4. The polynomial hierarchy

4.1 Turing reductions

Definition 1.

Let $A \subseteq \Sigma^*$, $B \subseteq \Delta^*$ be sets. Then, A is said to be *polynomial-time Turing-reducible* to B (in symbols: $A \leq_T^P B$) if and only if $A \in P^B$.

Remark: $\leq_m^P$-reducibility is special case of $\leq_T^P$: one oracle query and no post-computation.

Proposition 2.

(1.) $A \leq_m^P B \Rightarrow A \leq_T^P B$.

(2.) $\leq_T^P$ is reflexiv and transitive

(3.) $A \leq_T^P \overline{A}$.

4.2 The oracle hierarchy

For $\tau : \mathbb{N} \to \mathbb{N}$ define following classes:

$P^B[\tau]$ =def class of all sets that can be accepted by a POTM asking $\leq \tau(|x|)$ queries to B on input x

$$P^B[\mathrm{Pol}\,\tau] =_{def} \bigcup_{k \geq 1} P^B[\tau^k]$$

$$P^B[O(\tau)] =_{def} \bigcup_{k \geq 1} P^B[k \cdot \tau]$$

We use obvious extensions to class $\mathcal{K}$ of oracles

Proposition 3.

For any $\tau : \mathbb{N} \to \mathbb{N}$ and any set B,
$P = P^B[0] \subseteq P^B[\tau] \subseteq P^B[\mathrm{Pol}\,n] = P^{B^P}$.

Definition 4.

The polynomial hierarchy consists of the following classes:

(1.) $\textcircled{H}_0^P = \Delta_0^P = \Sigma_0^P = \Pi_0^P =_{def} P$

(2.)
$$\textcircled{H}_{k+1}^P =_{def} P^{\Sigma_k^P[O(\log n)]}$$
$$\Delta_{k+1}^P =_{def} P^{\Sigma_k^P}$$
$$\Sigma_{k+1}^P =_{def} NP^{\Sigma_k^P}$$
$$\Pi_{k+1}^P =_{def} \mathrm{co}\,\Sigma_{k+1}^P$$

(3.) $$PH =_{def} \bigcup_{k \geq 0} \left(\textcircled{H}_k^P \cup \Delta_k^P \cup \Sigma_k^P \cup \Pi_k^P \right)$$

Theorem 5

(1.) $\Theta_1^P = \Delta_1^P = P$, $\Sigma_1^P = NP$, $\Pi_1^P = coNP$.

(2.) $co\Sigma_k^P = \Pi_k^P$, $co\Delta_k^P = \Delta_k^P = co\Theta_k^P = \Theta_k^P$.

(3.) $\Sigma_k^P \cup \Pi_k^P \subseteq \Theta_{k+1}^P \subseteq \Delta_{k+1}^P \subseteq \Sigma_{k+1}^P \cap \Pi_{k+1}^P$

(4.) $NP \subseteq PH \subseteq PSPACE$

Proof: (only 4.)

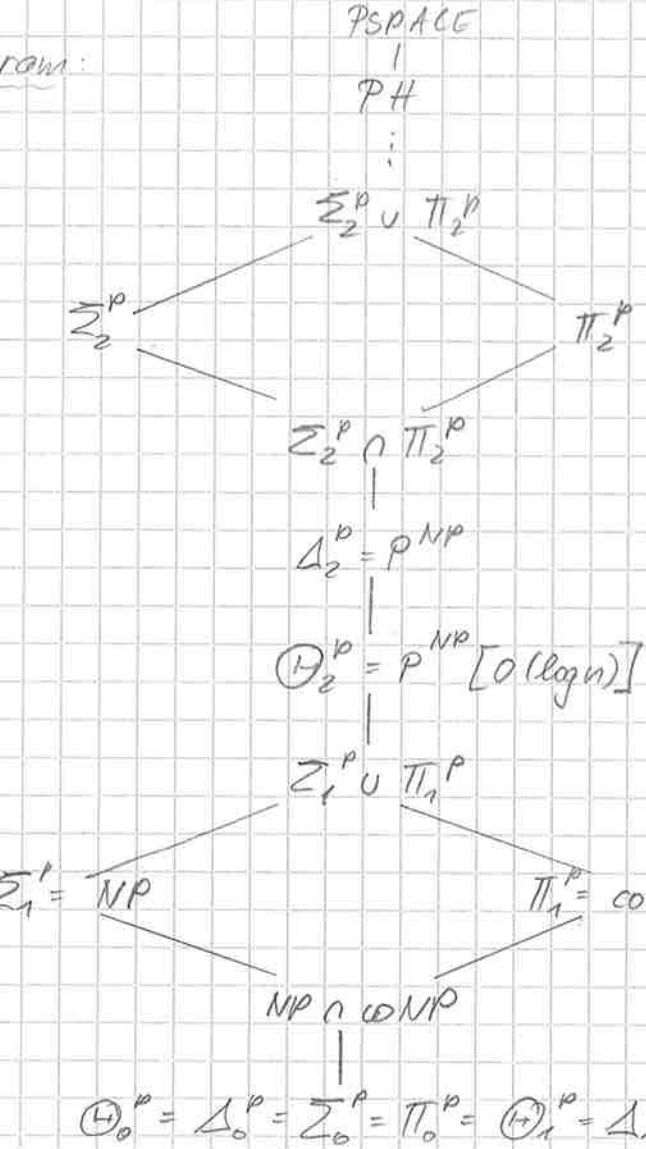
It is enough to show $\Sigma_k^P \subseteq PSPACE$: use induction

