CMSC 28100

Introduction to Complexity Theory

Spring 2025
Instructor: William Hoza

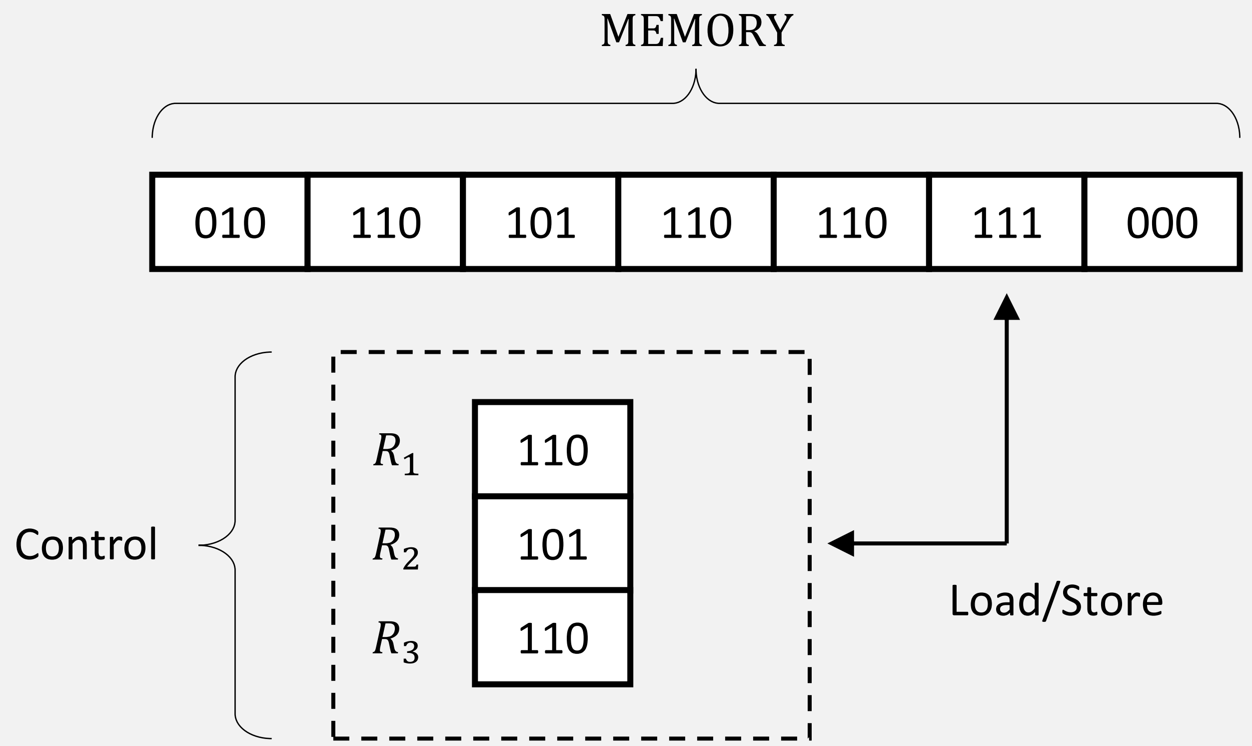
Which problems

can be solved

through computation?

Word RAM model

- Word RAM time complexity closely matches time complexity “in practice” on ordinary computers



- Some version of the word RAM model is typically assumed (implicitly or explicitly) in algorithms courses and the computing industry

Robustness of P

- Let $Y \subseteq \{0,1\}^*$

Theorem: If there is a word RAM program that decides Y in time $\mathrm{poly}(n)$,

then there is a Turing machine that decides Y in time $\mathrm{poly}(n)$.

- Proof omitted

Fine-grained vs. coarse-grained complexity

- If/when you care about the distinction between $O(n)$ time and $O(n^2)$ time, you should probably use the word RAM model
- In this course:
  - We focus on the distinction between polynomial time and exponential time
  - We can therefore continue using the Turing machine model

Which problems

can be solved

through computation?

