Polynomial Hierarchy

"A polynomial-bounded version of Kleene's Arithmetic Hierarchy becomes trivial if $\mathbf{P} = \mathbf{NP}$."

Karp, 1972

Larry Stockmeyer and Albert Meyer introduced polynomial hierarchy.

---

1. Larry Stockmeyer and Albert Meyer. The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space. SWAT'72.

Synopsis

1. Meyer-Stockmeyer's Polynomial Hierarchy
2. Stockmeyer-Wrathall Characterization
3. Chandra-Kozen-Stockmeyer Theorem
4. Infinite Hierarchy Conjecture
5. Time-Space Trade-Off

Meyer-Stockmeyer's Polynomial Hierarchy

Problem Beyond **NP**

Meyer and Stockmeyer observed that MINIMAL does not seem to have short witnesses.

$$\mathtt{MINIMAL} = \{\varphi \mid \varphi \text{ DNF} \wedge \forall \text{ DNF } \psi.|\psi|<|\varphi| \Rightarrow \exists u.\neg(\psi(u)\Leftrightarrow\varphi(u))\}.$$

Notice that $\overline{\mathtt{MINIMAL}}$ can be solved by an NDTM that queries SAT a polynomial time.

- Why DNF?

$$
\begin{aligned}
\mathbf{P}^{\mathcal{C}} &= \bigcup_{A \in \mathcal{C}} \mathbf{P}^{A}, \\
\mathbf{NP}^{\mathcal{C}} &= \bigcup_{A \in \mathcal{C}} \mathbf{NP}^{A}.
\end{aligned}
$$

Meyer-Stockmeyer's Definition

The complexity classes $\Sigma_i^p, \Pi_i^p, \Delta_i^p$ are defined as follows:

$$
\begin{aligned}
\Sigma_0^p &= \mathbf{P}, \\
\Sigma_{i+1}^p &= \mathbf{NP}^{\Sigma_i^p}, \\
\Delta_{i+1}^p &= \mathbf{P}^{\Sigma_i^p}, \\
\Pi_i^p &= \overline{\Sigma_i^p}.
\end{aligned}
$$

The following hold:

- $\Sigma_i^p \subseteq \Delta_{i+1}^p \subseteq \Sigma_{i+1}^p$,
- $\Pi_i^p \subseteq \Delta_{i+1}^p \subseteq \Pi_{i+1}^p$.

Notice that $\Pi_{i+1}^p = \mathbf{coNP}^{\Sigma_i^p}$ by definition.

The polynomial hierarchy is the complexity class $\mathbf{PH} = \bigcup_{i \geq 0} \Sigma_i^p$.

Natural Problem in the Second Level

"Synthesizing circuits is exceedingly difficult. It is even more difficult to show that a circuit found in this way is the most economical one to realize a function. The difficulty springs from the large number of essentially different networks available."

Claude Shannon, 1949

Umans showed in 1998 that the following language is Σ_2^p-complete.

$$\texttt{MIN-EQ-DNF} = \{\langle \varphi, k \rangle \mid \varphi \text{ DNF} \wedge \exists \text{ DNF } \psi.|\psi| \leq k \wedge \forall u.\psi(u) \Leftrightarrow \varphi(u)\}.$$

- $\overline{\texttt{MIN-EQ-DNF}}$ is the problem referred to by Shannon.
- The complexity of $\texttt{MINIMAL}$, as well as $\overline{\texttt{MINIMAL}}$, is not known.

Natural Problem in the Second Level

`SUCCINCT SET COVER`:

Given a set $S = \{\varphi_1, \ldots, \varphi_m\}$ of 3-DNF's and an integer k, is there a subset $S' \subseteq \{1, \ldots, m\}$ of size at most k such that $\bigvee_{i \in S'} \varphi_i$ is a tautology?

This is another Σ_2^p-complete problem (Umans, 1998).

Natural Problem in the Second Level

`EXACT INDSET` refers to the following problem:

$$\{\langle G, k\rangle \mid \text{the largest independent sets of } G \text{ are of size } k\}.$$

It is in Σ_2^p and is **DP**-complete.

