- In computability theory we can create a hierarchy of hard problems:
  Consider Halt-TM, then using oracles define $\text{Halt-TM}^{\text{Halt-TM}}$, & so on.
  What's the complexity analog?

The Polynomial Hierarchy

- The PH is a generalization of NP, coNP & lies well "below" PSpace.

- Consider the following optimization qn.:
  MinDNF $:= \{\phi \mid \phi$ is a DNF formula not equiv. to any smaller DNF$\}$.

- Alternatively, it is:
  $\{\phi \mid \forall \text{DNF } \psi, |\psi|<|\phi|, \exists s, \psi(s)\neq\phi(s)\}$.

- It seems to be beyond NP, coNP as it uses <u>two</u> different quantifiers.

- On the other hand, it does not seem as hard as QBF!

- This motivates a new class:

<u>Defn</u>: • A language $L \in \underline{\Pi_2^P}$ if $\exists$ poly-time TM M & a constant c s.t. $\forall x \in \{0,1\}^*$,

$$x \in L \text{ iff } \forall u \in \{0,1\}^{|x|^c}, \exists v \in \{0,1\}^{|x|^c}, M(x,u,v) = 1.$$

• A language $L \in \underline{\Sigma_2^P}$ if $\exists$ poly-time TM M & a constant c st. $\forall x \in \{0,1\}^*$, $x \in L$ iff $\exists u \in \{0,1\}^{|x|^c}, \forall v \in \{0,1\}^{|x|^c}, M(x,u,v) = \underline{1}$.

▷ Clearly, $\Sigma_2^P = \text{co-}\Pi_2^P$.

Proposition: (i) MinDNF $\in \Pi_2^P$.

(ii) NP $\cup$ coNP $\subseteq \Sigma_2^P \cap \Pi_2^P$.

(iii) $\Sigma_2^P \cup \Pi_2^P \subseteq$ Pspace.

- Why stop at two quantifiers!?

- We can define Σ_i & Π_i by alternating $\forall/\exists$ i times:

- $L \in \Sigma_i$ if $\exists$ poly-time TM M & a $c>0$ s.t. $\forall x$, $x \in L$ iff

$$\exists u_1 \, \forall u_2 \cdots\cdots Q_i u_i \quad M(x, u_1, \ldots, u_i) = 1.$$

strings in $\{0,1\}^{|x|^c}$

$Q_i :=$ $\exists$ resp. $\forall$ if i is odd resp. even.

- Π_i is defined in a similar way except that the quantifier-sequence begins with a '$\forall$'.
- Conventionally, $\Sigma_0 = \Pi_0 := P$.

Defn: • The *polynomial hierarchy* is:

$$\underline{PH} := \bigcup_{i \geq 0} \Sigma_i .$$

Proposition: (1) $\Sigma_1 = NP$, $\Pi_1 = coNP$.

(2) $\forall i \geq 0$, $\Sigma_i \subseteq \Sigma_{i+1}$, $\Pi_i \subseteq \Pi_{i+1}$.

(3) $\forall i \geq 0$, $\Pi_i = co\text{-}\Sigma_i$.

(4) $\forall i \geq 0$, $\Sigma_i \cup \Pi_i \subseteq \Sigma_{i+1} \cap \Pi_{i+1}$.

(5) $PH = \bigcup_{i \geq 0} \Pi_i$.

(6) $PH \subseteq Pspace$.

OPEN: We do not know whether it is indeed a hierarchy?

I.e. $\Sigma_0 \subsetneq \Sigma_1 \subsetneq \cdots$?

- We defined Σ_i & Π_i like NP, but with i <u>alternating</u> quantifiers on top of a poly-time TM.

▷ $PH = \bigcup_{i \geq 0} \Sigma_i = \bigcup_{i \geq 0} \Pi_i \subseteq$ Pspace.

constant many alternations

arbitrary many alternations

- <u>Defn:</u> If $\exists i$, $PH = \Sigma_i$ then we shall say that PH collapses to the i-th level.

<u>PH-conjecture</u>: PH does <u>not</u> collapse.

It is a generalization of "$P \neq NP$?".

- We now show several separations that follow from this conjecture.

