

# COMPLEXITY THEORY

## Lecture 17: The Polynomial Hierarchy

Markus Krötzsch  
Knowledge-Based Systems

TU Dresden, 10th Dec 2019

### ATM vs. DTM

We have observed four major relationships between alternating and deterministic complexity classes. For the special case of polynomial bounds, we got:

$$\text{APTime} \subseteq \text{PSPACE}$$

**How?** Deterministic depth-first search on ATMs computation tree.

$$\text{APTime} \supseteq \text{PSPACE}$$

**How?** Use alternation to implement Savitch-style middle-first search in polyspace.

$$\text{APSpace} \subseteq \text{ExpTime}$$

**How?** Analyse the exponential ATM configuration graph deterministically.

$$\text{APSpace} \supseteq \text{ExpTime}$$

**How?** Re-trace exponential computation path by verifying local changes.

### Review: ATM vs. DTM

### From Deterministic Time To Alternating Space

Let  $h : \mathbb{N} \rightarrow \mathbb{R}$  be a function in  $O(g)$  that defines the exact time bound for  $\mathcal{M}$  (no  $O$ -notation), and that can be computed in space  $O(\log g)$ .

```

01 ATMsimulateTM(TM M, input word w, time bound h) :
02   existentially guess s ≤ h(|w|) // halting step
03   existentially guess i ∈ {0, ..., s} // halting position
04   existentially guess ω ∈ Q × Γ // halting cell + state
05   if M would not halt in ω :
06     return false
07   for j = s, ..., 1 do :
08     existentially guess ⟨ω-1, ω0, ω1⟩ ∈ Ω3
09     if M(ω-1, ω0, ω1) ≠ ω :
10       return false
11     universally choose ℓ ∈ {-1, 0, 1}
12     ω := ωℓ
13     i := i + ℓ
14   // after tracing back s steps, check input configuration:
15   return "input configuration of M on w has ω at position i"

```

## A Remark on (Non)determinism

For each cell that is to be verified:

- we guess three predecessor cells,
- which we then verify recursively.

↪ The contents of the same cell is guessed in several places of the ATM computation tree (“in several recursive subprocesses”)

If processes do not exchange information,  
how do we know that the guesses are not contradicting each other?

Because of determinism:

- The simulated TM is deterministic
- Hence, if the starting point is determined, every future cell in every position is determined too
- Therefore, for every cell, there is only one possible guess that eventually leads to the right input tape

↪ Independent guesses, if correct, must generally be the same

## A Remark on Space-Constructibility

Our algorithm needs to compute  $h$  in logarithmic space w.r.t. its absolute value to implement the line

```
02  existentially guess  $s \leq h(|w|)$   // halting step
```

However, we could also avoid this:

- The algorithm from line 03 on checks if the TM halts after  $s$  steps
- We can make a similar algorithm that checks if the TM does **not** halt after  $s$  steps
- We can then use an overall algorithm that increments  $s$  one by one (starting from 1):
  - For each value of  $s$ , guess if the TM halts after this time or not
  - Check the guess using the above procedures
  - Stop when the halting configuration has been found
- Because of the time bound on the simulated TM,  $s$  will not become larger than  $2^{O(f)}$  here, so we can always store it in space  $f$ .

## Summary: Alternating vs. Deterministic Classes

We can sum up our findings as follows:

$$\begin{array}{ccccccc} L & \subseteq & PTime & \subseteq & PSpace & \subseteq & ExpTime & \subseteq & ExpSpace \\ & & \parallel & & \parallel & & \parallel & & \parallel \\ & & ALogSpace & \subseteq & APTime & \subseteq & APSPACE & \subseteq & AExpTime \end{array}$$

## The Polynomial Hierarchy

## Bounding Alternation

For ATMs, alternation itself is a resource. We can distinguish problems by how much alternation they need to be solved.