$L \in \mathbf{DP}$ if $L = L_0 \cap L_1$ for some $L_0 \in \mathbf{NP}$ and some $L_1 \in \mathbf{coNP}$. Clearly

$$\mathbf{NP}, \mathbf{coNP} \subseteq \mathbf{DP}.$$

Stockmeyer-Wrathall Characterization

In 1976, Stockmeyer defined Polynomial Hierarchy in terms of alternation of quantifier and Wrathall proved that it is equivalent to the original definition.

---

1. Larry Stockmeyer. The Polynomial-Time Hierarchy. Theoretical Computer Science, 3:1-22, 1976.
2. Celia Wrathall. Complete Sets and the Polynomial-Time Hierarchy. Theoretical Computer Science. 3:23-33, 1976.

Logic Characterization

Theorem. Suppose $i \geq 1$.

- $L \in \Sigma_i^p$ iff there exists a P-time TM $\mathbb{M}$ and a polynomial q such that for all $x \in \{0,1\}^*$,

$$x \in L \text{ iff } \exists u_1{\in}\{0,1\}^{q(|x|)}\forall u_2{\in}\{0,1\}^{q(|x|)} \ldots Q_i u_i{\in}\{0,1\}^{q(|x|)}.\mathbb{M}(x,\widetilde{u}) = 1.$$

- $L \in \Pi_i^p$ iff there exists a P-time TM $\mathbb{M}$ and a polynomial q such that for all $x \in \{0,1\}^*$,

$$x \in L \text{ iff } \forall u_1{\in}\{0,1\}^{q(|x|)}\exists u_2{\in}\{0,1\}^{q(|x|)} \ldots Q_i u_i{\in}\{0,1\}^{q(|x|)}.\mathbb{M}(x,\widetilde{u}) = 1.$$

---

1. Celia Wrathall. Complete Sets and the Polynomial-Time Hierarchy. Theoretical Computer Science. 3:23-33, 1976.

Proof of Wrathall Theorem

Let $\mathbb{M}$ be a P-time TM and q a polynomial such that $x \in L$ if and only if

$$\exists u_1 \in \{0,1\}^{q(|x|)} \ldots Qu_{i+1} \in \{0,1\}^{q(|x|)}.\mathbb{M}(x, u_1, \ldots, u_{i+1}) = 1.$$

Given x an NDTM guesses a u_1 and asks if the following is true

$$\forall u_2 \in \{0,1\}^{q(|x|)} \ldots Qu_{i+1} \in \{0,1\}^{q(|x|)}.\mathbb{M}(x, u_1, \ldots, u_{i+1}) = 1.$$

By induction hypothesis the above formula can be evaluated by querying a Σ_i^p oracle.

Proof of Wrathall Theorem

Let L be decided by a P-time NDTM $\mathbb{N}$ with access to some oracle $A \in \Sigma_i^p$. Now by Cook-Levin Theorem, $x \in L$ if and only if

$\exists \widetilde{z}.\exists c_1, \ldots, c_m, a_1, \ldots, a_k.\exists u_1, \ldots, u_k.(\mathbb{N}$ accepts x using choices $c_1, \ldots, c_m$ and answers $a_1, \ldots, a_k$ to the queries $u_1, \ldots, u_k) \wedge (\bigwedge_{i \in [k]} a_i = 1 \Rightarrow u_i \in A)$
$\wedge\ (\bigwedge_{i \in [k]} a_i = 0 \Rightarrow u_i \in \overline{A})$,

where $\widetilde{z}$ are introduced by the Cook-Levin reduction. We are done by induction.

Σ_iSAT

Let $\Sigma_i\mathtt{SAT}$ be the subset of $\mathtt{TQBF}$ that consists of all tautologies of the following form

$$\exists u_1 \forall u_2 \ldots Q_i u_i.\varphi(u_1, \ldots, u_i),$$

where $\varphi(u_1, \ldots, u_i)$ is a propositional formula.

Theorem (Meyer and Stockmeyer, 1972). $\Sigma_i\mathtt{SAT}$ is Σ_i^p-complete.

Proof.

