Polynomial Hierarchy and Related Results

Jaspreet Batra
Mankul Gupta

IIT Bombay

September 26, 2016

Overview

1. Recall Σ_2^P and Define Π_2^P
2. The Polynomial Hierarchy
3. Karp-Lipton Theorem and Meyer's Theorem

Recall Σ_2^P

Def. The class Σ_2^P

The class Σ_2^P is the set of all languages L for which there exists a polynomial time Turing Machine M and a polynomial time function q, such that $x \in \mathrm{L}$ iff $\exists u \in \{0,1\}^{q(|x|)}\ \forall v \in \{0,1\}^{q(|x|)}\ \mathrm{M}(x, u, v) = 1$.

- Need to go beyond non-determinism
- Recall NP $\equiv$ 'short witness'
- For some problems, there may not be one

Σ_2^P : Examples

- EXACT INDSET $= \{(G, k)$: the largest independent set in G has size exactly $k\}$
  - Compare with INDSET $= \{(G, k)$: G has an independent set of size $\geq k\}$: Short witness $\implies$ INDSET $\in$ NP.
  - For EXACT INDSET, no apparent short witness
- MIN-EQ-DNF $= \{(\varphi, k)$: $\exists$ DNF formula ψ of size $\leq k$ that is equivalent to the DNF formula $\varphi\}$
- $\exists$ ... $\forall$ ... $\mathrm{M}(x, u, v) = 1$
- EXACT INDSET, MIN-EQ-DNF $\in \Sigma_2^P$

Welcome Π_2^P

What co-NP is to NP, Π_2^P is to Σ_2^P.

Def. The class Π_2^P

$\Pi_2^P = \{\overline{L} : L \in \Sigma_2^P\}$

Turing Machine definition: ....

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

Examples: EXACT-INDSET, MIN-EQ-DNF $\in \Pi_2^P$

The Polynomial Hierarchy PH

- PH is the generalization of classes like NP, coNP, Σ_2^P and Π_2^P
- Languages which can be defined by combination of a polynomial time computable predicate and a constant number of $\forall$ or $\exists$ quantifiers

- Σ_i^P : x $\in$ L iff $\exists u_1 \ \forall u_2 \ \ldots \ Q_i u_i$ M$(x, u_1, u_2, ..., u_i) = 1$,
  where Q$_i$ = $\forall$ or $\exists$ depending on whether i is odd or even.
- Π_i^P : x $\in$ L iff $\forall u_1 \ \exists u_2 \ \ldots \ Q_i u_i$ M$(x, u_1, u_2, ..., u_i) = 1$,
  where Q$_i$ = $\forall$ or $\exists$ depending on whether i is even or odd.

- PH $= \cup_i \ \Sigma_i^P$

The Polynomial Hierarchy PH

- Σ_i^P : x $\in$ L iff $\exists u_1 \ \forall u_2 \ \ldots \ Q_i u_i$ M$(x, u_1, u_2, ..., u_i) = 1$, where Q$_i$ = $\forall$ or $\exists$ depending on whether i is odd or even.
- Π_i^P : x $\in$ L iff $\forall u_1 \ \exists u_2 \ \ldots \ Q_i u_i$ M$(x, u_1, u_2, ..., u_i) = 1$, where Q$_i$ = $\forall$ or $\exists$ depending on whether i is even or odd.

- See that NP $= \Sigma_1^P$, coNP $= \Pi_1^P$
- In general, $\Pi_i^P = \text{co}\Sigma_i^P$

- Also, $\Sigma_i^P \subseteq \Pi_{i+1}^P$
- So, PH $= \cup_{i>0} \Pi_i^P$

Does the Polynomial Hierarchy collapse?

What does it mean for the hierarchy to collapse?
If for some i, $\Sigma_{i+1}^P = \Sigma_i^P$, then $\Sigma_i^P = \text{PH}$,
and we say that the PH collapses to the ith level.

The conjectures (beliefs?) $\text{P} \neq \text{NP}$, and $\text{NP} \neq \text{coNP}$,
can be generalized to the conjecture (belief?) that
for every i, Σ_i^P is strictly contained in Σ_{i+1}^P.

Does the Polynomial Hierarchy collapse?

Theorem 1. For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $\mathsf{PH} = \Sigma_i^P$, i.e., the PH collapses to the ith level.

Theorem 2. If P = NP, then PH = P, i.e., the PH collapses to P.