We first classify computations by counting their quantifier alternations:

**Definition 17.1:** Let  $\mathcal{P}$  be a computation path of an ATM on some input.

- $\mathcal{P}$  is of type  $\Sigma_1$  if it consists only of existential configurations (with the exception of the final configuration)
- $\mathcal{P}$  is of type  $\Pi_1$  if it consists only of universal configurations
- $\mathcal{P}$  is of type  $\Sigma_{i+1}$  if it starts with a sequence of existential configurations, followed by a path of type  $\Pi_i$
- $\mathcal{P}$  is of type  $\Pi_{i+1}$  if it starts with a sequence of universal configurations, followed by a path of type  $\Sigma_i$

## Alternation-Bounded Complexity

We are interested in the power of ATMs that are both time/space-bounded and alternation-bounded:

**Definition 17.4:** Let  $f : \mathbb{N} \rightarrow \mathbb{R}^+$  be a function.  $\Sigma_i\text{Time}(f(n))$  is the class of all languages that are decided by some  $O(f(n))$ -time bounded  $\Sigma_i$  ATM. The classes  $\Pi_i\text{Time}(f(n))$ ,  $\Sigma_i\text{Space}(f(n))$  and  $\Pi_i\text{Space}(f(n))$  are defined similarly.

The most popular classes of these problems are the alternation-bounded polynomial time classes:

$$\Sigma_i\text{P} = \bigcup_{d \geq 1} \Sigma_i\text{Time}(n^d) \quad \text{and} \quad \Pi_i\text{P} = \bigcup_{d \geq 1} \Pi_i\text{Time}(n^d)$$

Hardness for these classes is defined by polynomial many-one reductions as usual.

## Alternation-Bounded ATMs

We apply alternation bounds to every computation path:

**Definition 17.2:** A  $\Sigma_i$  Alternating Turing Machine is an ATM for which every computation path on every input is of type  $\Sigma_j$  for some  $j \leq i$ .  
A  $\Pi_i$  Alternating Turing Machine is an ATM for which every computation path on every input is of type  $\Pi_j$  for some  $j \leq i$ .

Note that it's always ok to use fewer alternations (" $j \leq i$ ") but computation has to start with the right kind of quantifier ( $\exists$  for  $\Sigma_i$  and  $\forall$  for  $\Pi_i$ ).

**Example 17.3:** A  $\Sigma_1$  ATM is simply an NTM.

## Basic Observations

**Theorem 17.5:**  $\Sigma_1\text{P} = \text{NP}$  and  $\Pi_1\text{P} = \text{coNP}$ .

**Proof:** Immediate from the definitions.  $\square$

**Theorem 17.6:**  $\text{co}\Sigma_i\text{P} = \Pi_i\text{P}$  and  $\text{co}\Pi_i\text{P} = \Sigma_i\text{P}$ .

**Proof:** We observed previously that ATMs can be complemented by simply exchanging their universal and existential states. This does not affect the amount of time or space needed.  $\square$

## Example

### MINFORMULA

Input: A propositional formula  $\varphi$ .  
Problem: Is  $\varphi$  the shortest formula that is satisfied by the same assignments as  $\varphi$ ?

One can show that **MINFORMULA** is  $\Pi_2$ P-complete. Inclusion is easy:

```
01 MINFORMULA(formula  $\varphi$ ) :  
02   universally choose  $\psi :=$  formula shorter than  $\varphi$   
03   existentially guess  $\mathcal{I} :=$  assignment for variables in  $\varphi$   
04   if  $\varphi^{\mathcal{I}} = \psi^{\mathcal{I}}$  :  
05     return false  
06   else :  
07     return true
```

## The Polynomial Hierarchy

Like for NP and coNP, we do not know if  $\Sigma_i$ P equals  $\Pi_i$ P or not.

What we do know, however, is this:

### Theorem 17.7:

- $\Sigma_i$ P  $\subseteq$   $\Sigma_{i+1}$ P and  $\Sigma_i$ P  $\subseteq$   $\Pi_{i+1}$ P
- $\Pi_i$ P  $\subseteq$   $\Pi_{i+1}$ P and  $\Pi_i$ P  $\subseteq$   $\Sigma_{i+1}$ P

**Proof:** Immediate from the definitions. □

Thus, the classes  $\Sigma_i$ P and  $\Pi_i$ P form a kind of hierarchy: the **Polynomial (Time) Hierarchy**. Its entirety is denoted PH:

$$\text{PH} := \bigcup_{i \geq 1} \Sigma_i \text{P} = \bigcup_{i \geq 1} \Pi_i \text{P}$$

## Problems in the Polynomial Hierarchy

The “typical” problems in the Polynomial Hierarchy are restricted forms of **TRUE QBF**:

### TRUE $\Sigma_k$ QBF

Input: A quantified Boolean formula  $\varphi$  with at most  $k$  quantifier alternations of the form  $\exists X_1^1, X_2^1, \dots \forall X_1^2, X_2^2, \dots \mathcal{Q}_k X_1^k, X_2^k, \dots \psi$ .  
Problem: Is  $\varphi$  true?

