Semantic Polynomial Hierarchy
(compare Arithmetic/Borel Hierarchy)

Definition: $\Delta_0\mathbf{P} = \Sigma_0\mathbf{P} = \Pi_0\mathbf{P} := \mathbf{P}$

$$\Delta_{k+1}\mathbf{P} := \mathbf{P}^{\Sigma_k\mathbf{P}} = \mathbf{P}^{\Pi_k\mathbf{P}}$$

$$\Sigma_{k+1}\mathbf{P} := \mathbf{NP}^{\Sigma_k\mathbf{P}} = \mathbf{NP}^{\Pi_k\mathbf{P}}$$

$$\Pi_{k+1}\mathbf{P} := \mathbf{coNP}^{\Sigma_k\mathbf{P}} = \mathbf{coNP}^{\Pi_k\mathbf{P}}$$

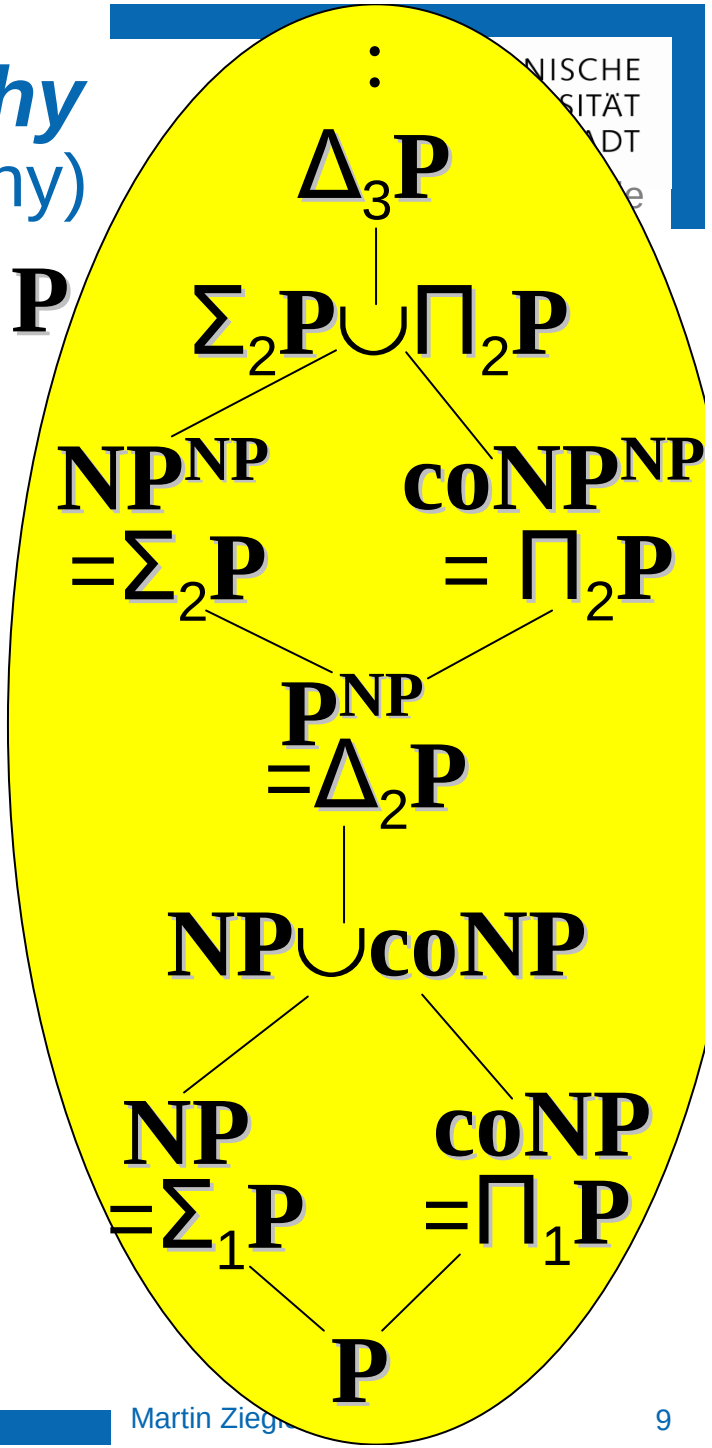
$$\mathrm{PH} := \bigcup \Sigma_k\mathbf{P}$$

Lemma: a) $\Delta_k\mathbf{P} = \text{co-}\Delta_k\mathbf{P}$

b) $\Delta_k\mathbf{P} \subseteq \Sigma_k\mathbf{P} \cap \Pi_k\mathbf{P}$

c) $\Sigma_k\mathbf{P} \cup \Pi_k\mathbf{P} \subseteq \Delta_{k+1}\mathbf{P}$

d) $\mathrm{PH} \subseteq \mathbf{PSPACE}$



Syntactic Polynomial Hierarchy

Theorem: a) $L \subseteq \{0,1\}^*$ belongs to **NP** iff

$L = \{ \underline{x} : \exists \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y} \rangle \in A \}$ for polyn. p and $A \in \mathbf{P}$

b) L belongs to Σ_{k+1} iff, for some polyn. p and $A \in \Pi_k$,

$L = \{ \underline{x} : \exists \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y} \rangle \in A \}$.

b) $\Leftrightarrow$ c)

c) L belongs to Π_{k+1} iff, for some polyn. p and $B \in \Sigma_k$,

$L = \{ \underline{x} : \forall \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y} \rangle \in B \}$

b) + c) $\Rightarrow$ d)

d) L belongs to Σ_k iff, for some polyn. p and $A \in \mathbf{P}$,

$L = \{ \underline{x} : \exists \underline{y}_1 \in \{0,1\}^{p(|\underline{x}|)} \; \forall \underline{y}_2 \in \{0,1\}^{p(|\underline{x}|)} \; \exists \underline{y}_3 \in \{0,1\}^{p(|\underline{x}|)} \; \ldots$

