Review: ATM vs. DTM
ATM vs. DTM

We have observed four major relationships between alternating and deterministic complexity classes.

- $\text{ApTime} \subseteq \text{Pspace}$

- $\text{ApTime} \supseteq \text{Pspace}$
  - 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.
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.
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.
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.
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.
Let $h : \mathbb{N} \to \mathbb{R}$ be a space-constructible function in $O(g)$ that defines the exact time bound for $M$ (no $O$-notation).

01 \texttt{AtmSimulateTm(TM } M, \text{ input word } w, \text{ time bound } h) :$
02 \quad \text{existentially guess } s \leq h(|w|) \quad \text{// halting step}
03 \quad \text{existentially guess } i \in \{0, \ldots, s\} \quad \text{// halting position}
04 \quad \text{existentially guess } \omega \in Q \times \Gamma \quad \text{// halting cell + state}
05 \quad \text{if } M \text{ would not halt in } \omega :$
06 \quad \quad \text{return false}
07 \quad \text{for } j = s, \ldots, 1 \text{ do :}$
08 \quad \quad \quad \text{existentially guess } \langle \omega_{-1}, \omega_0, \omega_1 \rangle \in \Omega^3
09 \quad \quad \quad \text{if } M(\omega_{-1}, \omega_0, \omega_{+1}) \neq \omega :$
10 \quad \quad \quad \quad \text{return false}
11 \quad \quad \text{universally choose } \ell \in \{-1, 0, 1\}
12 \quad \quad \omega := \omega_\ell
13 \quad \quad i := i + \ell
14 \quad \quad \text{// after tracing back } s \text{ steps, check input configuration :}
15 \quad \quad \text{return “input configuration of } M \text{ on } w \text{ has } \omega \text{ 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”)

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 (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?
A Remark on (Non)determinism

For each cell that is to be verified:

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

\(\leadsto\) 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

\(\leadsto\) Independent guesses, if correct, must generally be the same
A Remark on Space-Constructibility

Our algorithm needs space-constructibility of $h$ 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 $f$. 
A Remark on Space-Constructibility

Our algorithm needs space-constructibility of \( h \) to implement the line

\[
\text{02 existentially guess } s \leq h(|w|) \quad \text{// halting step}
\]

However, we could also avoid this:

- The algorithm from line \( \text{03} \) 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 \( f \).
We can sum up our findings as follows:

\[
\begin{align*}
L & \subseteq \text{PTime} & \subseteq \text{PSpace} & \subseteq \text{ExpTime} & \subseteq \text{ExpSpace} \\
\text{ALogSpace} & \subseteq \text{APT} & \subseteq \text{APSpace} & \subseteq \text{AExpTime}
\end{align*}
\]
The Polynomial Hierarchy
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 $P$ be a computation path of an ATM on some input.

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

\[
\begin{align*}
\Sigma_i P &= \bigcup_{d \geq 1} \Sigma_i \text{Time}(n^d) \\
\Pi_i P &= \bigcup_{d \geq 1} \Pi_i \text{Time}(n^d)
\end{align*}
\]

Hardness for these classes is defined by polynomial many-one reductions as usual.
Theorem 17.5: $\Sigma_1 P = NP$ and $\Pi_1 P = coNP$.

**Proof:** Immediate from the definitions. □
**Theorem 17.5:** $\Sigma_1 P = \mathbf{NP}$ and $\Pi_1 P = \mathbf{coNP}$.

**Proof:** Immediate from the definitions.

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

**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.
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:

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

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

$$\exists X_1^1, X_2^1, \ldots \forall X_1^2, X_2^2, \ldots \exists X_1^k, X_2^k, \ldots .\psi.$$

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 $\Sigma_k \mathbb{P}$-complete and True $\Pi_k$QBF is $\Pi_k \mathbb{P}$-complete.

**Note:** It is not known if there is any PH-complete problem.
Alternative Views on the Polynomial Hierarchy
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?
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:

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

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

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

$$L = \{w \mid \exists^{p} c_1. \forall^{p} c_2 \ldots \Omega_k^{p} c_k \text{ such that } (w\#c_1\#c_2\ldots\#c_k) \in V\}$$

where $\Omega_k = \exists$ if $k$ is odd, and $\Omega_k = \forall$ if $k$ is even.

An analogous result holds for $L \in \Pi_k P$.