**TRUE  $\Pi_k$ QBF** is defined analogously, using formulae with  $k$  quantifier alternations that start with  $\forall$  rather than  $\exists$ .

**Theorem 17.8:** For every  $k$ , True  $\Sigma_k$ QBF is  $\Sigma_k$ P-complete and True  $\Pi_k$ QBF is  $\Pi_k$ P-complete.

**Note:** It is not known if there is any PH-complete problem.

## Alternative Views on the Polynomial Hierarchy

## Certificates

For NP, we gave an alternative definition based on **polynomial-time verifiers** that use a given polynomial certificate (witness) to check acceptance. Can we extend this idea to alternation-bounded ATMs?

**Notation:** Given an input word  $w$  and a polynomial  $p$ , we write  $\exists^p c$  as abbreviation for “there is a word  $c$  of length  $|c| \leq p(|w|)$ .” Similarly for  $\forall^p c$ .

We can rephrase our earlier characterisation of polynomial-time verifiers:

$\mathbf{L} \in \text{NP}$  iff there is a polynomial  $p$  and language  $\mathbf{V} \in \text{P}$  such that

$$\mathbf{L} = \{w \mid \exists^p c \text{ such that } (w\#c) \in \mathbf{V}\}$$

## Oracles (Revision)

Recall how we defined oracle TMs:

**Definition 3.15:** An **Oracle Turing Machine** (OTM) is a Turing machine  $\mathcal{M}$  with a special tape, called the oracle tape, and distinguished states  $q_?$ ,  $q_{\text{yes}}$ , and  $q_{\text{no}}$ . For a language  $\mathbf{O}$ , the **oracle machine**  $\mathcal{M}^{\mathbf{O}}$  can, in addition to the normal TM operations, do the following:

Whenever  $\mathcal{M}^{\mathbf{O}}$  reaches  $q_?$ , its next state is  $q_{\text{yes}}$  if the content of the oracle tape is in  $\mathbf{O}$ , and  $q_{\text{no}}$  otherwise.

Let  $\mathbf{C}$  be a complexity class:

- For a language  $\mathbf{O}$ , we write  $\mathbf{C}^{\mathbf{O}}$  for the class of all problems that can be solved by a C-TM with oracle  $\mathbf{O}$ .
- For a complexity class  $\mathbf{O}$ , we write  $\mathbf{C}^{\mathbf{O}}$  for the class of all problems that can be solved by a C-TM with an oracle from class  $\mathbf{O}$ .

Note: this notation will only be used for complexity classes  $\mathbf{C}$  where it is clear what a “C-TM with an oracle” is.

## Certificates for bounded ATMs

**Theorem 17.9:**  $\mathbf{L} \in \Sigma_k^{\text{P}}$  iff there is a polynomial  $p$  and language  $\mathbf{V} \in \text{P}$  such that

$$\mathbf{L} = \{w \mid \exists^p c_1 \cdot \forall^p c_2 \dots \mathcal{Q}_k^p c_k \text{ such that } (w\#c_1\#c_2\#\dots\#c_k) \in \mathbf{V}\}$$

where  $\mathcal{Q}_k = \exists$  if  $k$  is odd, and  $\mathcal{Q}_k = \forall$  if  $k$  is even.

An analogous result holds for  $\mathbf{L} \in \Pi_k^{\text{P}}$ .

**Proof sketch:**

$\Rightarrow$ : Similar as for NP. Use  $c_i$  to encode the non-deterministic choices of the ATM. With all choices given, the acceptance on the specified path can be checked in polynomial time.

$\Leftarrow$ : Use an ATM to implement the certificate-based definition of  $\mathbf{L}$ , by using universal and existential choices to guess the certificate before running a polynomial time verifier.  $\square$

## The Polynomial Hierarchy – Alternative Definition

We recursively define the following complexity classes:

**Definition 17.10:**

- $\Sigma_0^{\text{P}} := \text{P}$  and  $\Sigma_{k+1}^{\text{P}} := \text{NP}^{\Sigma_k^{\text{P}}}$
- $\Pi_0^{\text{P}} := \text{P}$  and  $\Pi_{k+1}^{\text{P}} := \text{coNP}^{\Pi_k^{\text{P}}}$

**Remark:**

Complementing an oracle (language/class) does not change expressivity: we can just swap states  $q_{\text{yes}}$  and  $q_{\text{no}}$ . Therefore  $\Sigma_{k+1}^{\text{P}} = \text{NP}^{\Pi_k^{\text{P}}}$  and  $\Pi_{k+1}^{\text{P}} := \text{coNP}^{\Sigma_k^{\text{P}}}$ .

