$$INDSET = \{\langle G, k\rangle : \exists \text{IS } I \text{ of } G \text{ s.t. } |I| \geq k\}$$

$$EXACT\ INDSET = \{\langle G, k\rangle : \exists \text{IS } |I| = k \text{ of } G \text{ s.t. } \forall \text{ IS } I', |I'| \leq |I|\}$$

$$MIN{-}EQ{-}DNF = \{\langle \phi, k\rangle : \exists \text{DNF formula } |\psi| \leq k \text{ s.t. } \forall u : \phi(u) = \psi(u)\}$$

$$\overline{MIN - EQ - DNF} = \{\langle \phi, k\rangle : \forall \text{DNF formula } |\psi| \leq k, \exists u : \phi(u) \neq \psi(u)\}$$

Definition 1 (NP)

$L \in NP$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)} : M(x, u) = 1.$$

Definition 2 (Σ_2^p)

$L \in \Sigma_2^p$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)}\ \forall v \in \{0,1\}^{q(|x|)} : M(x, u, v) = 1.$$

Definition 3 (Σ_2^p)

$L \in \Sigma_2^p$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)}\ \forall v \in \{0,1\}^{q(|x|)} : M(x,u,v) = 1.$$

Examples:

$$EXACT\ INDSET = \{\langle G,k\rangle : \exists \text{IS } |I| = k \text{ of } G \text{ s.t. } \forall \text{ IS } I', |I'| \leq |I|\}$$

$$MIN{-}EQ{-}DNF = \{\langle \phi,k\rangle : \exists \text{DNF formula } |\psi| \leq k \text{ s.t. } \forall u : \phi(u) = \psi(u)\}$$

Definition 4 (Π_2^p)

$L \in \Pi_2^p$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \forall u \in \{0,1\}^{q(|x|)}\ \exists v \in \{0,1\}^{q(|x|)} : M(x,u,v) = 1.$$

Examples:

$$\overline{MIN - EQ - DNF} = \{\langle \phi,k\rangle : \forall \text{DNF formula } |\psi| \leq k, \exists u : \phi(u) \neq \psi(u)\}$$

Definition 5 (Σ_2^p)

$L \in \Sigma_2^p$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)}\ \forall v \in \{0,1\}^{q(|x|)} : M(x,u,v) = 1.$$

- $NP \subseteq \Sigma_2^p$ (use verifier $M(x,u,v)$ for $L \in NP$, just ignore input v)
- $coNP \subseteq \Sigma_2^p$ (use verifier $M(x,u,v)$ for $L \in coNP$, just ignore input u)
- Similarly $NP \subseteq \Pi_2^p$, $coNP \subseteq \Pi_2^p$
- $NP = \Sigma_1^p$, $coNP = \Pi_1^p$.

Definition 6 (Σ_i^p)

For $i \geq 1$, $L \in \Sigma_i^p$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow$$
$$\exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \ldots Q_i u_i \in \{0,1\}^{q(|x|)} : M(x, u_1, \ldots, u_i) = 1$$

where $Q_i = \exists$ or $\forall$ if $i =$odd or even respectively.

Definition 7 (Polynomial hierarchy)

The polynomial hierarchy is the set $PH = \bigcup_i \Sigma_i^p$.

Definition 8 (Π_i^p)

For $i \geq 1$, $L \in \Pi_i^p$ if there exists a polynomial-time TM M and polynomial q such that $\forall x \in \{0,1\}^*$,

$$x \in L \Leftrightarrow$$

$$\forall u_1 \in \{0,1\}^{q(|x|)} \exists u_2 \in \{0,1\}^{q(|x|)} \ldots Q_i u_i \in \{0,1\}^{q(|x|)} : M(x, u_1, \ldots, u_i) = 1$$

where $Q_i = \forall$ or $\exists$ if i =odd or even respectively.

Equivalently, $\Pi_i^p = \{L : \overline{L} \in \Sigma_i^p\}$.

Definition 9 (Polynomial hierarchy)

The polynomial hierarchy is the set $PH = \bigcup_i \Sigma_i^p$.

We can extend definitions to have $\Sigma_0^p = P = coP = \Pi_0^p$ (no quantifiers)

Lemma 10

$PH = \bigcup_i \Pi_i^p$

Proof: $\Sigma_i^p \subseteq \Pi_{i+1}^p \subseteq \Sigma_{i+2}^p$

Theorem 11

If $P = NP$, then the hierarchy collapses to P (i.e., $PH = P$).

