

Chapter 5: Polynomial hierarchy and alternations

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

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

$MIN-EQ-DNF = \{\langle \phi, 1^k \rangle : \exists \text{DNF formula } |\psi| \leq k \text{ s.t. } \forall u : \phi(u) = \psi(u)\}$

$\overline{MIN-EQ-DNF} = \{\langle \phi, 1^k \rangle : \forall \text{DNF formula } |\psi| \leq k, \exists u : \phi(u) \neq \psi(u)\}$

Chapter 5: Polynomial hierarchy and alternations

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 $\forall x \in \{0, 1\}^*$,

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

Examples:

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

$$MIN-EQ-DNF = \{\langle \phi, 1^k \rangle : \exists \text{DNF formula } |\psi| \leq k \text{ s.t. } \forall u : \phi(u) = \psi(u)\}$$

Chapter 5: Polynomial hierarchy and alternations

Definition 3 ($coNP$)

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

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

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:

$$MIN-EQ-DNF = \{\langle \phi, 1^k \rangle : \forall \text{DNF formula } |\psi| \leq k, \exists u : \phi(u) \neq \psi(u)\}$$

Chapter 5: Polynomial hierarchy and alternations

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 $\bar{M}(x, u, v)$ for $L \in coNP$, just ignore input u)
- Similarly $NP \subseteq \Pi_2^P$, $coNP \subseteq \Pi_2^P$
- $NP = \Sigma_1^P$, $coNP = \Pi_1^P$.
- $\Sigma_0^P = P = coP = \Pi_0^P$ (no quantifiers)

Chapter 5: Polynomial hierarchy and alternations

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 $\forall x \in \{0, 1\}^*$,

$$x \in L \Leftrightarrow$$

$$\exists u_1 \in \{0, 1\}^{q(|x|)} \forall u_2 \in \{0, 1\}^{q(|x|)} \dots \mathbf{Q}_i u_i \in \{0, 1\}^{q(|x|)} : M(x, u_1, \dots, u_i) = 1$$

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

Definition 7 (Polynomial hierarchy)

The **polynomial hierarchy** is the set $PH = \bigcup_{i \geq 0} \Sigma_i^p$.

Chapter 5: Polynomial hierarchy and alternations

Definition 8 (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 $\forall x \in \{0, 1\}^*$,

$$x \in L \Leftrightarrow$$

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

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

Definition 9 (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 $\forall x \in \{0, 1\}^*$,

$$x \in L \Leftrightarrow$$

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

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

Equivalently, $\Pi_i^P = \{L : \bar{L} \in \Sigma_i^P\}$.

Lemma 10

$$PH = \bigcup_{i \geq 0} \Pi_i^P$$

Proof:

$\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+2}^P$, just like $NP = \Sigma_1^P \subseteq \Pi_2^P$ and $coNP = \Pi_1^P \subseteq \Sigma_2^P$.

Then

- $PH = \bigcup_{i \geq 0} \Sigma_i^P \subseteq \bigcup_{i \geq 1} \Pi_i^P = \bigcup_{i \geq 0} \Pi_i^P$
- $\bigcup_{i \geq 0} \Pi_i^P = \bigcup_{i \geq 1} \Pi_i^P \subseteq \bigcup_{i \geq 2} \Sigma_i^P = \bigcup_{i \geq 0} \Sigma_i^P = PH$

□

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 $i = k : \text{Let } L \in \Sigma_k^P. \text{ Then}$

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

Define L' s.t.

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

$$\begin{aligned} \Rightarrow L' &\in \Pi_{k-1}^P \stackrel{IH}{\subseteq} P \Rightarrow \text{poly-time TM } M' \text{ decides } L' \\ \Rightarrow (1) \text{ implies } x &\in L \Leftrightarrow \exists u_1 : M'(x, u_1) = 1 \\ \Rightarrow L &\in NP = P \end{aligned}$$

□

Theorem 12

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

Proof: Same as proof of Theorem 11

Chapter 5: Polynomial hierarchy and alternations

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 $L \in \Sigma_i^P$.