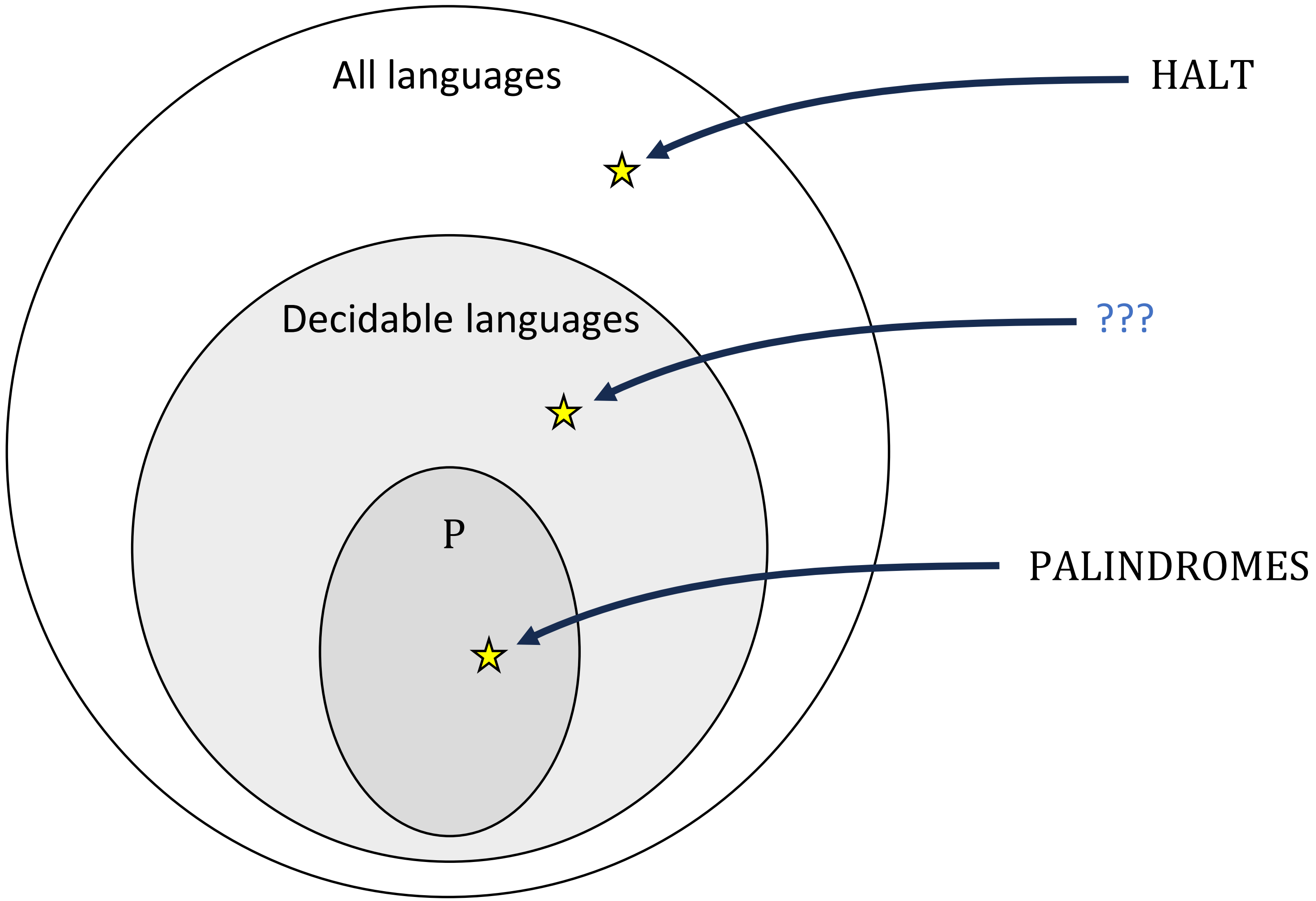
Which languages are in $\mathbf{P}$?

