Relativized Complexity Classes

Reminder: Turing reduction, oracle-TM $M^?$ has state $q_?$ and query tape: for $O\subseteq\Sigma^*$, $q_?\to q_1$ if contents $\in O$, else $\to q_0$

Theorem (Baker, Gill, Solovay 1975):
There exist $A,B\subseteq\Sigma^*$ such that $\mathbf{P}^A=\mathbf{NP}^A$ and $\mathbf{P}^B\neq\mathbf{NP}^B$

Definition: Fix some class $\mathbf{C}$ of languages.

$\mathbf{P}^{\mathbf{C}}$:= { $L\subseteq\Sigma^*$ decided by polytime ODTM M^O, $O\in\mathbf{C}$}

$\mathbf{NP}^{\mathbf{C}}$:= { $L\subseteq\Sigma^*$ decided by polytime O**N**TM M^O, $O\in\mathbf{C}$}

Examples:

a) MinCircuit $\in$ $\mathbf{coNP}^{\mathrm{SAT}}=\mathbf{coNP}^{\mathbf{NP}}\subseteq\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ (Exercise)

b) $\mathbf{P}^{\mathbf{P}}=\mathbf{P}$, $\mathbf{NP}^{\mathbf{P}}=\mathbf{NP}$, $\mathbf{PSPACE}^{\mathbf{PSPACE}}=\mathbf{PSPACE}$

c) $\mathbf{NP}\cup\mathbf{coNP}\subseteq\mathbf{P}^{\mathbf{NP}}$; „≠“ unless $\mathbf{NP}=\mathbf{coNP}$ (Exercise)

Semantic Polynomial Hierarchy
(compare Arithmetic/Borel Hierarchy)

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

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

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

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

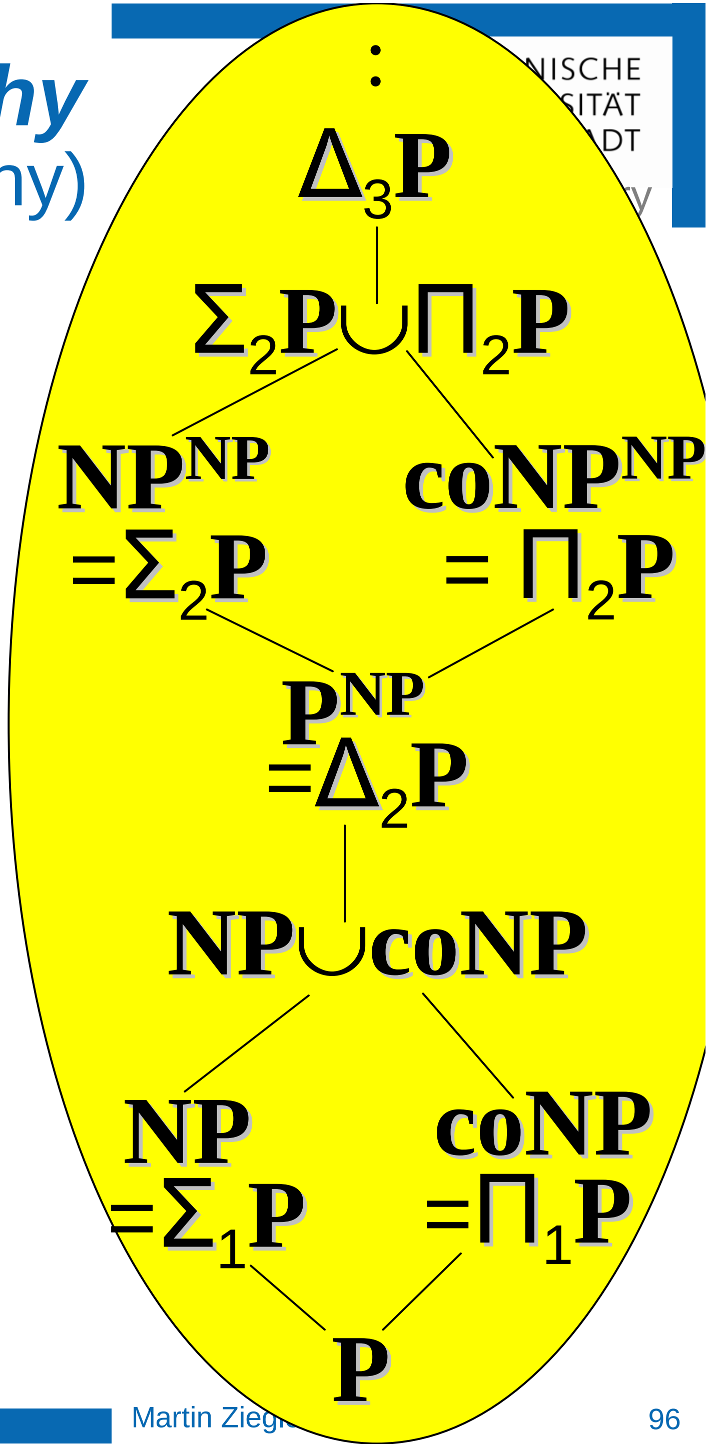
$\mathrm{PH} := \bigcup \Sigma_k\mathbf{P}$

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



Theorem: a) $L \subseteq \{0,1\}^*$ belongs to **NP** iff ($\surd$)
$L = \{ \underline{x} : \exists \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x},\underline{y} \rangle \in A \}$ 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 $A \in \mathbf{P}$,
$L = \{ \underline{x} : \exists \underline{y}_1 \in \{0,1\}^{p(|\underline{x}|)} \ \forall \underline{y}_2 \in \{0,1\}^{p(|\underline{x}|)} \ \exists \underline{y}_3 \in \{0,1\}^{p(|\underline{x}|)} \ \ldots$
$\ldots \ Q\underline{y}_k \in \{0,1\}^{p(|\underline{x}|)} : \langle \underline{x},\underline{y}_1,\underline{y}_2,\underline{y}_3,\ldots,\underline{y}_k \rangle \in A \}$

"$\exists$" if k odd, "$\forall$" else

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

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 $A\in\Pi_k$,
$L = \{\ \underline{x} : \exists \underline{y}\in\{0,1\}^{p(|\underline{x}|)} : \langle \underline{x},\underline{y}\rangle\in A\ \}$ $:\in\Sigma'_{k+1}$

Proof b) „⇐“: by induction on k, $L\in\mathbf{NP}^{\Pi_k} = \Sigma_{k+1}$ √
„⇒“: 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, $B\in\Sigma_k=\Sigma'_k$ (ind.hyp)
$A=$
$\{\ \underline{z} : \exists \underline{v}_1,\ldots,\underline{v}_{q(|\underline{z}|)},\underline{w}_1,\ldots,\underline{w}_{q(|\underline{z}|)}\in\{0,1\}^{q(|\underline{z}|)} : \langle \underline{z},\underline{v}_1,\ldots,\underline{w}_{q(|\underline{z}|)}\rangle\in C\ \}$
$C := \{\langle \underline{z},\underline{v}_1,\ldots,\underline{w}_m\rangle$: $M^?$ 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.