

Polynomial hierarchy

In computational complexity theory, the **polynomial hierarchy** (sometimes called the **polynomial-time hierarchy**) is a hierarchy of complexity classes that generalize the classes **P**, **NP** and **co-NP** to oracle machines. It is a resource-bounded counterpart to the arithmetical hierarchy and analytical hierarchy from mathematical logic.

1 Definitions

There are multiple equivalent definitions of the classes of the polynomial hierarchy.

1. For the oracle definition of the polynomial hierarchy, define

$$\Delta_0^P := \Sigma_0^P := \Pi_0^P := P,$$

where **P** is the set of decision problems solvable in polynomial time. Then for $i \geq 0$ define

$$\Delta_{i+1}^P := P^{\Sigma_i^P}$$

$$\Sigma_{i+1}^P := NP^{\Sigma_i^P}$$

$$\Pi_{i+1}^P := \text{coNP}^{\Sigma_i^P}$$

where P^A is the set of decision problems solvable in polynomial time by a Turing machine augmented by an oracle for some complete problem in class **A**; the classes NP^A and coNP^A are defined analogously. For example, $\Sigma_1^P = NP$, $\Pi_1^P = \text{coNP}$, and $\Delta_2^P = P^{NP}$ is the class of problems solvable in polynomial time with an oracle for some NP-complete problem.

2. For the existential/universal definition of the polynomial hierarchy, let L be a language (i.e. a decision problem, a subset of $\{0,1\}^*$), let p be a polynomial, and define

$$\exists^p L := \left\{ x \in \{0,1\}^* \mid \left(\exists w \in \{0,1\}^{\leq p(|x|)} \right) \langle x, w \rangle \in L \right\},$$

where $\langle x, w \rangle \in \{0,1\}^*$ is some standard encoding of the pair of binary strings x and w as a single binary string. L represents a set of ordered pairs of strings, where the first string x is a member of $\exists^p L$, and the second string w is a “short” ($|w| \leq p(|x|)$) witness testifying that x is a member of $\exists^p L$. In other words, $x \in \exists^p L$ if and only if there exists a short witness w such that $\langle x, w \rangle \in L$. Similarly, define

$$\forall^p L := \left\{ x \in \{0,1\}^* \mid \left(\forall w \in \{0,1\}^{\leq p(|x|)} \right) \langle x, w \rangle \in L \right\}$$

Note that De Morgan’s laws hold: $(\exists^p L)^c = \forall^p L^c$ and $(\forall^p L)^c = \exists^p L^c$, where L^c is the complement of L .

Let \mathcal{C} be a class of languages. Extend these operators to work on whole classes of languages by the definition

$$\exists^p \mathcal{C} := \{ \exists^p L \mid p \text{ is a polynomial and } L \in \mathcal{C} \}$$

$$\forall^p \mathcal{C} := \{ \forall^p L \mid p \text{ is a polynomial and } L \in \mathcal{C} \}$$

Again, De Morgan’s laws hold: $\text{co} \exists^p \mathcal{C} = \forall^p \text{co} \mathcal{C}$ and $\text{co} \forall^p \mathcal{C} = \exists^p \text{co} \mathcal{C}$, where $\text{co} \mathcal{C} = \{ L^c \mid L \in \mathcal{C} \}$.

The classes **NP** and **co-NP** can be defined as $NP = \exists^P P$, and $\text{coNP} = \forall^P P$, where **P** is the class of all feasibly (polynomial-time) decidable languages. The polynomial hierarchy can be defined recursively as

$$\Sigma_0^P := \Pi_0^P := P$$

$$\Sigma_{k+1}^P := \exists^P \Pi_k^P$$

$$\Pi_{k+1}^P := \forall^P \Sigma_k^P$$

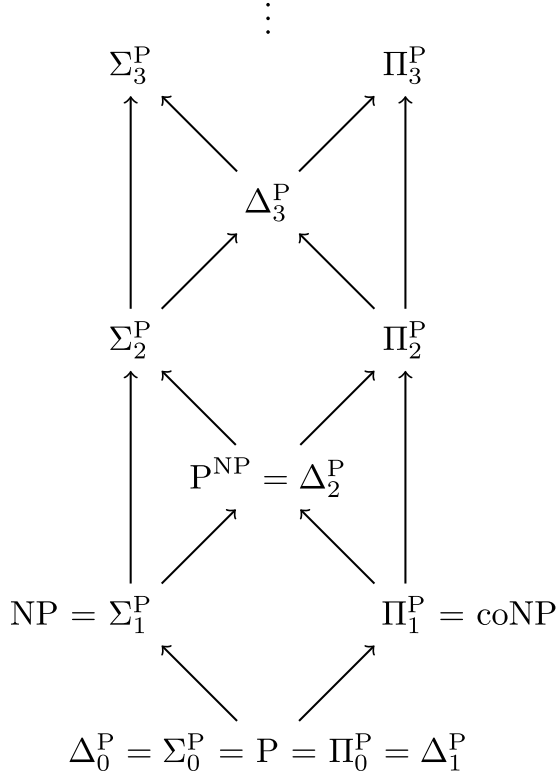
Note that $NP = \Sigma_1^P$, and $\text{coNP} = \Pi_1^P$.

This definition reflects the close connection between the polynomial hierarchy and the arithmetical hierarchy, where **R** and **RE** play roles analogous to **P** and **NP**, respectively. The analytic hierarchy is also defined in a similar way to give a hierarchy of subsets of the real numbers.

3. An equivalent definition in terms of alternating Turing machines defines Σ_k^P (respectively, Π_k^P) as the set of decision problems solvable in polynomial time on an alternating Turing machine with k alternations starting in an existential (respectively, universal) state.