(i) base of induction $k=0$: $P \subseteq PSPACE$.

(ii) inductive step $k>0$:

$$\Sigma_k^P = NP^{\Sigma_k^P} \subseteq NP^{PSPACE} = PSPACE.$$

inclusion diagram:



Proposition 6.

(1.) Σ_k^p is closed under $\cap, \cup, \times, \exists^p_m$.

(2.) Π_k^p is closed under $\cap, \cup, \times, \forall^p_m$.

(3.) $\oplus_k^p, \Delta_k^p$ is closed under $\cup, \cap, \times, \exists^p_m$.

4.3 The quantifier hierarchy

For a set B, define

$$B_\wedge =_{def} \{ (x_1, \ldots, x_m) \mid m \geq 1,\ x_1 \in B \wedge \ldots \wedge x_m \in B \}$$
$$B_\vee =_{def} \{ (x_1, \ldots, x_m) \mid m \geq 1,\ x_1 \in B \vee \ldots \vee x_m \in B \}$$

Lemma 7.

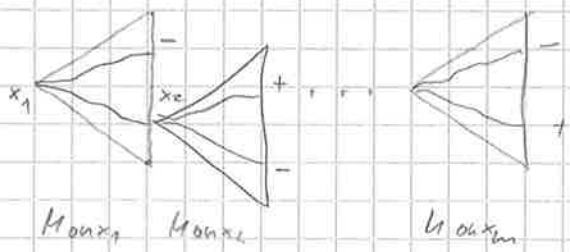
For any set B, $k \geq 0$, the following holds:

(1.) $B \in \Sigma_k^p \Rightarrow B_\wedge, B_\vee \in \Sigma_k^p$

(2.) $B \in \Pi_k^p \Rightarrow B_\wedge, B_\vee \in \Pi_k^p$

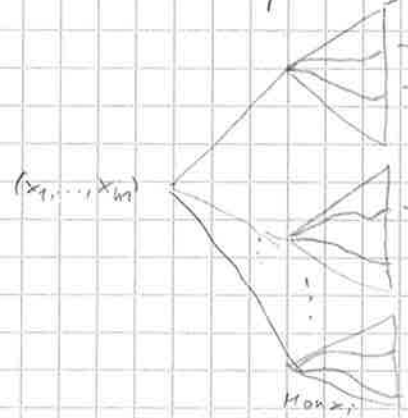
Proof: Statements are true for $k = 0$. Suppose $k > 0$.

(1.) Let $B \in \Sigma_k^p = NP^{\Sigma_{k-1}^p}$; i.e., there is NPTM M accepting B with oracle $D \in \Sigma_{k-1}^p$ in polynomial time p. Define $M_\wedge$ to be that NPTM that accepts B with oracle D as follows, on input $x = (x_1, \ldots, x_m)$:



running time
$\leq \sum_{i=1}^{m} p(|x_i|)$
$\leq |x| \cdot p(|x|)$

Define $M_\vee$ to be that NPTM that accepts B with oracle D as follows, on input $x = (x_1, \ldots, x_m)$:



running time.
$\leq |x| + p(|x|)$

(2.) $B \in \Pi_k^p \Rightarrow \overline{B} \in \Sigma_k^p \Rightarrow (\overline{B})_\Lambda = \overline{(B_\Lambda)} \in \Sigma_k \Rightarrow B_\Lambda \in \Pi_k^p$