Hence, we can also see that  $\Sigma_k^{\text{P}} = \text{co}\Pi_k^{\text{P}}$ .

**Question:**

How do these relate to our earlier definitions of the PH classes?

## Oracle TMs vs. ATMs

It turns out that this new definition leads to a familiar class of problems:<sup>1</sup>

**Theorem 17.11:** For all  $k \geq 1$ , we have  $\Sigma_k^P = \Sigma_k P$  and  $\Pi_k^P = \Pi_k P$ .

**Proof:** We only prove the case  $\Sigma_k^P = \Sigma_k P$  – the other follows by complementation. The proof is by induction on  $k$ .

**Base case:**  $k = 1$ .

The claim follows since  $\Sigma_1^P = NP^P = NP$  and  $\Sigma_1 P = NP$  (as noted before).

<sup>1</sup>Because of this result, both of our notations are used interchangeably in the literature, independently of the definition used.

## Oracle TMs vs. ATMs (2)

**Induction step:** assume the claim holds for  $k$ . We show  $\Sigma_{k+1}^P = \Sigma_{k+1} P$ .

“ $\supseteq$ ” Assume  $L \in \Sigma_{k+1} P$ .

- By Theorem 17.9, for some language  $V \in P$  and polynomial  $p$ :  
 $L = \{w \mid \exists^p c_1. \forall^p c_2 \dots \mathcal{O}_{k+1}^p c_{k+1} \text{ such that } (w\#c_1\#c_2\#\dots\#c_{k+1}) \in V\}$
- By Theorem 17.9, the following defines a language in  $\Pi_k P$ :  
 $L' := \{(w\#c_1) \mid \forall^p c_2 \dots \mathcal{O}_k^p c_{k+1} \text{ such that } (w\#c_1\#c_2\#\dots\#c_{k+1}) \in V\}$ .
- The following algorithm in  $NP^{L'}$  decides  $L$ :  
on input  $w$ , non-deterministically guess  $c_1$ ;  
then check  $(w\#c_1) \in L'$  using the  $L'$  oracle
- By induction,  $L' \in \Pi_k^P$ . Hence, the algorithm runs in  $NP^{\Pi_k^P} = NP^{\Sigma_k^P} = \Sigma_{k+1}^P$

## Oracle TMs vs. ATMs (3)

**Induction step:** assume the claim holds for  $k$ . We show  $\Sigma_{k+1}^P = \Sigma_{k+1} P$ .

“ $\subseteq$ ” Assume  $L \in \Sigma_{k+1}^P$ .

- There is an  $\Sigma_{k+1}^P$ -TM  $\mathcal{M}$  that accepts  $L$ , using an oracle  $O \in \Sigma_k^P$ .
  - By induction,  $O \in \Sigma_k P$  and thus  $\bar{O} \in \Pi_k P$  for its complement
  - For an  $\Sigma_{k+1} P$  algorithm, first guess (and verify) an accepting path of  $\mathcal{M}$  including results of all oracle queries.
  - Then universally branch to verify all guessed oracle queries:
    - For queries  $w \in O$  with guessed answer “no”, use  $\Pi_k P$  check for  $w \in \bar{O}$
    - For queries  $w \in O$  with guessed answer “yes”, use  $\Pi_{k-1} P$  check for  $(w\#c_1) \in O'$ , where  $O'$  is constructed as in the  $\supseteq$ -case, and  $c_1$  is guessed in the first  $\exists$ -phase
- 

## Summary and Outlook

The **Polynomial Hierarchy** is a hierarchy of complexity classes between  $P$  and  $PSPACE$

It can be defined by stacking **NP-oracles** on top of  $P/NP/coNP$ , or, equivalently, by **bounding alternation** in polytime ATMs

The typical complete problems for the classes in the polynomial hierarchy are QBF with bounded forms of quantifier alternation

### What's next?

- Some more about the polynomial hierarchy
- End-of-year consultation
- Computing with circuits