \Pi_k$ if and only if there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a language $A \in \Sigma_{k-1}$ with

$$L = \{x \mid \forall w \in \{0,1\}^{p(|x|)} : (x, w) \in A\}.$$

Alternative characterizations

Corollary 7.6

$L \in \Sigma_k$ if and only if there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a language $A \in \mathbf{P}$ with

$$L = \left\{ x \;\middle|\; \begin{array}{l} \exists w_1 \in \{0,1\}^{p(|x|)} \forall w_2 \in \{0,1\}^{p(|x|)} \dots \\ Q_k w_k \in \{0,1\}^{p(|x|)} : (x, w_1, w_2, \dots, w_k) \in A \end{array} \right\},$$

here $Q_k = \exists$, if k is odd, and $Q_k = \forall$ otherwise.

Alternative characterizations

Corollary 7.7

$L \in \Pi_k$ if and only if there is a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a language $A \in \mathbf{P}$ with

$$L = \left\{ x \;\middle|\; \begin{array}{l} \forall w_1 \in \{0,1\}^{p(|x|)} \exists w_2 \in \{0,1\}^{p(|x|)} \ldots \\ Q_k w_k \in \{0,1\}^{p(|x|)} : (x, w_1, w_2, \ldots, w_k) \in A \end{array} \right\},$$

here $Q_k = \forall$, if k is odd, and $Q_k = \exists$ otherwise.

Consequences

Corollary 7.8

PH $\subseteq$ **PSPACE**.

Corollary 7.9

If there is a $k \in \mathbb{N}$ *with* $\Sigma_k = \Pi_k$*, then* $\Sigma_l = \Sigma_k = \Pi_k = \Pi_l$ *for all* $l \geq k$*, i.e. the polynomial time hierarchy collapses to its* k*-th level.*

Corollary 7.10

- *If* **NP** $=$ **P**, *then* **PH** $=$ **P**.
- *If* **NP** $=$ *co*-**NP**, *then* **PH** $=$ **NP**.

Proof of Theorem 7.4 $\Leftarrow$

- Let L be a language such that a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a language $A \in \Pi_{k-1}$ exist with

$$L = \{x \mid \exists w \in \{0,1\}^{p(|x|)} : (x, w) \in A\}.$$

- Consider the following OTM

$M_L^? =$ "On input x:

1. Nondeterministically choose $w \in \{0,1\}^{p(|x|)}$.
2. Write (x, w) onto the oracle tape.
3. From state q_{no} go to state q_{accept}, from state q_{yes} go to state q_{reject}."

Proof of Theorem 7.4 $\Leftarrow$

- Consider the following OTM

> $M_L^? =$ "On input x:
>
> 1. Nondeterministically choose $w \in \{0,1\}^{p(|x|)}$.
> 2. Write (x, w) onto the oracle tape.
> 3. From state q_{no} go to state q_{accept}, from state q_{yes} go to state q_{reject}."

- $L(M_L^{\bar{A}}) = L$
- $\bar{A} \in \Sigma_{k-1}$

$\Rightarrow$ $L \in \Sigma_k$

Proof of Theorem 7.4 $\Rightarrow$

- induction over k
- induction basis for $k = 1$, i.e. for $\Sigma_1 = \mathbf{NP}$
- follows from

Theorem 3.4

$L \subseteq \Sigma^*$ is in **NP**, *if and only if $k \in \mathbb{N}$ and $A \in$* **P** *exist with*

$$L = \left\{ x \in \Sigma^* \mid \exists z \in \{0,1\}^{|x|^k} : (x,z) \in A \right\}.$$

Proof of Theorem 7.4 $\Rightarrow$ (induction step)

Start from

$$L \in \Sigma_k \Rightarrow \begin{cases} \text{there is a polynomial time NOTM } M^? \\ \text{and a language } K \in \Sigma_{k-1} \text{ with } L\big(M^K\big) = L. \end{cases}$$

Induction hypothesis

$$K \in \Sigma_{k-1} \Rightarrow \begin{cases} \text{there is a polynomial } q : \mathbb{N} \to \mathbb{N} \\ \text{and a language } S \in \Pi_{k-2} \\ \text{with } K = \{z \mid \exists w \in \{0,1\}^{q(|z|)} : (z,w) \in S\}. \end{cases}$$

Computations of $M^?$

We say that a string $y \in \{0,1\}^*$ describes a computation of $M^?$ on input x if y fixes the nondeterministic choices of $M^?$ and fixes the answers to the oracle queries of $M^?$.

