

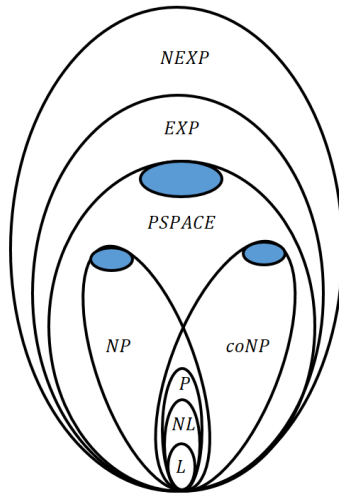
CSL853: Complexity Theory

Ragesh Jaiswal, CSE, IIT Delhi

Complexity Diagram

Complexity Diagram

Our current view of complexity classes



The Polynomial Hierarchy

The Polynomial Hierarchy

The complexity class Σ_2^P

- Consider the following problems:
 - $\text{INDSET} = \{\langle G, k \rangle : \text{graph } G \text{ has an independent set of size } \geq k\}$.
 - $\text{EXACT-INDSET} = \{\langle G, k \rangle : \text{the largest independent set in } G \text{ has size exactly } k\}$.
 - $\text{MIN-EQ-DNF} = \{\langle \psi, k \rangle : \exists \text{ DNF formula } \psi' \text{ of size } \leq k \text{ that is equivalent to the DNF formula } \psi\}$.
- In which complexity classes do these languages belong?
 - $\text{INDSET} \in \text{NP}$: Since there is a short certificate.
 - $\text{EXACT-INDSET} \stackrel{?}{\in} \text{NP}$?
 - $\text{MIN-EQ-DNF} \stackrel{?}{\in} \text{NP}$?

The Polynomial Hierarchy

The complexity class Σ_2^P

- Consider the following problems:
 - $\text{INDSET} = \{\langle G, k \rangle : \text{graph } G \text{ has an independent set of size } \geq k\}$.
 - $\text{EXACT-INDSET} = \{\langle G, k \rangle : \text{the largest independent set in } G \text{ has size exactly } k\}$.
 - $\text{MIN-EQ-DNF} = \{\langle \psi, k \rangle : \exists \text{ DNF formula } \psi' \text{ of size } \leq k \text{ that is equivalent to the DNF formula } \psi\}$.
- In which complexity classes do these languages belong?
 - $\text{INDSET} \in \text{NP}$: Since there is a short certificate.
 - $\text{EXACT-INDSET} \stackrel{?}{\in} \text{NP}$? **Not known**
 - $\text{MIN-EQ-DNF} \stackrel{?}{\in} \text{NP}$? **Not known**

The Polynomial Hierarchy

The complexity class Σ_2^P

- Consider the following problems:
 - $\text{INDSET} = \{\langle G, k \rangle : \text{graph } G \text{ has an independent set of size } \geq k\}$.
 - $\text{EXACT-INDSET} = \{\langle G, k \rangle : \text{the largest independent set in } G \text{ has size exactly } k\}$.
 - $\text{MIN-EQ-DNF} = \{\langle \psi, k \rangle : \exists \text{DNF formula } \psi' \text{ of size } \leq k \text{ that is equivalent to the DNF formula } \psi\}$.
- In which complexity classes do these languages belong?
 - $\text{INDSET} \in \text{NP}$: Since there is a short certificate.
 - $\text{EXACT-INDSET} \stackrel{?}{\in} \text{NP}$.
 - $\text{MIN-EQ-DNF} \stackrel{?}{\in} \text{NP}$.

Definition (Σ_2^P)

The class Σ_2^P is the set of all languages L for which there exists a polynomial-time TM M and a polynomial q such that

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

for every $x \in \{0, 1\}^*$.

The Polynomial Hierarchy

The complexity class Σ_2^P

- Consider the following problems:
 - INDSET = $\{\langle G, k \rangle : \text{graph } G \text{ has an independent set of size } \geq k\}$.
 - EXACT-INDSET = $\{\langle G, k \rangle : \text{the largest independent set in } G \text{ has size exactly } k\}$.
 - MIN-EQ-DNF = $\{\langle \psi, k \rangle : \exists \text{ DNF formula } \psi' \text{ of size } \leq k \text{ that is equivalent to the DNF formula } \psi\}$.

Definition (Σ_2^P)

The class Σ_2^P is the set of all languages L for which there exists a polynomial-time TM M and a polynomial q such that

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

for every $x \in \{0, 1\}^*$.