**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 $L$, by using universal and existential choices to guess the certificate before running a polynomial time verifier. □
Recall how we defined oracle TMs:

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

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

Let $C$ be a complexity class:

- For a language $O$, we write $C^O$ for the class of all problems that can be solved by a $C$-TM with oracle $O$.

- For a complexity class $O$, we write $C^O$ for the class of all problems that can be solved by a $C$-TM with an oracle from class $O$. 
We recursively define the following complexity classes:

**Definition 17.10:**

- $\Sigma^P_0 := P$ and $\Sigma^P_{k+1} := NP^{\Sigma^P_k}$
- $\Pi^P_0 := P$ and $\Pi^P_{k+1} := coNP^{\Pi^P_k}$
The Polynomial Hierarchy – Alternative Definition

We recursively define the following complexity classes:

**Definition 17.10:**

- \( \Sigma^P_0 := \text{P} \) and \( \Sigma^P_{k+1} := \text{NP}^{\Sigma^P_k} \)
- \( \Pi^P_0 := \text{P} \) and \( \Pi^P_{k+1} := \text{coNP}^{\Pi^P_k} \)

**Remark:**

Complementing an oracle (language/class) does not change expressivity: we can just swap states \( q_{yes} \) and \( q_{no} \). Therefore \( \Sigma^P_{k+1} = \text{NP}^{\Pi^P_k} \) and \( \Pi^P_{k+1} := \text{coNP}^{\Sigma^P_k} \).

Hence, we can also see that \( \Sigma^P_k = \text{co}\Pi^P_k \).
We recursively define the following complexity classes:

**Definition 17.10:**
- $\Sigma^P_0 := P$ and $\Sigma^P_{k+1} := \text{NP}^{\Sigma^P_k}$
- $\Pi^P_0 := P$ and $\Pi^P_{k+1} := \text{coNP}^{\Pi^P_k}$

**Remark:**
Complementing an oracle (language/class) does not change expressivity: we can just swap states $q_{\text{yes}}$ and $q_{\text{no}}$. Therefore $\Sigma^P_{k+1} = \text{NP}^{\Pi^P_k}$ and $\Pi^P_{k+1} := \text{coNP}^{\Sigma^P_k}$.

Hence, we can also see that $\Sigma^P_k = \text{coNP}_k$.

**Question:**
How do these relate to our earlier definitions of the PH classes?
It turns out that this new definition leads to a familiar class of problems:\(^1\)

**Theorem 17.11:** For \( k \geq 1 \), 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 \( \Sigma_1^P = \text{NP}^P = \text{NP} \) and \( \Sigma_1 P = \text{NP} \) (as noted before).

---

\(^1\)Because of this result, both of our notations are used interchangeably in the literature, independently of the definition used.
**Induction step:** assume the claim holds for $k$. We show $\Sigma^P_{k+1} = \Sigma_{k+1}^P$.

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

- By Theorem 17.9, for some language $V \in \mathsf{P}$ and polynomial $p$:
  $$L = \{w \mid \exists^p c_1. \forall^p c_2 \ldots Q^p_{k+1} c_{k+1} \text{ such that } (w\#c_1\#c_2\ldots\#c_{k+1}) \in V\}$$

- By Theorem 17.9, the following defines a language in $\Pi^P_k$:
  $$L' := \{(w\#c_1) \mid \forall^p c_2 \ldots Q^p_{k} c_{k+1} \text{ such that } (w\#c_1\#c_2\ldots\#c_{k+1}) \in V\}.$$  

- The following algorithm in $\mathsf{NP}^{L'}$ decides $L$:
  on input $w$, non-deterministically guess $c_1$;
  then check $(w\#c_1) \in L'$ using the $L'$ oracle

- By induction, $L' \in \Pi^P_k$. Hence, the algorithm runs in $\mathsf{NP}^{\Pi^P_k} = \mathsf{NP}^{\Sigma^P_k} = \Sigma^P_{k+1}$
**Induction step:** assume the claim holds for $k$. We show $\Sigma^P_{k+1} = \Sigma_{k+1}^P$.

“$\subseteq$” Assume $L \in \Sigma^P_{k+1}$.

- There is an $\Sigma^P_{k+1}$-TM $M$ that accepts $L$, using an oracle $O \in \Sigma^P_k$.
- By induction, $O \in \Sigma_k^P$ and thus $\overline{O} \in \Pi_k^P$ for its complement.
- For an $\Sigma^P_{k+1}$ algorithm, first guess (and verify) an accepting path of $M$ 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 $w \in \overline{O}$.
  - 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 $\exists$-case, and $c_1$ is guessed in the first $\exists$-phase.