$B \in \Pi_k^p \Rightarrow \overline{B} \in \Sigma_k^p \Rightarrow (\overline{B})_\Lambda = \overline{(B_\Lambda)} \in \Sigma_k^p \Rightarrow B_\Lambda \in \Pi_k^p$ ■

Let $\mathcal{K}$ be a class of sets. Define new classes:

$A \in \exists\mathcal{K} \Leftrightarrow_{def}$ there exist $B \in \mathcal{K}$ and polynomial p s.t.
$A = \{x \mid (\exists z, |z| = p(|x|))[(x,z) \in B]\}$

$A \in \forall\mathcal{K} \Leftrightarrow_{def}$ there exist $B \in \mathcal{K}$ and polynomial p s.t.
$A = \{x \mid (\forall z, |z| = p(|x|))[(x,z) \in B]\}$

Remark:

① $\exists P = NP$, $\forall P = coNP$

② $co\exists\mathcal{K} = \forall co\mathcal{K}$.

$A \in co\exists\mathcal{K} \Rightarrow \overline{A} \in \exists\mathcal{K} \Rightarrow \overline{A} = \{x \mid (\exists z, |z| = p(|x|))[(x,z) \in B]\}$
$\Rightarrow \overline{A} = \{x \mid (\forall z, |z| = p(|x|))[(x,z) \notin B]\}$
$\Rightarrow A = \{x \mid (\forall z, |z| = p(|x|))[(x,z) \in \overline{B}]\}$
$\Rightarrow A \in \forall co\mathcal{K}$

Theorem 8.

(1.) $\forall\Sigma_k^p = \Pi_{k+1}^p$, $\exists\Pi_k^p = \Sigma_{k+1}^p$ for $k \geq 0$

(2.) $\exists\Sigma_k^p = \Sigma_k^p$, $\forall\Pi_k^p = \Pi_k^p$ for $k \geq 1$

Proof: (1.)(Induction on k)

- Basis of induction $k = 0$. $\exists P = NP$, $\forall P = co NP$.
- Inductive step $k > 0$: We show $\Sigma_{k+1}^p = \exists\Pi_k^p$:

$\subseteq$ Let $A \in \Sigma_{k+1}^p = NP^{\Sigma_k^p}$, i.e., there ex. NPTM M accepting A in polynomial time p using oracle $B \in \Sigma_k^p$.

Define the set

$$A_M =_{def} \{ (x, a_1, \dots, a_r, b_1, \dots, b_s, z_1, \dots, z_s) \mid$$
M accepts x on computation path
$a_1, \dots, a_r$ if M, along the path,
asks exactly queries $z_1, \dots, z_s$
with (hypothetical) answers $b_1, \dots, b_s$
from the oracle $\}$

It holds that $A_M \in P$

We conclude:

$x \in A \Leftrightarrow$ M accepts x with oracle B

$\Leftrightarrow$ there ex. nondeterministic comp. path of M
$\vec{a} = (a_1, \dots, a_r)$, oracle queries $\vec{z} = (z_1, \dots, z_s)$,
answers $\vec{b} = (b_1, \dots, b_s)$ s.t.

(i) $(x, a_1, \dots, a_r, b_1, \dots, b_s, z_1, \dots, z_s) \in A_M$

(ii) $z_i \in B \Leftrightarrow b_i = 1$ for $i \in \{1, \dots, s\}$

$$\Leftrightarrow (\exists \vec{a})(\exists \vec{b})(\exists \vec{z}) \Big[(x, \vec{a}, \vec{b}, \vec{z}) \in A_M \wedge \bigwedge_{b_i=1} z_i \in B \wedge \bigwedge_{b_i=0} z_i \notin B \Big]$$

$$(*) \quad \Leftrightarrow (\exists \vec{a})(\exists \vec{b})(\exists \vec{z}) \Big[(x, \vec{a}, \vec{b}, \vec{z}) \in A_M \wedge (z_i)_{b_i=1} \in B_1 \wedge (z_i)_{b_i=0} \in \overline{B}_1 \Big]$$