Clearly $\Sigma_i\mathtt{SAT} \in \Sigma_i^p$. The completeness is defined with regards to Karp reduction. □

Theorem (Stockmeyer, Wrathall, 1976). **PH** $\subseteq$ **PSPACE**.

Chandra-Kozen-Stockmeyer Theorem

  

Ashok Chandra, Dexter Kozen and Larry Stockmeyer introduced Alternating Turing Machines that give alternative characterization of complexity classes.

---

1. Alternation. Journal of the ACM, 28(1):114-133, 1981.

Alternating Turing Machine

An Alternating Turing Machine (ATM) is an NDTM in which every state is labeled by an element of $\{\exists, \forall, \texttt{accept}, \texttt{halt}\}$.

We say that an ATM $\mathbb{A}$ accepts x if there is a subtree Tr of the execution tree of $\mathbb{A}(x)$ satisfying the following:

- The initial configuration is in Tr.
- All leaves of Tr are labeled by $\texttt{accept}$.
- If a node labeled by $\forall$ is in Tr, both children are in Tr.
- If a node labeled by $\exists$ is in Tr, one of its children is in Tr.

Complexity via ATM

For every $T : \mathbf{N} \to \mathbf{N}$, we say that an ATM $\mathbb{A}$ runs in $T(n)$-time if for every input $x \in \{0,1\}^*$ and for all nondeterministic choices, $\mathbb{A}$ halts after at most $T(|x|)$ steps.

- **ATIME**$(T(n))$ contains L if there is a $cT(n)$-time ATM $\mathbb{A}$ for some constant c such that, for all $x \in \{0,1\}^*$, $x \in L$ if and only if $\mathbb{A}(x) = 1$.
- **ASPACE**$(S(n))$ is defined analogously.

Example of ATM

TQBF is solvable by an ATM in quadratic time and linear space.

Complexity Class via ATM

$$
\begin{aligned}
\mathbf{AL} &= \mathbf{ASPACE}(\log n), \\
\mathbf{AP} &= \bigcup_{c>0} \mathbf{ATIME}(n^c), \\
\mathbf{APSPACE} &= \bigcup_{c>0} \mathbf{ASPACE}(n^c), \\
\mathbf{AEXP} &= \bigcup_{c>0} \mathbf{ATIME}(2^{n^c}), \\
\mathbf{AEXPSPACE} &= \bigcup_{c>0} \mathbf{ASPACE}(2^{n^c}).
\end{aligned}
$$

Theorem. Assume the relevant time/space functions are constructible. Then

1. $\mathbf{NSPACE}(S(n)) \subseteq \mathbf{ATIME}(S^2(n))$.
2. $\mathbf{ATIME}(T(n)) \subseteq \mathbf{SPACE}(T(n))$.
3. $\mathbf{ASPACE}(S(n)) \subseteq \bigcup_{c>0} \mathbf{TIME}(c^{S(n)})$.
4. $\mathbf{TIME}(T(n)) \subseteq \mathbf{ASPACE}(\log T(n))$.

---

1. Savitch's proof. Recursive calls are implemented using $\forall$-state. We need to assume that $S(n)$ is constructible in $S(n)^2$ time.
2. Traversal of configuration tree. Counters of length $T(n)$. We need to assume that $T(n)$ is also space constructible.
3. Depth first traversal of configuration graph.
4. Backward guessing ($\exists$) and parallel checking ($\forall$) in the configuration circuit.

Chandra-Kozen-Stockmeyer Theorem

$$
\begin{array}{ccccccccc}
 & & \mathbf{AL} & \subseteq & \mathbf{AP} & \subseteq & \mathbf{APSPACE} & \subseteq & \mathbf{AEXP} & \ldots \\
 & & = & & = & & = & & = & \ldots \\
\mathbf{L} & \subseteq & \mathbf{P} & \subseteq & \mathbf{PSPACE} & \subseteq & \mathbf{EXP} & \subseteq & \mathbf{EXPSPACE} & \ldots
\end{array}
$$

Bounded Alternation

$L \in \mathbf{\Sigma}_i\mathbf{TIME}(T(n))/\mathbf{\Pi}_i\mathbf{TIME}(T(n))$ if

L is accepted by an $O(T(n))$-time ATM $\mathbb{A}$ with q_{start} labeled by $\exists/\forall$, and on every path the machine $\mathbb{A}$ may alternate at most $i-1$ times.

