Complexity Reading Group 10/8/2015
Brown University

1 Recap/Background

Definition 0: Recall that **NP** is the set of all languages L for which there exists a polynomial time TM M and a polynomial q such that:

$$x \in L \equiv \exists u \in \{0,1\}^{q(|x|)} \; M(x,u) = 1 \tag{1}$$

We call u a *witness* or *certificate* for x.

Note: $\mathbf{P} = \Sigma_0^P$, $\mathbf{NP} = \Sigma_1^P$, and $\mathbf{coNP} = \Pi_1^P$.

Consequently, **coNP** is the set of all languages whose complements are in **NP**. It's worth noting that it is believed $\mathbf{coNP} \neq \mathbf{NP}$, which I actually found a bit surprising.

2 Polynomial Hierarchy

Basic Idea:

- A generalization of **P**, **NP**, **coNP**.
- Three ways to define it.
    1. Quantified predicates
    2. Alternating Turing Machines
    3. Oracles
- Useful for many different investigations in complexity.

Definition 1: 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:

$$x \in L \equiv \exists u \in \{0,1\}^{q(|x|)} \; \forall v \in \{0,1\}^{q(|x|)} M(x,u,v) = 1 \tag{2}$$

We can define Π_2^P as $\{\bar{L} : L \in \Sigma_2^P\}$, but more specifically:

Definition 2: The class Π_2^P is the set of all languages L for which there exists a polynomial time TM M and a polynomial q such that, $\forall_x : x \in \{0,1\}^*$:

$$x \in L \equiv \forall u \in \{0,1\}^{q(|x|)} \ \exists v \in \{0,1\}^{q(|x|)} M(x,u,v) = 1 \tag{3}$$

2.1 Generalized Definition

PH generalizes the classes **NP**, **coNP**, Σ_2^P, and Π_2^P to include all languages that can be defined by a polynomial-time predicate.

Definition 6: For $i \geq 1$, $L \in \Sigma_i^P$ if $\exists$ poly-time TM, M, and a polynomial q, s.t.:

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

Where $Q_i = \begin{cases} \forall & i = 0 \mod 2 \\ \exists & i = 1 \mod 2 \end{cases}$

$$\text{Polynomial Hierarchy } (PH) = \cup_i \Sigma_i^P$$

$$\Pi_i^P = \textbf{co}\Sigma_i^P = \{\bar{L} : L \in \Sigma_i^P\}$$

$$\textbf{coNP} = \Pi_i^P$$

$$\textbf{NP} = \Sigma_i^P$$

So:

$$\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+2}^P \rightarrow PH = \cup_i \Pi_i^P$$

Also note that: $\forall_{i \geq 1} : \Pi_i^P = \textbf{co}\Sigma_i^P = \{\bar{L} : L \in \Sigma_i^P\}$

Note: there are other equivalent definitions, which we're not going into.

3 Results

We believe $\mathbf{P} \neq \mathbf{NP}$, and $\mathbf{NP} \neq \mathbf{coNP}$. Using the polynomial hierarchy, we can generalize this claim to say $\forall_{i \geq 1} : \Sigma_i^P \subset \Sigma_{i+1}^P$, meaning that the *polynomial hierarchy does not collapse.*

If the polynomial hierarchy *does* collapse, then there is some i such that $\Sigma_i^P = \cup_j \Sigma_j^P = PH$.

3.1 Theorem 5.6

Theorem 5.6:

1. For every $i \geq 1$, if $\Sigma_i^P = \Pi_i^P$, then $PH = \Sigma_i^P$, i.e. the hierarchy collapses to the i-th level.
2. If $\mathbf{P} = \mathbf{NP}$, then $PH = \mathbf{P}$, (i.e. the hierarchy collapses to $\mathbf{P}$).

Proof of 5.6.2: Strategy: suppose $\mathbf{P} = \mathbf{NP}$, prove by induction on i that $\Sigma_i^P, \Pi_i^P \subseteq \mathbf{P}$.

Base Case (i=1): Clearly true for $i = 1$, since under our assumption, $\mathbf{P} = \mathbf{NP} = \mathbf{coNP}$.