We know that $B_1 \in \Sigma_k^p \overset{(IV)}{=} \exists \Pi_{k-1}^p$, $\overline{B}_1 \in \Pi_k^p$,
i.e., there ex. $C \in \Pi_{k-1}^p$, pol. q s.t. $u \in B_1 \Leftrightarrow (\exists v, |v| = q(|u|)) [(u, v) \in C]$

$$(*) \Leftrightarrow (\exists \vec{a})(\exists \vec{b})(\exists \vec{z})(\exists v) \Big[\underbrace{(x, \vec{a}, \vec{b}, \vec{z}) \in A_M}_{P \text{ predicate}} \wedge \underbrace{((z_i)_{b_i=1}, v) \in C}_{\Pi_{k-1}^p \text{ pred.}} \wedge \underbrace{((z_i)_{b_i=0}, v) \in \overline{B}_1}_{\Pi_k^p \text{ pred.}} \Big]$$

$$\Leftrightarrow (\exists w,\ |w| = t(|x|))\big[\ (x,w) \in D\big]$$

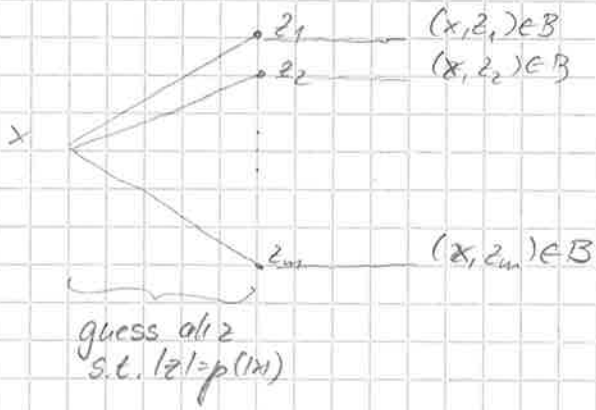
where D is defined to be

$$D =_{def} \Big\{ (x, \vec{a}, \vec{b}, \vec{z}, v) \;\Big|\; (x, \vec{a}, \vec{b}, \vec{z}) \in A_M \wedge$$
$$((z_i)_{b_i=1}, v) \in C \wedge$$
$$((z_i)_{b_i=0}, v) \in \bar{B} \Big\}$$

Clearly, $D \in \Pi_k^p$. Hence, $\Sigma_{k+1}^p \subseteq \exists \Pi_k^p$.

$\boxed{\supseteq}$ Let $A \in \exists \Pi_k^p$, i.e., there ex. $B \in \Pi_k^p$, pol. p s.t. $x \in A \Leftrightarrow (\exists z)\big[\ |z| = p(|x|) \wedge (x,z) \in B\big]$.

Define M to be the NPTM that accepts A using oracle B as follows, on input x:



For $\Pi_{k+1}^p = \forall \Sigma_k^p$ conclude:

$$A \in \Pi_{k+1}^p \Leftrightarrow \bar{A} \in \Sigma_{k+1}^p \Leftrightarrow \bar{A} \in \exists \Pi_k^p \Leftrightarrow A \in co\exists \Pi_k^p = \forall co\Pi_k^p = \forall \Sigma_k^p$$

(2.) Exercise. ∎

Notation: For polynomial p, predicate P denote

$$(\exists^p z)\big[P(x,z)\big] =_{def} (\exists z, |z| = p(|x|))\big[P(x,z)\big] = (\exists z)\big[|z| = p(|x|) \wedge P(x,z)\big]$$

$$(\forall^p z)\big[P(x,z)\big] =_{def} (\forall z, |z| = p(|x|))\big[P(x,z)\big] = (\forall z)\big[|z| = p(|x|) \rightarrow P(x,z)\big]$$

Corollary 9.

For $k \geq 1$, the following holds:

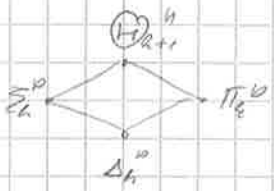
(1.) $\underbrace{\exists \forall \exists \forall \ldots}_{k} P = \Sigma_k^p$, $\underbrace{\forall \exists \forall \exists \ldots}_{k} P = \Pi_k^p$

(2.) $A \in \Sigma_k^p \Leftrightarrow$ there ex. $B \in P$, polynomial p s.t.
$x \in A \Leftrightarrow (\exists^p z_1)(\forall^p z_2)(\exists^p z_3) \ldots [(x, z_1, \ldots, z_k) \in B]$

(3.) $A \in \Pi_k^p \Leftrightarrow$ there ex. $B \in P$, polynomial p s.t.
$x \in A \Leftrightarrow (\forall^p z_1)(\exists^p z_2)(\forall^p z_3) \ldots [(x, z_1, \ldots, z_k) \in B]$

Proof: Clear ∎

Theorem 10.



(1.) $\Sigma_k^p = \Pi_k^p \Rightarrow \Sigma_k^p = PH$

(2.) $\Sigma_k^p = \Delta_k^p \Rightarrow \Sigma_k^p = PH$

(3.) $\Sigma_k^p = \Theta_{k+1}^p \Rightarrow \Sigma_k^p = PH$

(4.) $PH = PSPACE \rightarrow PH = \Sigma_k^p$ for some $k \geq 0$.