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

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)

Chapter 5: Polynomial hierarchy and alternations

Theorem 16

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

Proof:

L is **PH-complete**

$\Rightarrow \forall L' \in PH : L' \leq_P L$

$\Rightarrow L' \in \Sigma_i^P$

$\Rightarrow PH \subseteq \Sigma_i^P$

□

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 .

□

Alternating TMs

- ATMs similar to NDTMs.
- 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 $(C_0 =) C_{start}, C_1, C_2, \dots, C_m, \dots, C_{accept}$
Let $q_{start}, q_1, q_2, \dots, q_m, \dots, q_{accept}$ be the ATM states
 - 1 $C_{accept} := \text{ACCEPT}$
 - 2 If $\text{label}(q_m) = \exists$ then
$$C_m := \text{ACCEPT} \Leftrightarrow \exists (C_m, C_k) \in E_{G_{M,x}} : C_k = \text{ACCEPT}$$
 - 3 If $\text{label}(q_m) = \forall$ then
$$C_m := \text{ACCEPT} \Leftrightarrow \forall (C_m, C_k) \in E_{G_{M,x}} : C_k = \text{ACCEPT}$$
 - 4 ATM M accepts iff $C_{start} = \text{ACCEPT}$

Chapter 5: Polynomial hierarchy and alternations

Definition 17

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

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

Claim 1

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

Proof hints (for $\Sigma_i^P \subseteq \bigcup_{c \geq 0} \Sigma_i \text{TIME}(n^c)$):

- Copy branching decisions u_1, u_2, \dots, u_i using two \exists, \forall states alternatively ($i - 1$ alterations)
- Then running of $M(x, u_1, u_2, \dots, u_i)$ 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} !
- $L \in NP^{SAT}$: There is poly-time TM M^{SAT} and polynomial q s.t.
$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)} : M^{SAT}(x, u) = 1$$
- Let $L \in \Sigma_2^P$. Then
$$x \in L \Leftrightarrow \exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} : M(x, u_1, u_2) = 1$$
- $L' = \{\langle x, u_1 \rangle : \forall u_2 \in \{0,1\}^{q(|x|)} : M(x, u_1, u_2) = 1\} \Rightarrow L' \in coNP$
 $\Rightarrow \langle x, u_1 \rangle \stackrel{?}{\in} L'$ 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 $a_1, a_2, \dots, a_k \Rightarrow$ Guess them!
- $x \in L \Leftrightarrow \exists c, a_1, \dots, a_k : N(x, c, a) = 1 \dots$ but what if a_1, \dots, a_k are not SAT-oracle answers to questions $\phi_1(q_1), \dots, \phi_k(q_k)???$
- Need to make sure:
 - If $a_i = 0$ (i.e., $\phi_i(v_i)$ unsatisfiable) then $\forall v_i \phi_i(v_i) = 0$ holds
 - If $a_i = 1$ (i.e., $\phi_i(u_i)$ satisfiable) then $\exists u_i \phi_i(u_i) = 1$ holds

Chapter 5: Polynomial hierarchy and alternations

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

- Include these checks in formula for L :

$$x \in L \Leftrightarrow \exists c, a_1, \dots, a_k, u_1, \dots, u_k \forall v_1, \dots, v_k :$$

$$N(x, c, a) = 1 \text{ AND}$$

$$\forall i : (a_i = 1 \Rightarrow \phi_i(u_i) = 1) \wedge (a_i = 0 \Rightarrow \phi_i(v_i) = 0)$$

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

Theorem 20

$$\Sigma_i^P = NP^{\Sigma_{i-1} SAT}$$

Proof:

Exactly as before. □

Chapter 5: Polynomial hierarchy and alternations

An unconditional result (finally...)

Definition 21

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

Theorem 22

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

Proof: Omitted (read 5.4)