Proof: Induction on i to prove $\Sigma_i^p, \Pi_i^p \subseteq P$:

1. $i = 0 : \Sigma_0^p = \Pi_0^p = P$
2. $i = k - 1 : \Sigma_{k-1}^p, \Pi_{k-1}^p \subseteq P$
3. $i = k$: Let $L \in \Sigma_k^p$. Then

$$x \in L \Leftrightarrow \exists u_1 \forall u_2 \ldots Q_k u_k : M(x, u_1, \ldots, u_k) = 1 \qquad (1)$$

Define L' s.t.

$$\langle x, u_1 \rangle \in L' \Leftrightarrow \forall u_2 \ldots Q_k u_k : M(x, u_1, u_2, \ldots, u_k) = 1$$

$\Rightarrow L' \in \Pi_{k-1}^p \overset{(2)}{\subseteq} P \Rightarrow$ poly-time TM M' decides L'
$\Rightarrow$ (1) implies $x \in L \Leftrightarrow \exists u_1 : M'(x, u_1) = 1$
$\Rightarrow L \in NP = P$ □

Theorem 12

For every $i \geq 0$, if $\Sigma_i^p = \Pi_i^p$ then the hierarchy collapses to ith level (i.e., $PH = \Sigma_i^p$).

Proof: Same as proof of Theorem 11

Definition 13 (Σ_i^p-hardness)

L is Σ_i^p-hard if $L' \leq_P L$ for every $L' \in \Sigma_i^p$.

Definition 14 (Σ_i^p-completeness)

L is Σ_i^p-complete if

1. L is Σ_i^p-hard, and
2. $L \in \Sigma_i^p$.

$$\Sigma_i^p - SAT = \{\langle \exists u_1 \forall u_2 \ldots Q_i u_i \ \phi(u_1, u_2, \ldots, u_i) = 1 \rangle \text{ is TRUE}\}$$

Theorem 15

$\Sigma_i^p - SAT$ is Σ_i^p-complete.

Note: $\Sigma_i^p - SAT$ is special case of $TQBF$ (or $QSAT$ if ϕ is CNF)

Theorem 16

If some $L \in \Sigma_i^p$ is PH-complete, then $PH = \Sigma_i^p$.

Proof:

L is PH-complete
$\Rightarrow \forall L' \in PH : L' \leq_P L$
$\Rightarrow L' \in \Sigma_i^p$
$\Rightarrow PH \subseteq \Sigma_i^p$ $\square$

Does PH have complete problems?

Corollary 1

If $PH = PSPACE$, then the hierarchy collapses.

Proof: $TQBF$ is PH-complete and belongs to Σ_i^p for some i. $\square$

Alternating TMs

- ATMs similar to NDTMs. Certificate tape contains $u_1, u_2, \ldots, u_i$.
- Each state (other than q_{start}, q_{accept}) has label $\exists$ or $\forall$.
- ATM M runs in time $T(|x|)$ if $M(x)$ halts after $T(|x|)$ steps for every possible certificate strings. $\Rightarrow$ Configuration graph is a DAG
- ATM acceptance: $G_{M,x}$ is a DAG
  $\Rightarrow$ Topological order $(C_0 =) C_{start}, C_1, C_2, \ldots, C_m, \ldots, C_{accept}$
  Let $q_{start}, q_1, q_2, \ldots, q_m, \ldots, q_{accept}$ be the ATM states

  1. $C_{accept} := ACCEPT$
  2. If $label(q_m) = \exists$ then
     $$C_m := ACCEPT \Leftrightarrow \exists (C_m, C_k) \in E_{G_{M,x}} : C_k = ACCEPT$$
  3. If $label(q_m) = \forall$ then
     $$C_m := ACCEPT \Leftrightarrow \forall (C_m, C_k) \in E_{G_{M,x}} : C_k = ACCEPT$$
  4. ATM M accepts iff $C_{start} = ACCEPT$

Definition 17

For every $i \geq 0$, $L \in \Sigma_i TIME(T(n))$ (resp. $L \in \Pi_i TIME(T(n))$) iff accepted by $T(n)$-time ATM with

- $label(q_{start}) = \exists$ (resp. $label(q_{start}) = \forall$)
- For all x, every path in $G_{M,x}$ has at most $i - 1$ state label alterations

Claim 1

For every $i \geq 0$, $\Sigma_i^p = \bigcup_{c \geq 0} \Sigma_i TIME(n^c)$ *and* $\Pi_i^p = \bigcup_{c \geq 0} \Pi_i TIME(n^c)$.