<u>Theorem 1</u>: If for an $i \geq 1$, $\Sigma_i = \Pi_i$, then PH collapses to the i-th level.

Proof: • Say, $\Sigma_i = \Pi_i$. What is Σ_{i+1}?

• An $L \in \Sigma_{i+1}$ iff $\exists$ poly-time TM M & a $c>0$ s.t. $\forall x$,

$x \in L$ iff $\exists u_1 \forall u_2 \cdots Q_{i+1} u_{i+1}$

u's of length $|x|^c$ $\quad M(x, u_1, \ldots, u_{i+1}) = 1$.

• Define a related language $L' :=$

$\{(y,z) \mid \forall u_2 \exists u_3 \cdots Q_{i+1} u_{i+1}\ M(y,z,u_2,\ldots,u'_{i+1}) = 1\}$.

z & u's of length $|y|^c$

• Clearly, $L' \in \Pi_i = \Sigma_i$.

• Also, we see that: $x \in L$ iff $\exists u_1, (x,u_1) \in L'$.

• The above two observations together mean:

$$L \in \Sigma_i$$

$$\Rightarrow \Sigma_{i+1} \subseteq \Sigma_i \Rightarrow \Sigma_{i+1} = \Sigma_i$$

$$\Rightarrow \Sigma_{i+1} = \Sigma_i = \Pi_i = \Pi_{i+1}.$$

• By induction, $\forall j \geq i$, $\Sigma_j = \Sigma_i = \Pi_i = \Pi_j$

$\Rightarrow PH = \Sigma_i$. $\square$

Corollary: If for an $i \geq 0$, $\Sigma_i = \Sigma_{i+1}$ then PH collapses to the i-th level.

Proof: • Let $\Sigma_i = \Sigma_{i+1}$.

$\Rightarrow \Pi_i = \Pi_{i+1}$

• We know $\Pi_i \cup \Sigma_i \subseteq \Pi_{i+1} \cap \Sigma_{i+1}$.

$\Rightarrow \Sigma_{i+1} = \Pi_{i+1} = \Sigma_i = \Pi_i$.

• By Theorem 1 we get $PH = \Sigma_i$. $\square$

Corollary: $P = NP \Leftrightarrow PH = P$.

Complete problems in PH

- Suppose A is a PH-complete problem (under poly-time reductions).
- Then, $\exists i$, $A \in \Sigma_i$.

Implying $\Sigma_i = PH$!

▷ PH-conjecture $\Rightarrow$ PH $\subsetneq$ Pspace.

Proof: • Assuming the PH-conjecture, we deduce, as above, that there are no PH-complete problems.

• On the other hand, there is a Pspace-complete problem.

$\Rightarrow$ PH $\subsetneq$ Pspace. □

Σ_i-complete problems

Defn: For $i \geq 1$, define $\underline{\Sigma_i Sat}$:=
$\{ \phi(u_1, \ldots, u_i) \mid \phi(\bar{x})$ be a boolean CNF formula with a partition of $x_1, \ldots, x_n$ into $u_1, \ldots, u_i$ s.t. $\exists u_1 \forall u_2 \cdots Q_i u_i$, $\phi(u_1, \ldots, u_i) = 1 \}$.

not quite a QBF

Theorem: $\Sigma_i Sat$ is Σ_i-complete.

$\Sigma_1 Sat$ is Sat.

Proof:

• By defn, $\Sigma_i Sat \in \Sigma_i$.

- Any $L \in \Sigma_i$ has a corresponding poly-time TM M.
- The computation of M can be captured in a CNF formula ϕ.

  (by Cook-Levin reduction)
- This reduces the qn. $x \in L$ to the truth of the quantified formula $\exists u_1 \forall u_2 \cdots Q_i u_i \; \phi(x, u_1, \ldots, u_i)$.

$\Rightarrow$

Σ_iSat is Σ_i-hard as well. $\square$

<u>Defn:</u> For $i \geq 1$, define <u>Π_iSat</u> $:= \{\phi(u_1, \ldots, u_i) \mid$ ϕ is a boolean DNF formula with a partition of $x_1, \ldots, x_n$ into $u_1, \ldots, u_i$ s.t. $\forall u_1 \exists u_2 \cdots Q_i u_i \; \phi(u_1, \ldots, u_i) = 1\}$.