2 Relations between classes in the polynomial hierarchy

The definitions imply the relations:



Commutative diagram equivalent to the polynomial time hierarchy. The arrows denote inclusion.

$$\Sigma_i^P \subseteq \Delta_{i+1}^P \subseteq \Sigma_{i+1}^P$$

$$\Pi_i^P \subseteq \Delta_{i+1}^P \subseteq \Pi_{i+1}^P$$

$$\Sigma_i^P = \text{co}\Pi_i^P$$

Unlike the arithmetic and analytic hierarchies, whose inclusions are known to be proper, it is an open question whether any of these inclusions are proper, though it is widely believed that they all are. If any $\Sigma_k^P = \Sigma_{k+1}^P$, or if any $\Sigma_k^P = \Pi_k^P$, then the hierarchy *collapses to level k*: for all $i > k$, $\Sigma_i^P = \Sigma_k^P$. In particular, if $P = NP$, then the hierarchy collapses completely.

The union of all classes in the polynomial hierarchy is the complexity class **PH**.

3 Properties

The polynomial hierarchy is an analogue (at much lower complexity) of the **exponential hierarchy** and **arithmetical hierarchy**.

It is known that PH is contained within **PSPACE**, but it is not known whether the two classes are equal. One useful reformulation of this problem is that $\text{PH} = \text{PSPACE}$ if and only if **second-order logic over finite structures** gains no additional power from the addition of a **transitive closure operator**.

If the polynomial hierarchy has any **complete problems**, then it has only finitely many distinct levels. Since there are **PSPACE-complete** problems, we know that if $\text{PSPACE} = \text{PH}$, then the polynomial hierarchy must collapse, since a PSPACE-complete problem would be a Σ_k^P -complete problem for some k .

Each class in the polynomial hierarchy contains \leq_m^P -complete problems (problems complete under polynomial-time many-one reductions). Furthermore, each class in the polynomial hierarchy is *closed under \leq_m^P -reductions*: meaning that for a class \mathcal{C} in the hierarchy and a language $L \in \mathcal{C}$, if $A \leq_m^P L$, then $A \in \mathcal{C}$ as well. These two facts together imply that if K_i is a complete problem for Σ_i^P , then $\Sigma_{i+1}^P = \text{NP}^{K_i}$, and $\Pi_{i+1}^P = \text{coNP}^{K_i}$. For instance, $\Sigma_2^P = \text{NP}^{\text{SAT}}$. In other words, if a language is defined based on some oracle in \mathcal{C} , then we can assume that it is defined based on a complete problem for \mathcal{C} . Complete problems therefore act as “representatives” of the class for which they are complete.

The **Sipser–Lautemann theorem** states that the class **BPP** is contained in the second level of the polynomial hierarchy.

Kannan’s theorem states that for any k , Σ_2 is not contained in **SIZE**(n^k).

Toda’s theorem states that the polynomial hierarchy is contained in $\text{P}^{\#P}$.

4 Problems in the polynomial hierarchy

- An example of a natural problem in Σ_2^P is *circuit minimization*: given a number k and a circuit A computing a **Boolean function** f , determine if there is a circuit with at most k gates that computes the same function f . Let \mathcal{C} be the set of all boolean circuits. The language

$$L = \{ \langle A, k, B, x \rangle \in \mathcal{C} \times \mathbb{N} \times \mathcal{C} \times \{0, 1\}^* \mid B \text{ has at most } k \text{ gates, and } A(B, x) = f(x) \}$$

is decidable in polynomial time. The language

$$CM = \left\{ \langle A, k \rangle \in \mathcal{C} \times \mathbb{N} \mid \begin{array}{l} \text{there exists a circuit } B \text{ with at most } k \text{ gates} \\ \text{such that } A \text{ and } B \text{ compute the same function} \end{array} \right\}$$

is the circuit minimization language. $CM \in \Sigma_2^P (= \exists^P \forall^P P)$ because L is decidable in polynomial time and because, given $\langle A, k \rangle$, $\langle A, k \rangle \in CM$ if and only if *there exists* a circuit B such that *for all* inputs x , $\langle A, k, B, x \rangle \in L$.

- A complete problem for Σ_k^P is **satisfiability for quantified Boolean formulas with k alternations of quantifiers** (abbreviated **QBF_k** or **QSAT_k**).

This is the version of the **boolean satisfiability problem** for Σ_k^P . In this problem, we are given a Boolean formula f with variables partitioned into k sets X_1, \dots, X_k . We have to determine if it is true that

$$\exists X_1 \forall X_2 \exists X_3 \dots f$$

That is, is there an assignment of values to variables in X_1 such that, for all assignments of values in X_2 , there exists an assignment of values to variables in X_3, \dots f is true?

The variant above is complete for Σ_k^P . The variant in which the first quantifier is “for all”, the second is “exists”, etc., is complete for Π_k^P .

5 See also

- EXPTIME
- Exponential hierarchy
- Arithmetic hierarchy

6 References

1. A. R. Meyer and L. J. Stockmeyer. The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space. *In Proceedings of the 13th IEEE Symposium on Switching and Automata Theory*, pp. 125–129, 1972. The paper that introduced the polynomial hierarchy.
2. L. J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, vol.3, pp. 1–22, 1976.
3. C. Papadimitriou. Computational Complexity. Addison-Wesley, 1994. Chapter 17. *Polynomial hierarchy*, pp. 409–438.
4. Michael R. Garey and David S. Johnson (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman. ISBN 0-7167-1045-5. Section 7.2: The Polynomial Hierarchy, pp. 161–167.