- Claim 1: EXACT-INDSET $\in \Sigma_2^P$.
- Claim 2: MIN-EQ-DNF $\in \Sigma_2^P$.

The Polynomial Hierarchy

The complexity class Σ_2^P

Definition (Σ_2^P)

The class Σ_2^P is the set of all languages L for which there exists a polynomial-time TM M and a polynomial q such that

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

for every $x \in \{0, 1\}^*$.

- Claim 1: EXACT-INDSET $\in \Sigma_2^P$.
- Claim 2: MIN-EQ-DNF $\in \Sigma_2^P$.
- Claim 3: NP $\in \Sigma_2^P$ and coNP $\in \Sigma_2^P$.

The Polynomial Hierarchy

The complexity class Σ_i^P

Definition (Σ_i^P)

For $i \geq 1$, a language L is in Σ_i^P if there exists a polynomial-time TM M and a polynomial q such that

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

where Q_i denotes $\forall$ or $\exists$ depending on whether i is even or odd, respectively.

Definition (Π_i^P)

$$\forall i \geq 1, \Pi_i^P = \text{co}\Sigma_i^P = \{\bar{L} : L \in \Sigma_i^P\}.$$

Definition (PH)

The *polynomial hierarchy* is the set $\text{PH} = \cup_i \Sigma_i^P$.

The Polynomial Hierarchy

The complexity class Σ_i^P

Definition (Σ_i^P)

For $i \geq 1$, a language L is in Σ_i^P if there exists a polynomial-time TM M and a polynomial q such that

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

where Q_i denotes $\forall$ or $\exists$ depending on whether i is even or odd, respectively.

Definition (Π_i^P)

$$\forall i \geq 1, \Pi_i^P = \text{co}\Sigma_i^P = \{\bar{L} : L \in \Sigma_i^P\}.$$

Definition (PH)

The *polynomial hierarchy* is the set $\text{PH} = \cup_i \Sigma_i^P$.

- Claim 1: $\text{PH} = \cup_{i \geq 0} \Pi_i^P$.

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Proof.

- We will show by induction that $\forall j > i, \Sigma_j^P = \Sigma_i^P$ and $\Pi_j^P = \Pi_i^P$.
- Base case ($j = i + 1$):
 - Consider $L \in \Sigma_{i+1}^P$. From the definition, there is a polynomial-time TM M such that

$$x \in L \Leftrightarrow \exists u_1 \forall u_2 \dots Q_{i+1} u_{i+1} \ M(x, u_1, \dots, u_{i+1}) = 1.$$

- Define L' :

$$\langle x, u_1 \rangle \in L' \Leftrightarrow \forall u_2 \dots Q_{i+1} u_{i+1} \ M(x, u_1, \dots, u_{i+1}) = 1.$$

- Claim: $L' \in \Pi_i^P = \Sigma_i^P$.

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Proof.

- We will show by induction that $\forall j > i, \Sigma_j^P = \Sigma_i^P$ and $\Pi_j^P = \Pi_i^P$.
- Base case ($j = i + 1$):
 - Consider $L \in \Sigma_{i+1}^P$. From the definition, there is a polynomial-time TM M such that $x \in L \Leftrightarrow \exists u_1 \forall u_2 \dots Q_{i+1} u_{i+1} M(x, u_1, \dots, u_{i+1}) = 1$.
 - Define L' such that $\langle x, u_1 \rangle \in L' \Leftrightarrow \forall u_2 \dots Q_{i+1} u_{i+1} M(x, u_1, \dots, u_{i+1}) = 1$.
 - Claim 1: $L' \in \Pi_i^P = \Sigma_i^P$.
 - So, there is a polynomial-time TM M' such that

$$\langle x, u \rangle \in L' \Leftrightarrow \exists u'_1 \forall u'_2 \dots Q_{i+1} u'_i M'(x, u_1, \dots, u_i) = 1.$$

- Claim 2: $L \in \Sigma_i^P$.

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Proof.

- We will show by induction that $\forall j > i, \Sigma_j^P = \Sigma_i^P$ and $\Pi_j^P = \Pi_i^P$.
- Base case ($j = i + 1$):
- Inductive case: Let $j > i$. If $\Sigma_j^P = \Sigma_i^P$ and $\Pi_j^P = \Pi_i^P$, then $\Sigma_{j+1}^P = \Sigma_i^P$ and $\Pi_{j+1}^P = \Pi_i^P$
 - Arguments are similar to the base case.



The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

- Does there exist a PH-complete language?

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

- Does there exist a PH-complete language?

Theorem

If there exists a language L that is PH-complete, then there exists an i such that $\text{PH} = \Sigma_i^P$.