Complete Problems

- Σ_i^P-completeness: L is Σ_i^P-complete if L $\in \Sigma_i^P$ and for every L' $\in \Sigma_i^P$, L' $\leq_p$ L.
- Similarly, Π_i^P-completeness and PH-completeness.
- For every $i \in N$, Σ_i^P and Π_i^P have complete problems.
- The same is not likely true for the polynomial hierarchy itself. That is, it is believed that no language is PH-complete. (We can show that PH collapses otherwise.)

Polynomial Hierarchy via Oracle Machines

Definition of oracle machines.

for every O $\subseteq \{0,1\}^*$, P^O is the set containing every language that can be decided by a polynomial time deterministic TM with oracle access to O and similarly NP^O is the set of all languages which are decided by polynomial time NDTM with oracle access to O.

Theorem

For every i $\geq$ 2, $\Sigma_i^P = \mathrm{NP}^{\Sigma_{i-1}SAT}$, where the classes in right hand side denotes the set of languages decided by polynomial-time NDTMs with access to the oracle $\Sigma_{i-1}SAT$

Karp-Lipton Theorem

- Recall P/poly: Poly-time solvable given a poly-length external advice
- P/poly is a huge class
  - P $\subseteq$ P/Poly.
  - We have also seen BPP $\subseteq$ P/Poly.
  - Even some undecidable languages are in P/poly.
- So, it's natural to ask whether NP $\subseteq$ P/poly ?
- Karp and Lipton's motivation: does SAT have small circuits ?

Karp-Lipton Theorem

If NP $\subseteq$ P/poly, then PH $= \Sigma_2^P$.

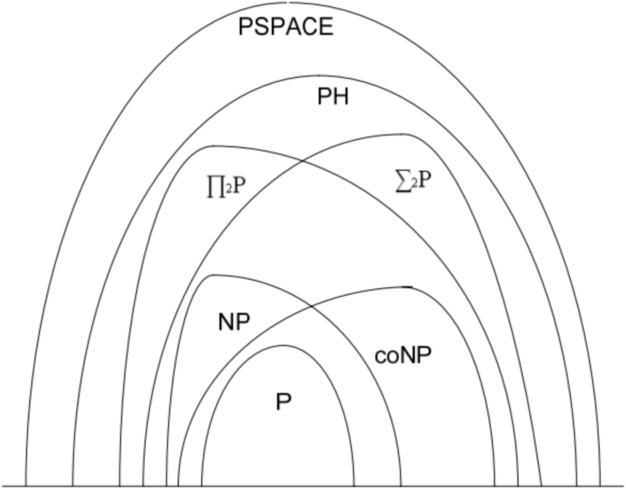
Meyer's Theorem

Is EXP in P/poly?

Meyer's Theorem

If EXP $\subseteq$ P/poly, then EXP $= \Sigma_2^P$.

So, where we at?



[Image source: Lecture notes by perso.esiee.fr/ mustafan]

But what happens when ...

www.scottaaronson.com/writings/phcollapse.pdf

POLYNOMIAL HIERARCHY COLLAPSES

Thousands Feared Tractable

by Scott Aaronson

PSPACE, April 12, 7PM EST—The polynomial hierarchy collapsed to the second level at 4:20PM this afternoon, prompting a frantic search for surviving hard problems. Over five hundred languages have been confirmed Σ_2^P-decidable, and rescue workers fear the count may reach as high as $\aleph_0$.

Despite ongoing investigation, the cause of the collapse remains unknown. Though many blamed sabotage by disgruntled computer-science majors, undergraduates insisted they lack the know-how to carry out such an attack. Some, including Dr. Gregory Chaitin of IBM's T.J. Watson Research Center, believe the collapse was an accident, with no explanation outside of itself. But citing Gödel's theorem, Chaitin cautioned that even an inconsistency in the Zermelo-Fraenkel axioms cannot be ruled out.

At an emergency press conference, President Stephen Cook declared that "today, we mourn the collapse of a hierarchy that symbolized our deepest hopes and conjectures. Yet let us renew our deter-

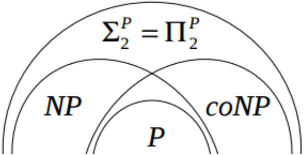


PHOTO: The scene of the devastation.

collapse. "PH was built to take a lot of abuse, at least relative to an oracle," he said. "P = BQP, satisfying assignments constructible via nonadaptive NP queries, you name it. I'm afraid we're up against a new, nonrelativizing menace."

The recursively enumerable languages were nearly unanimous in support of the victims, with all but

[Source: www.scottaaronson.com]

References

The End