$\square$
More Classes in PH

We defined $\Sigma_k^P$ and $\Pi_k^P$ by relativising NP and coNP with oracles.

What happens if we start from P instead?
We defined $\Sigma_k^P$ and $\Pi_k^P$ by relativising NP and coNP with oracles.

What happens if we start from P instead?

**Definition 17.12:** $\Delta_0^P := P$ and $\Delta_{k+1}^P := P^{\Sigma_k^P}$.

Some immediate observations:

- $\Delta_1^P = P^P = P$
- $\Delta_2^P = P^{NP} = P^{coNP}$
- $\Delta_k^P \subseteq \Sigma_k^P$ (since $P \subseteq NP$) and $\Delta_k^P \subseteq \Pi_k^P$ (since $P \subseteq coNP$)
- $\Sigma_k^P \subseteq \Delta_{k+1}^P$ and $\Pi_k^P \subseteq \Delta_{k+1}^P$
Problems for $\Delta^p_k$?

$\Delta^p_k$ seems to be less common in practice, but there are some known complete problems for $P^{NP} = \Delta^p_2$:

**Uniquely Optimal TSP** [Papadimitriou, JACM 1984]

Input: Undirected graph $G$ with edge weights (distances).

Problem: Is there exactly one shortest travelling salesman tour on $G$?

**Divisible TSP** [Krentel, JCSS 1988]

Input: Undirected graph $G$ with edge weights; number $k$.

Problem: Is the shortest travelling salesman tour on $G$ divisible by $k$?

**Odd Final SAT** [Krentel, JCSS 1988]

Input: Propositional formula $\varphi$ with $n$ variables.

Problem: Is $X_n$ true in the lexicographically last assignment satisfying $\varphi$?
Is the Polynomial Hierarchy Real?

Questions:

- Are all of these classes really distinct? Nobody knows.
- Are any of these classes really distinct? Nobody knows.
- Are any of these classes distinct from $P$? Nobody knows.
- Are any of these classes distinct from $PSpace$? Nobody knows.

$\Delta^P_0 = \Sigma^P_0 = \Pi^P_0 = \Delta^P_1 = P$

$\Sigma^P_k$ and $\Pi^P_k$ are the $k$th levels of the polynomial hierarchy.

$\Sigma^P_2 = NP^{NP}$ and $\Pi^P_2 = coNP^{NP}$

$\Delta^P_2 = P^{NP}$
Is the Polynomial Hierarchy Real?

Questions:

Are all of these classes really distinct?
Questions:
Are all of these classes really distinct?
Nobody knows.
Is the Polynomial Hierarchy Real?

Questions:

Are all of these classes really distinct?
Nobody knows.

Are any of these classes really distinct?
Is the Polynomial Hierarchy Real?

Questions:

Are all of these classes really distinct? Nobody knows.

Are any of these classes really distinct? Nobody knows.
Is the Polynomial Hierarchy Real?

Questions:

Are all of these classes really distinct?  Nobody knows.

Are any of these classes really distinct?  Nobody knows.

Are any of these classes distinct from P?
Questions:

Are all of these classes really distinct? Nobody knows.

Are any of these classes really distinct? Nobody knows.

Are any of these classes distinct from P? Nobody knows.

Are any of these classes distinct from PSPACE? Nobody knows.

What do we know then?
Is the Polynomial Hierarchy Real?

Questions:

Are all of these classes really distinct?
Nobody knows.

Are any of these classes really distinct?
Nobody knows.

Are any of these classes distinct from P?
Nobody knows.

Are any of these classes distinct from PSpace?
Is the Polynomial Hierarchy Real?

Questions:

Are all of these classes really distinct? Nobody knows.

Are any of these classes really distinct? Nobody knows.

Are any of these classes distinct from P? Nobody knows.

Are any of these classes distinct from PSpace? Nobody knows.
Questions:

Are all of these classes really distinct?
Nobody knows.

Are any of these classes really distinct?
Nobody knows.

Are any of these classes distinct from P?
Nobody knows.

Are any of these classes distinct from PSpace?
Nobody knows.

What do we know then?
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.

"Most experts" think that:

- The polynomial hierarchy does not collapse completely (same as $P \neq NP$)
- The polynomial hierarchy does not collapse on any level (in particular $PH \neq PSpace$ and there is no PH-complete problem)

But there can always be surprises . . .

**What’s next?**

- Some more about the polynomial hierarchy
- End-of-year consultation
- Holidays