Proof:

(1.) Suppose $\Sigma_k^p = \Pi_k^p$. We show $\Sigma_{k+m}^p = \Sigma_k^p$ for all $m \geq 1$ by induction on m:

- $m = 1$: $\Sigma_{k+1}^p = \exists \Pi_k^p = \exists \Sigma_k^p = \Sigma_k^p$
- $m \geq 1$: $\Sigma_{k+m}^p = NP^{\Sigma_{k+m-1}^p} \overset{(IV)}{=} NP^{\Sigma_k^p} = \Sigma_{k+1}^p \overset{(IV)}{=} \Sigma_k^p$

(2.) $\Sigma_k^p = \Delta_k^p \subseteq \Pi_k^p \Rightarrow \Sigma_k^p = \Pi_k^p$

(3.) $\Sigma_k^p = \Theta_{k+1}^p \supseteq \Pi_k^p \Rightarrow \Sigma_k^p = \Pi_k^p$

(4.) Suppose $PH = PSPACE$. Choose set $A \leq_m^{\log}$-complete f. PSPACE. Then, $A \in PH$, i.e., there ex. $k \geq 0$ s.t. $A \in \Sigma_k^p$.
It follows $PSPACE \subseteq \mathcal{R}_m^{\log}(2A3) \subseteq \mathcal{R}_m^{\log}(\Sigma_k^p) = \Sigma_k^p$. ∎

4.4 Complete problems

We use $\overline{x_i}$ to denote a sequence of prop. variables.

Define

$$SAT_k =_{df} \{ H \mid H(\overline{x_1}, \ldots, \overline{x_k}) \text{ is a propositional formula such that } (\exists \overline{z_1})(\forall \overline{z_2})(\exists \overline{z_3}) \ldots (Q \overline{z_k})[H(\overline{z_1}, \ldots, \overline{z_k})] \text{ is true} \}$$

$$QBF =_{df} \bigcup_{k \geq 1} SAT_k$$

(quantified boolean formulas)

Theorem 11

(1.) SAT_k is $\leq_m^{\log}$-complete for Σ_k^P for $k \geq 1$.

(2.) $\overline{SAT_k}$ is $\leq_m^{\log}$-complete for Π_k^P for $k \geq 1$.

(3.) QBF is $\leq_m^{\log}$-complete for PSPACE.

Proof: (only (1.))

(1.) In the proofs of Thm. 2.13, 2.14 (NP-compl. of C-SAT, SAT), we constructed for $A \leq_m^{\log} SAT$ for $A \in NP$, formulas

$$H_n^A(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{p(n)})$$

for each n, p polynomial, such that

$$a_1 a_2 \ldots a_n \in A \iff H_n^A(a_1, \ldots, a_n, x_{n+1}, \ldots, x_{p(n)}) \in SAT$$

Let $B \in \Sigma_k^P$, k odd (w.l.o.g.), i.e., there ex. $C \in P$, polynomial q s.t.

$$z \in B \iff (\exists z_1)(\forall z_2) \ldots (\exists z_k)[|z_1| = \ldots = |z_k| = q(|z|) \wedge (z, z_1, \ldots, z_k) \in C]$$

$$\iff (\exists z_1)(\forall z_2) \ldots (\forall z_{k-1})[|z_1| = \ldots = |z_{k-1}| = q(|z|) \wedge (z, z_1, \ldots, z_{k-1}) \in A]$$

where $A =_{df} \{(z, z_1, \ldots, z_{k-1}) \mid (\exists z_k)[|z_k| = q(|z|) \wedge (z, z_1, \ldots, z_k) \in C]\}$

Then, $A \in NP$.

Let $r(n) = n + (k-1)q(n)$ and let H_n^A be constructed as above.

We conclude:

$$z \in B \iff (\exists z_1)(\forall z_2)\dots(\forall z_{k-1})$$
$$\left[H^A_{r(|z|)}(z, z_1, \dots, z_{k-1}, x_{r(|z|)+1}, \dots, x_{p(r(|z|))}) \in \right]$$
$$\iff H^A_{r(|z|)}(z, \overline{y}_1, \dots, \overline{y}_{k-1}, \overline{y}_k) \in SAT_k$$

where $\overline{y}_i$ is the variable for bits of z_i (ie $\{1,\dots,k-1\}$) and $\overline{y}_k = (x_{r(|z|)}, \dots, x_{p(r(|z|))})$