Polynomial Hierarchy Defined via ATM

Theorem. For every $i \geq 1$, the following hold:

$$\begin{aligned} \Sigma_i^p &= \bigcup_{c>0} \Sigma_i\mathbf{TIME}(n^c), \\ \Pi_i^p &= \bigcup_{c>0} \Pi_i\mathbf{TIME}(n^c). \end{aligned}$$

Use the logical characterization.

Infinite Hierarchy Conjecture

Theorem. If $\mathbf{NP} = \mathbf{P}$ then $\mathbf{PH} = \mathbf{P}$.

Suppose $\Sigma_i^p = \mathbf{P}$. Then $\Sigma_{i+1}^p = \mathbf{NP}^{\Sigma_i^p} = \mathbf{NP}^{\mathbf{P}} = \mathbf{NP} = \mathbf{P}$.

Theorem (Meyer and Stockmeyer, 1972). For every $i \geq 1$, if $\Sigma_i^p = \Pi_i^p$ then $\mathbf{PH} = \Sigma_i^p$.

Suppose $\Sigma_k^p = \Pi_k^p$. Then $\Sigma_{k+1}^p = \Sigma_k^p = \Pi_k^p = \Pi_{k+1}^p$.

Theorem. If there exists a language L that is **PH**-complete with regards to Karp reduction, then some i exists such that $\mathbf{PH} = \Sigma_i^p$.

If such a language L exists, then $L \in \Sigma_i^p$ for some i. Consequently every language in **PH** is Karp reducible to L.

Theorem. If **PH** $=$ **PSPACE**, then **PH** collapses.

If **PH** $=$ **PSPACE**, then `TQBF` would be **PH**-complete.

Infinite Hierarchy Conjecture. Polynomial Hierarchy does not collapse.

Many results in complexity theory take the following form

"If something is not true, then the polynomial hierarchy collapses".

Time-Space Trade-Off

To summarize our current understanding of NP-completeness from an algorithmic point of view, it suffices to say that at the moment we cannot prove either of the following statements:

$$
\begin{aligned}
\mathtt{SAT} &\notin \mathbf{TIME}(n), \\
\mathtt{SAT} &\notin \mathbf{SPACE}(\log n).
\end{aligned}
$$

We can however prove that $\mathtt{SAT}$ cannot be solved by any TM that runs in both linear time and logspace. Notationally,

$$\mathtt{SAT} \notin \mathbf{TISP}(n, \log n).$$

TISP

Suppose $S, T : \mathbf{N} \to \mathbf{N}$. A problem is in

$$\mathbf{TISP}(T(n), S(n))$$

if it is decided by a TM that on every input x takes at most $O(T(|x|))$ time and uses at most $O(S(|x|))$ space.

Time-Space Tradeoff for $\mathtt{SAT}$

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

We show that $\mathbf{NTIME}(n) \nsubseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$, which implies the theorem for the following reason:

1. Using Cook-Levin reduction a problem $L \in \mathbf{NTIME}(n)$ is reduced to a formula, every bit of the formula can be computed in logarithmic space and polylogarithmic time.
2. If $\mathtt{SAT} \in \mathbf{TISP}(n^{1.1}, n^{0.1})$, then F could be computed in $\mathbf{TISP}(n^{1.1}\mathrm{polylog}(n), n^{0.1}\mathrm{polylog}(n))$.
3. But then one would have $L \in \mathbf{TISP}(n^{1.2}, n^{0.2})$.

The proof of $\mathbf{NTIME}(n) \nsubseteq \mathbf{TISP}(n^{1.2}, n^{0.2})$ is given next.

The Cook-Levin reduction makes use of the configuration circuit.

$\mathbf{TISP}(n^{12}, n^2) \subseteq \Sigma_2\mathbf{TIME}(n^8)$.

Suppose L is decided by $\mathbb{M}$ using n^{12} time and n^2 space.