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Theorem

If there exists a language L that is PH-complete, then there exists an i such that $\text{PH} = \Sigma_i^P$.

- Does there exist a PH-complete language? **This is unlikely.**
- What is the relationship between PH and PSPACE?

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Theorem

If there exists a language L that is PH-complete, then there exists an i such that $\text{PH} = \Sigma_i^P$.

- Does there exist a PH-complete language? **This is unlikely.**
- What is the relationship between PH and PSPACE? **$\text{PH} \subseteq \text{PSPACE}$.**

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Theorem

If there exists a language L that is PH-complete, then there exists an i such that $\text{PH} = \Sigma_i^P$.

- Does there exist a PH-complete language? **This is unlikely.**
- What is the relationship between PH and PSPACE? **$\text{PH} \subseteq \text{PSPACE}$.**
- Is PH equal to PSPACE?

The Polynomial Hierarchy

Collapse of polynomial hierarchy

Theorem

For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\text{PH} = \Sigma_i^P$; that is, the hierarchy collapses to the i^{th} level.

Theorem

If there exists a language L that is PH-complete, then there exists an i such that $\text{PH} = \Sigma_i^P$.

- Does there exist a PH-complete language? **This is unlikely.**
- What is the relationship between PH and PSPACE? **$\text{PH} \subseteq \text{PSPACE}$.**
- Is PH equal to PSPACE? **This is unlikely.**

The Polynomial Hierarchy

Complete problem for Σ_i^P

Theorem (Complete problem for Σ_i^P)

For every $i \geq 1$, the class Σ_i^P has the following complete problem involving quantified boolean expression of the following type with a limited number of alternations:

$$\Sigma_i\text{SAT} = \exists u_1 \forall u_2 \exists \dots Q_i u_i \ \psi(u_1, \dots u_i) = 1$$

where ψ is a boolean formula not necessarily in the CNF form, each u_i is a vector of boolean variables, and Q_i is $\forall$ or $\exists$ depending on whether i is even or odd respectively.

The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem (Alternate definition of Σ_i^P)

For every $i \geq 2$, $\Sigma_i^P = \text{NP}^{\Sigma_{i-1}\text{SAT}}$, where the latter denotes the set of languages decided by polynomial-time NDTM's with access to the oracle $\Sigma_{i-1}\text{SAT}$.

- We will show the following easier theorem that can be generalised easily to obtain the above theorem.

Theorem

$$\Sigma_2^P = \text{NP}^{\text{SAT}}.$$

The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem

$$\Sigma_2^P = \text{NP}^{\text{SAT}}.$$

Proof.

- Claim 1: $\Sigma_2^P \subseteq \text{NP}^{\text{SAT}}$.
 - For any $L \in \Sigma_2^P$, there is a TM M and a polynomial q such that
$$x \in L \Leftrightarrow \exists u_1 \in \{0, 1\}^{q(|x|)} \forall u_2 \in \{0, 1\}^{q(|x|)} M(x, u_1, u_2) = 1$$
 - Claim 1.1 There is an oracle NDTM M' with SAT oracle that makes only once call to the oracle and decides L .

The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem

$$\Sigma_2^P = \text{NP}^{\text{SAT}}.$$

Proof.

- Claim 1: $\Sigma_2^P \subseteq \text{NP}^{\text{SAT}}$.
- Claim 2: $\text{NP}^{\text{SAT}} \subseteq \Sigma_2^P$.
 - Consider any $L \in \text{NP}^{\text{SAT}}$. This means that there is a NDTM M that is allowed to make SAT oracle queries to decide L . Let the oracle queries of the machine be denoted by $\psi_1, \dots, \psi_k$.

The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem

$$\Sigma_2^P = \text{NP}^{\text{SAT}}.$$

Proof.

- Claim 1: $\Sigma_2^P \subseteq \text{NP}^{\text{SAT}}$.
- Claim 2: $\text{NP}^{\text{SAT}} \subseteq \Sigma_2^P$.
 - Consider any $L \in \text{NP}^{\text{SAT}}$. This means that there is a NDTM M that is allowed to make SAT oracle queries to decide L . Let the oracle queries of the machine be denoted by $\psi_1, \dots, \psi_k$.
 - Claim 2.1: For a suitable choice of c_i 's, a_i 's, u_i 's, and v_i 's, we may write

$$x \in L \iff \exists c_1, \dots, c_m, a_1, \dots, a_k, u_1, \dots, u_k \quad \forall v_1, \dots, v_k s.t.$$

M accepts x using choices $c_1, \dots, c_m$ and answers $a_1, \dots, a_k$

AND

$$\forall i \in [k] \text{ if } a_i = 1 \text{ then } \psi_i(u_i) = 1$$

AND

$$\forall i \in [k] \text{ if } a_i = 0 \text{ then } \psi_i(v_i) = 0$$

and hence $L \in \Sigma_2^P$.