"$\exists$" if k odd, "$\forall$" else $\; Q \underline{y}_k \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y}_1, \underline{y}_2, \underline{y}_3, \ldots, \underline{y}_k \rangle \in A \}$

$\Sigma_{k+1}\mathbf{P} := \mathbf{NP}^{\Sigma_k \mathbf{P}}$ $\qquad$ $\Pi_{k+1}\mathbf{P} := \mathbf{coNP}^{\Sigma_k \mathbf{P}}$

Syntactic NP^O

Theorem: a) $L \subseteq \{0,1\}^*$ belongs to $\mathbf{NP}^O$ iff

$L = \{ \underline{x} : \exists \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y} \rangle \in A \}$ for polyn. p and $A \in \mathbf{P}^O$

b) L belongs to Σ_{k+1} iff, for some polyn. p and $A \in \Pi_k$,

$L = \{ \underline{x} : \exists \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y} \rangle \in A \}$

Σ'_{k+1}

Proof b) „$\Leftarrow$“: by induction on k, $L \in \Sigma_{k+1} = \mathbf{NP}^{\Sigma_k}$ $\surd$

„$\Rightarrow$“: induction $L \in \mathbf{NP}^{\Sigma_k} \Rightarrow L = \{\underline{x} : \exists \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x}, \underline{y} \rangle \in A\}$,

$A \in \mathbf{P}^{\Sigma_k}$ but $\notin \Pi_k$. Instead show: $\mathbf{P}^{\Sigma_k} \subseteq \Sigma'_{k+1}$ + Exercise

$A \in \mathbf{P}^{\Sigma_k}$ decided by $q(n)$-time DTM M^B, $B \in \Sigma_k = \Sigma'_k$: $A =$

$\{ \underline{z} : \exists \underline{v}_1, \ldots, \underline{v}_{q(|\underline{z}|)}, \underline{w}_1, \ldots, \underline{w}_{q(|\underline{z}|)} \in \{0,1\}^{q(|\underline{z}|)} : \langle \underline{z}, \underline{v}_1, \ldots, \underline{w}_{q(|\underline{z}|)} \rangle \in C \}$

$C := \{\langle \underline{z}, \underline{v}_1, \ldots, \underline{w}_m \rangle :$ $M^?$ accepts $\underline{z}$ querying only $\underline{v}_1, \ldots, \underline{w}_m$

and $\underline{v}_1, \ldots, \underline{v}_m \in B$ and $\underline{w}_1, \ldots, \underline{w}_m \notin B$ $\}$ $\in \Sigma'_{k+1}$ q.e.d.

Sipser–Gács–Lautemann

Theorem: $\mathbf{BPP} \subseteq \Sigma_2 \cap \Pi_2$ *„Derandomization“*

Notation: $\underline{y},\underline{z} \in \{0,1\}^m \Rightarrow \underline{y} \oplus \underline{z}$:= componentw. xor

Now fix $p(n)$-time NTM M for $L \in \mathbf{BPP}$.

For input $\underline{x}$, M guesses a random string $\underline{r} \in \{0,1\}^{p(n)}$.

$R_M(\underline{x})$:= { all $\underline{r} \in \{0,1\}^{p(n)}$ leading M to accept $\underline{x}$ } $\in \mathbf{P}$

- $\underline{x} \in L \Rightarrow \mathrm{Card}(R_M(\underline{x})) \geq (1-2^{-n}) \cdot 2^{p(n)}$
- $\underline{x} \notin L \Rightarrow \mathrm{Card}(R_M(\underline{x})) \leq 2^{-n} \cdot 2^{p(n)}$

→Exercise

Goal: $L = \{ \underline{x} \mid \exists \underline{t}_1,\ldots,\underline{t}_{p(|\underline{x}|)} \in \{0,1\}^{p(|\underline{x}|)} :$

$\forall \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \exists i=1,\ldots,p(|\underline{x}|): \underline{y} \oplus \underline{t}_i \in R_M(\underline{x}) \} \in \Sigma_2$

$\Leftrightarrow \{0,1\}^p \subseteq \bigcup_i (R_M(\underline{x}) \oplus \underline{t}_i)$

Erdős' Probabilistic Method

TECHNISCHE UNIVERSITÄT DARMSTADT
Komplexitätstheorie

Hypothesis: $R \subseteq \{0,1\}^p$, $\mathrm{Card}(R) \geq (1-2^{-n}) \cdot 2^p$

Claim: $\exists \underline{t}_1,\ldots,\underline{t}_p \in \{0,1\}^p : \forall \underline{y} \in \{0,1\}^p \quad \exists j \leq p: \ \underline{y} \oplus \underline{t}_j \in R$

Probablistic proof:

Consider random $\underline{t}_1,\ldots,\underline{t}_p$.

For any fixed $\underline{y} \in \{0,1\}^p$:

- $\Pr_{\underline{t}}[\ \underline{y} \oplus \underline{t} \notin R\ ] \leq 2^{-n}$
- $\Pr_{\underline{t}_1,\ldots,\underline{t}_r}[\ \forall j \leq p: \underline{y} \oplus \underline{t}_j \notin R\ ] \leq (2^{-n})^p$
- $\Pr_{\underline{t}_1,\ldots,\underline{t}_r}[\ \exists \underline{y} \in \{0,1\}^p: \forall j \leq p: \underline{y} \oplus \underline{t}_j \notin R\ ] \leq 2^p \cdot (2^{-n})^p < 1$

↓ Exercise

■