- Given input x a node of $G_{\mathbb{M},x}$ is of length $O(n^2)$.
- $x \in L$ iff $C_{\texttt{accept}}$ can be reached from $C_{\texttt{start}}$ in n^{12} steps.
- There is such a path iff there exist n^6 nodes $C_1, \ldots, C_{n^6}$, whose total length is $O(n^8)$, such that, for all $i \in \{1, \ldots, n^6\}$,
  C_i can be reached from C_{i-1} in $O(n^6)$-steps.
- The latter condition can be verified in $O(n^6 \log n)$-time by resorting to a universal machine.

It is now easy to see that $L \in \Sigma_2\mathbf{TIME}(n^8)$.

If $\mathbf{NTIME}(n) \subseteq \mathbf{TIME}(n^{1.2})$ then $\Sigma_2\mathbf{TIME}(n^8) \subseteq \mathbf{NTIME}(n^{9.6})$.

Suppose $L \in \Sigma_2\mathbf{TIME}(n^8)$. Then some c, d and $(O(n^8))$-time TM $\mathbb{M}$ exist such that $x \in L$ iff

$$\exists u \in \{0,1\}^{c|x|^8}.\forall v \in \{0,1\}^{d|x|^8}.\mathbb{M}(x,u,v) = 1. \tag{1}$$

Given $\mathbb{M}$ one can design a linear time NDTM $\mathbb{N}$ that given $x \circ u$ returns 1 iff $\exists v \in \{0,1\}^{d|x|^8}.\mathbb{M}(x,u,v) = 0$.

- By assumption there is some $O(n^{1.2})$-time TM $\mathbb{D}$ such that $\mathbb{D}(x,u) = 1$ iff $\exists v \in \{0,1\}^{d|x|^8}.\mathbb{M}(x,u,v) = 0$.
- Consequently $\overline{\mathbb{D}}(x,u) = 1$ iff $\forall v \in \{0,1\}^{d|x|^8}.\mathbb{M}(x,u,v) = 1$.

It follows that there is an $O(n^{9.6})$ time NDTM $\mathbb{C}$ such that

$$\mathbb{C}(x) = 1 \text{ iff } \exists u \in \{0,1\}^{c|x|^8}.\overline{\mathbb{D}}(x,u) = 1 \text{ iff } (1) \text{ holds iff } x \in L,$$

implying that $L \in \mathbf{NTIME}(n^{9.6})$.

$$
\begin{array}{rcl}
\mathbf{NTIME}(n) & \subseteq & \mathbf{TISP}(n^{1.2}, n^{0.2}),\ \text{hypothesis} \\
& \Downarrow & \\
\mathbf{NTIME}(n^{10}) & \subseteq & \mathbf{TISP}(n^{12}, n^{2}) \\
& \Downarrow & \\
\mathbf{NTIME}(n^{10}) & \subseteq & \Sigma_2\mathbf{TIME}(n^{8}),\ \text{alternation introduction} \\
& \Downarrow & \\
\mathbf{NTIME}(n^{10}) & \subseteq & \mathbf{NTIME}(n^{9.6}),\ \text{alternation elimination,} \\
& \text{but} & \\
\mathbf{NTIME}(n^{9.6}) & \subsetneq & \mathbf{NTIME}(n^{10}),\ \text{diagonalization.}
\end{array}
$$

Proof by Indirect Diagonalization

Suppose we want to prove $\mathbf{NTIME}(n) \not\subseteq \mathbf{TISP}(T(n), S(n))$.

1. Assume $\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(T(n), S(n))$.
2. Derive unlikely inclusions of complexity classes.
   - Introduce alternation to speed up space bound computation.
   - Eliminate alternation using hypothesis.
3. Derive a contradiction using a diagonalization argument.

Lance Fortnow proved the first time-space lower bound. A survey on the time-space lower bounds for satisfiability is given by Dieter van Melkebeek.

---

1. Lance Fortnow. Time-Space Tradeoffs for Satisfiability. Journal of Computer and System Sciences, 60:337-353, 2000.
2. Dieter van Melkebeek. A Survey of Lower Bounds for Satisfiability and Related Problems. Foundations and Trends in Theoretical Computer Science, 2:197-303, 2007.