Inductive Case:

We let:

$$\Sigma_{i-1}^P, \Pi_{i-1}^P \subseteq \mathbf{P} \tag{IH}$$

And want to show:

$$\Sigma_i^P, \Pi_i^P \subseteq \mathbf{P} \tag{WTS}$$

Let $L \in \Sigma_i^P$, we show that $L \in \mathbf{P}$.

By definition there exists a polynomial time machine M and a polynomial q such that

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

Consider language L', defined as:

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

Note that $L' \in \Pi_{i-1}^P$, so under the IH is in $\mathbf{P}$. Consequently, there is a TM M', such that:

$$x \in L \equiv \exists u_1 \in \{0,1\}^{q(|x|)} M'(x, u_1) = 1$$

But this means $L \in \mathbf{NP}$, and hence, under our assumption, $L \in \mathbf{P}$. □

(An identical idea shows that if $L \in \Pi_i^P$, then $L \in P$)

Definition 7: A language L is Σ_i^P-complete if $L \in \Sigma_i^P$ and for every $L' \in \Sigma_i^P, L' \leq_p L$

Note: we can define Π_i^P-completeness and PH-completeness in the same way.

Below we show that for every $i \in \mathbb{N}$, both Σ_i^P and Π_i^P have complete problems.

In contrast, the polynomial-hierarchy is believed not to have a complete problem!

Claim 5.7: Suppose that there exists a language L that is **PH**-complete, then there exists an i such that $\mathbf{PH} = \Sigma_i^P$, i.e. the hierarchy collapses to the i-th level.

One other fun fact: $\mathbf{PH} \subseteq \mathbf{PSPACE}$.

3.2 Theorem 6.13

Recall the definition of $\mathbf{P}_{\text{poly}}$:

Theorem 6.13: $\mathbf{NP} \subseteq \mathbf{P}_{\text{poly}} \rightarrow PH = \Sigma_2^P$

Proof: To show $\mathbf{PH} = \Sigma_2^P$, it is enough to show $\Pi_2^P \subset \Sigma_2^P$, in particular, it suffices to show that Σ_2^P contains the Π_2^P-complete language Π_2SAT consisting of all true formulae of the form:

$$\forall u \in \{0,1\}^n \exists v \in \{0,1\}^n \phi(u,v) = 1 \tag{4}$$

Where ϕ is an unquantified Boolean formula.

If $\mathbf{NP} \subseteq \mathbf{P}_{poly}$ then there is a polynomial p and a $p(n)$-sized circuit family $\{C_n\}_{n\in\mathbb{N}}$, such that, for every Boolean formula ϕ and $u \in \{0,1\}^n$, $C_n(\phi, u) = 1$, iff there exists $v \in \{0,1\}^n$ such that $\phi(u,v) = 1$.

From an earlier result, we know that there is a $q(n)$ sized circuit family $\{C'_n\}_{n\in\mathbb{N}}$ such that for every such formula ϕ and $u \in \{0,1\}^n$, if there is a string $v \in \{0,1\}^n$ such that $\phi(u,v) = 1$ then $C'_n(\phi, u)$ outputs such a string v.

Since C'_n can be described using $10q(n)^2$ bits, it follows that if Eq. 4 is true, then we know:

$$\exists w \in \{0,1\}^{10q(n)^2} \forall u \in \{0,1\}^n w \text{ describes a circuit } C' \text{ s.t. } \phi(u, C'(\phi, u)) = 1 \tag{5}$$

Yet if Eq. 4 is false, then the above is false too, so consequently Eq. 5 is logically equivalent.

Since evaluating a circuit on an input can be done in polynomial time, evaluating the truth of Eq. 5 can be done in Σ_2^P. Therefore we can evaluate Eq. 4 in Σ_2^P as well. □

4 In Summary

- The polynomial hierarchy is the set of languages that can be defined via a constant number of alternating quantifiers. It also has equivalent definitions via alternating TMs and oracle TMs. It contains several natural problems that are not known (or believed) to be in NP.
- We conjecture that the hierarchy does not collapse in the sense that each of its levels is distinct from the previous ones.

4.1 Problems to Check Out

- 5.1
- 5.4
- 5.11