<u>Corollary:</u> Π_iSat is Π_i-complete.

PH via oracle machines

- Like NP represents computation on non-deterministic TMs.
  What does PH represent?

Defn: • For complexity classes C_1, C_2 we define the class $C_1^{C_2} := \bigcup_{L \in C_2} C_1^L$.

▷ $P^{NP} = P^{SAT}$.

▷ $NP^{NP} = NP^{SAT}$.

- We intend to show $NP^{NP} = \Sigma_2$!

Theorem: $\forall i \geq 2$, $\Sigma_i = NP^{\Sigma_{i-1} Sat}$.

Proof sketch:

• We exhibit the ideas by taking $i=2$.

• Let $L \in \Sigma_2$.

Then there is a poly-time TM M &

a constant $c>0$ s.t.

(1) - - - - $\forall x, \quad x \in L$ iff $\exists u_1 \forall u_2 \, M(x, u_1, u_2) = 1$.

in $\{0,1\}^{|x|^c}$

- The associated language $L' :=$
  $\{(y, z) \mid \forall u_2 \in \{0,1\}^{|y|^c}, M(y, z, u_2) = 1\}$
  is in Π_1.
- Thus, $\overline{L'}$ can be decided by an oracle to SAT.

$\Rightarrow \overline{L'} \in P^{SAT} \Rightarrow L' \in P^{SAT}$.

- We could rewrite eqn.(1) as:

$x \in L$ iff $\exists u_1, (x, u_1) \in L'$.

$\Rightarrow L \in NP^{SAT}$

$\Rightarrow \Sigma_2 \subseteq NP^{SAT}$.

- Let $L \in NP^{SAT}$. Say, L is decided by a poly-time NDTM N using SAT oracle.
- N makes <u>choices</u> in its execution path & <u>queries</u> the oracle on CNF formulas.

- Let us study an execution of N on x.
- Say, N makes the bit choices,

  $c_1, c_2, \ldots, c_m \in \{0,1\}$.

- Say, N queries SAT on the formulas, $\phi_{\bar{c},1}, \phi_{\bar{c},2}, \ldots, \phi_{\bar{c},k}$ & gets answers, $a_1, a_2, \ldots, a_k \in \{0,1\}$.

- Then, $x \in L$ iff $\exists c_1, \ldots, c_m, a_1, \ldots, a_k$, ($N$ accepts x on the path $\langle c_1, \ldots, c_m \rangle$ & $\langle a_1, \ldots, a_k \rangle$ are the correct answers).

iff

$$\exists \bar{c}, \bar{a}\ \overbrace{\exists u_1, \ldots, u_k}^{\text{for YES answers}}\ \forall \overbrace{v_1, \ldots, v_k}^{\text{for NO answers}} \text{ s.t.}$$

N accepts x on the path $\bar{c}$ & the answers $\langle a_1, \ldots, a_k \rangle$ AND

$\forall i \in [k], (a_i = 1 \Rightarrow \phi_{\bar{c},i}(u_i) = 1)$ AND

$\forall i \in [k], (a_i = 0 \Rightarrow \phi_{\bar{c},i}(v_i) = 0)$.

$\Rightarrow L \in \Sigma_2$. $\Rightarrow NP^{SAT} \subseteq \Sigma_2$.

$\Rightarrow \Sigma_2 = NP^{SAT} = NP^{NP}$. $\square$

- Exercise: Complete the pf. for $i > 2$.

- Thus, $\Sigma_2 = NP^{NP}$, $\Sigma_3 = NP^{NP^{NP}}$, ...

- Note: $P^P = P$ but NP^{NP} is conjectured to be harder than NP.

Between PH & Pspace: Counting

- Define #SAT: $\{\text{boolean formula } \phi\} \longrightarrow \mathbb{N}$
  $\phi \mapsto$ #sat. assgn. of ϕ.

- Is #SAT eff. computable?

Definition: FP $:= \{ f \mid f$ is a fn. $\{0,1\}^* \to \mathbb{N}$, computable by a poly-time TM $M_f \}$.

Open: #SAT $\notin$ FP?