The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem (Alternate definition of Σ_i^P)

For every $i \geq 2$, $\Sigma_i^P = \text{NP}^{\Sigma_{i-1}\text{SAT}}$, where the latter denotes the set of languages decided by polynomial-time NDTM's with access to the oracle $\Sigma_{i-1}\text{SAT}$.

- Note that by the above definition, $\Sigma_2^P = \text{NP}^{\text{SAT}}$.
- Since SAT is complete for NP, we may abuse notation and use $\Sigma_2^P = \text{NP}^{\text{NP}}$.
- Similarly, $\Sigma_3^P = \text{NP}^{\text{NP}^{\text{NP}}}$ and so on.
- Note that we may also write, $\Sigma_3^P = \text{NP}^{\Sigma_2^P} = \text{NP}^{\Pi_2^P}$ and so on.
- Claim: Let $A = \text{P}^{\text{NP}} (= \text{P}^{\text{coNP}})$. Then
 - ① $\Sigma_1^P = \text{NP} \subseteq A$.
 - ② $\Pi_1^P = \text{coNP} \subseteq A$.
 - ③ $A \subseteq \Sigma_2^P$.
 - ④ $A \subseteq \Pi_2^P$.

The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem (Alternate definition of Σ_i^P)

For every $i \geq 2$, $\Sigma_i^P = \text{NP}^{\Sigma_{i-1}\text{SAT}}$, where the latter denotes the set of languages decided by polynomial-time NDTM's with access to the oracle $\Sigma_{i-1}\text{SAT}$.

- Note that by the above definition, $\Sigma_2^P = \text{NP}^{\text{SAT}}$.
- Since SAT is complete for NP, we may abuse notation and use $\Sigma_2^P = \text{NP}^{\text{NP}}$.
- Similarly, $\Sigma_3^P = \text{NP}^{\text{NP}^{\text{NP}}}$ and so on.
- Note that we may also write, $\Sigma_3^P = \text{NP}^{\Sigma_2^P} = \text{NP}^{\Pi_2^P}$ and so on.
- Claim: Let $A = \text{P}^{\text{NP}} (= \text{P}^{\text{coNP}})$. Then
 - ① $\Sigma_1^P = \text{NP} \subseteq A$.
 - ② $\Pi_1^P = \text{coNP} \subseteq A$.
 - ③ $A \subseteq \Sigma_2^P$.
 - ④ $A \subseteq \Pi_2^P$.
- We denote A by Δ_2^P .

The Polynomial Hierarchy

Hierarchy via Oracle machines

Theorem (Alternate definition of Σ_i^P)

For every $i \geq 2$, $\Sigma_i^P = \text{NP}^{\Sigma_{i-1}\text{SAT}}$, where the latter denotes the set of languages decided by polynomial-time NDTM's with access to the oracle $\Sigma_{i-1}\text{SAT}$.

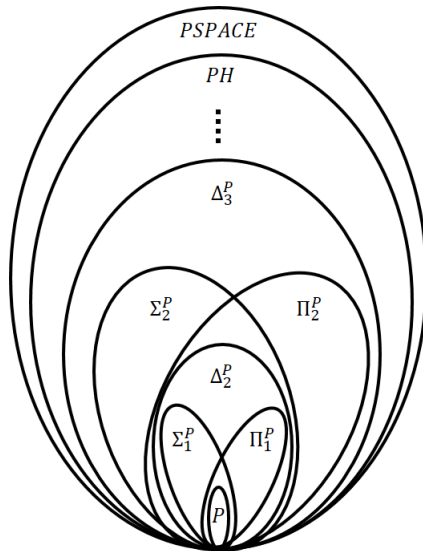
Theorem (Δ_1^P)

For every $i \geq 2$, $\Delta_1^P = \text{P}^{\Sigma_{i-1}\text{SAT}}$, where the latter denotes the set of languages decided by polynomial-time TM's with access to the oracle $\Sigma_{i-1}\text{SAT}$.

- So, we have $\Delta_2^P = \text{P}^{\text{NP}}$, $\Delta_3^P = \text{P}^{\text{NP}^{\text{NP}}}$ and so on.

Complexity Diagram

The Polynomial Hierarchy



End