Proof of Theorem 7.4 $\Rightarrow$ (induction step)

Start from

$$L \in \Sigma_k \Rightarrow \begin{cases} \text{there is a polynomial time NOTM } M^? \\ \text{and a language } K \in \Sigma_{k-1} \text{ with } L\big(M^K\big) = L. \end{cases}$$

Induction hypothesis

$$K \in \Sigma_{k-1} \Rightarrow \begin{cases} \text{there is a polynomial } q : \mathbb{N} \to \mathbb{N} \\ \text{and a language } S \in \Pi_{k-2} \\ \text{with } K = \{z \mid \exists w \in \{0,1\}^{q(|z|)} : (z,w) \in S\}. \end{cases}$$

Computations of $M^?$

$$B := \{(x,y) \mid y \text{ describes an accepting computation of } M^? \text{ on input } x\}$$

Proof of Theorem 7.4 $\Rightarrow$ (induction step)

- $h : \mathbb{N} \to \mathbb{N}$ polynomial such that for all $x \in \{0,1\}^*$ an accepting computation of $M^?$ on input x can be described by a string $y \in \{0,1\}^{h(|x|)}$.
- $$x \in L \Leftrightarrow \exists y \in \{0,1\}^{h(|x|)}\colon \text{ } y \text{ describes an accepting computation of } M^? \text{ on input } x \text{ and the query answers contained in } y \text{ correspond to oracle } K.$$

Proof of Theorem 7.4 $\Rightarrow$ (induction step)

A refined version of language B

$$A := \{(x, y, w_1, \ldots, w_s) \mid (x, y) \in B,\ u_i \in \bar{K} \text{ for the oracle queries } u_1, \ldots, u_t \text{ that are answered with } q_{\text{no}} \text{ in } y \text{ and } (v_i, w_i) \in S \text{ for the oracle queries } v_1, \ldots, v_s \text{ in } y \text{ that are answered with } q_{\text{yes}} \text{ in } y.\}$$

Basic observation

$L = \{x \mid \exists z : (x, z) \in A\}$

Need to show: $A \in \Pi_{k-1}$.

Proof of Theorem 7.4 $\Rightarrow$ (induction step)

A refined version of language B

$$A := \{(x, y, w_1, \ldots, w_s) \mid (x, y) \in B,\ u_i \in \bar{K} \text{ for the oracle queries } u_1, \ldots, u_t \text{ that are answered with } q_{\mathrm{no}} \text{ in } y \text{ and } (v_i, w_i) \in S \text{ for the oracle queries } v_1, \ldots, v_s \text{ in } y \text{ that are answered with } q_{\mathrm{yes}} \text{ in } y.\}$$

$$(x, y, w_1, \ldots, w_s) \in \bar{A} \Leftrightarrow \begin{cases} (x, y) \in \bar{B} & \text{or} \\ \text{there is } i \in \{1, \ldots, t\} \text{ with } u_i \in K & \text{or} \\ \text{there is } i \in \{1, \ldots, s\} \text{ with } (v_i, w_i) \in \bar{S} \end{cases}$$

Proof of Theorem 7.4 $\Rightarrow$ (induction step)

$$(x, y, w_1, \ldots, w_s) \in \bar{A} \Leftrightarrow$$

$$\begin{cases} (x, y) \in \bar{B} & \text{or} \\ \text{there is } i \in \{1, \ldots, t\} \text{ with } u_i \in K & \text{or} \\ \text{there is } i \in \{1, \ldots, s\} \text{ with } (v_i, w_i) \in \bar{S} & \end{cases}$$

- $\bar{B} \in \Sigma_{k-1}$, since $B \in \mathbf{P}$;
- $K \in \Sigma_{k-1}$ by definition;
- $\bar{S} \in \Sigma_{k-1}$, since $S \in \Pi_{k-2}$ by induction hypothesis and $\Pi_{k-2} \subseteq \Pi_{k-1}$.

$\Rightarrow$ $\bar{A} \in \Sigma_{k-1}$, since Σ_{k-1} is closed under union

$\Rightarrow$ $A \in \Pi_{k-1}$