Proof hints:

- Copy certificate tape contents $u_1, u_2, \ldots, u_i$ using $\exists, \forall, \ldots, Q_i$ states ($i - 1$ alterations)
- Then running of $M(x, u_1, u_2, \ldots, u_i)$ is deterministic, i.e., single path in $G_{M,x}$, with all states labeled Q_i (doesn't matter what Q_i is)

□

Theorem 18

$\Sigma_2^p = NP^{SAT}$

Proof: $\Sigma_2^p \subseteq NP^{SAT}$

- Oracle for SAT is same as oracle for $\overline{SAT}$!
- Let $L \in \Sigma_2^p$. Then
  $$x \in L \Leftrightarrow \exists u_1 \in \{0,1\}^{q(|x|)} \; \forall u_2 \in \{0,1\}^{q(|x|)} : M(x, u_1, u_2) = 1$$
- $L' = \{\langle x, u_1 \rangle : \forall u_2 \in \{0,1\}^{q(|x|)} : M(x, u_1, u_2) = 1\} \Rightarrow L' \in coNP$
  $\Rightarrow \langle x, u_1 \rangle \overset{?}{\in} L'$ becomes a $\overline{SAT}$ (or SAT) question ($coNP$-complete)
- $x \in L \Leftrightarrow \exists u_1 \in \{0,1\}^{q(|x|)} : M^{SAT}(x, u_1) = 1 \Rightarrow L \in NP^{SAT}$

□

Theorem 19

$\Sigma_2^p = NP^{SAT}$

Proof: $NP^{SAT} \subseteq \Sigma_2^p$

- Let $L \in NP^{SAT}$. Then
$$x \in L \Leftrightarrow \exists c \in \{0,1\}^{q(|x|)} : N^{SAT}(x,c) = 1$$
- N^{SAT} asks k SAT-questions $\phi_i(q_i)$, and gets answers $a_i = 0$ or 1
- $N(x,c)$ can run without oracle if it already knows all oracle answers $a_1, a_2, \ldots, a_k \Rightarrow$ Guess them!
- $x \in L \Leftrightarrow \exists c, a_1, \ldots, a_k : N(x,c,a) = 1$ **...but** what if $a_1, \ldots, a_k$ are not SAT-oracle answers to questions $\phi_1(q_1), \ldots, \phi_k(q_k)$???
- Need to make sure:
  1. If $a_i = 0$ (i.e., $\phi_i(v_i)$ unsatisfiable) then $\forall v_i \; \phi_i(v_i) = 0$ holds
  2. If $a_i = 1$ (i.e., $\phi_i(u_i)$ satisfiable) then $\exists u_i \; \phi_i(u_i) = 1$ holds

Proof: $NP^{SAT} \subseteq \Sigma_2^p$ (cont'd)

- Include these checks in formula for L:

$$
\begin{aligned}
x \in L \Leftrightarrow \exists c, a_1, \ldots, a_k, u_1, \ldots, u_k \forall v_1, \ldots, v_k :& \\
& N(x, c, a) = 1 \text{ AND} \\
& \forall i : (a_i = 0 \Rightarrow \phi_i(u_i) = 1) \wedge (a_i = 1 \Rightarrow \phi_i(v_i) = 0)
\end{aligned}
$$

- A poly-time TM $M(x, c, a, u, v)$ can decide the last two lines
- $x \in L \Leftrightarrow \exists c, a_1, \ldots, a_k, u_1, \ldots, u_k \forall v_1, \ldots, v_k : M(x, c, a, u, v) = 1$
  $\Rightarrow L \in \Sigma_2^p$ □

An unconditional result (finally...)

Definition 20

$TISP(T(n), S(n))$ is the set of languages decided by a TM $M(x)$ which uses time $O(T(|x|))$ and space $O(S(|x|))$.

Theorem 21

$SAT \notin TISP(n^{1.1}, n^{0.1})$.

Proof: Omitted (read 5.4)