Which languages are not in $\mathbf{P}$?

Intractability

- How can we prove that certain languages are outside P?
- Certainly $\mathrm{HALT} \notin \mathrm{P}$
- Is every decidable language in P?
  - This would mean that every algorithm can be modified to make it run in polynomial time!

Intractability vs. undecidability



Intractability vs. undecidability

Theorem: There exists $Y \subseteq \{0,1\}^*$ such that Y is decidable, but $Y \notin \mathrm{P}$.

- **Proof**: Let $Y = \left\{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } 2^{|\langle M \rangle|} \text{ steps}\right\}$
- On the next three slides, we will show that Y is decidable and $Y \notin \mathrm{P}$

Proof that Y is decidable

$Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } 2^{|\langle M \rangle|} \text{ steps}\}$

- An algorithm that decides Y:

Given the input $\langle M \rangle$:

1. Simulate M on $\langle M \rangle$ for $2^{|\langle M \rangle|}$ steps
2. If it rejects within that time, accept
3. Otherwise, reject

Proof that $Y \notin$ P

Which of the following best describes what we've proven?

A: We showed that $T(n) > 2^n$ for a single value of n

B: We showed that $T(n) > 2^n$ for all n

C: We showed that $T(n) > 2^n$ for all sufficiently large n

D: We showed that $T(n) > 2^n$ for infinitely many n

Respond at PollEv.com/whoza or text "whoza" to 22333

- Let R be a TM that decide
- Let $T: \mathbb{N} \to \mathbb{N}$ be the time complexity of R, and let $n = |\langle R \rangle|$
- Does R accept $\langle R \rangle$? No, because that would imply $\langle R \rangle \notin Y$
- Does R reject $\langle R \rangle$ within 2^n steps? No, because that would imply $\langle R \rangle \in Y$
- Only remaining possibility: R rejects $\langle R \rangle$ after more than 2^n steps
- Therefore, $T(n) > 2^n$… but this does not imply $T(n) \neq \text{poly}(n)$ ☹️

Proof that $Y \notin \mathrm{P}$

$Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } 2^{|\langle M \rangle|} \text{ steps}\}$

- Let R be a TM that decides Y, with time complexity $T: \mathbb{N} \to \mathbb{N}$
- Add dummy states! For infinitely many values of n, there exists a TM R_n such that R_n decides Y, R_n has time complexity T, and $|\langle R_n \rangle| = n$
- Each R_n must reject $\langle R_n \rangle$ after more than 2^n steps
  - Otherwise, it would get trapped in a liar paradox
- Therefore, $T(n) > 2^n$ for infinitely many values of n, hence $T(n) \neq \mathrm{poly}(n)$

The Time Hierarchy Theorem

- Using the same proof idea, we can prove a more general theorem:

Time Hierarchy Theorem: For every* function $T: \mathbb{N} \to \mathbb{N}$ such that $T(n) \geq n$, there is a language $Y \in \mathrm{TIME}(T^4)$ such that $Y \notin \mathrm{TIME}\big(o(T)\big)$.

  - *assuming T is a "reasonable" time complexity bound. We will come back to this

- "$\mathrm{TIME}\big(o(T)\big)$" means the set of languages that are decidable in time $o(T)$
- "Given more time, we can solve more problems"

Proof of the Time Hierarchy Theorem

- Let $Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } T(|\langle M \rangle|) \text{ steps}\}$
- On the next four slides, we will prove:
  - $Y \in \mathrm{TIME}(T^4)$
  - $Y \notin \mathrm{TIME}\big(o(T)\big)$

Proof that $Y \in \mathrm{TIME}(T^4)$

$Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } T(|\langle M \rangle|) \text{ steps}\}$

- An algorithm that decides Y:

Given the input $\langle M \rangle$:

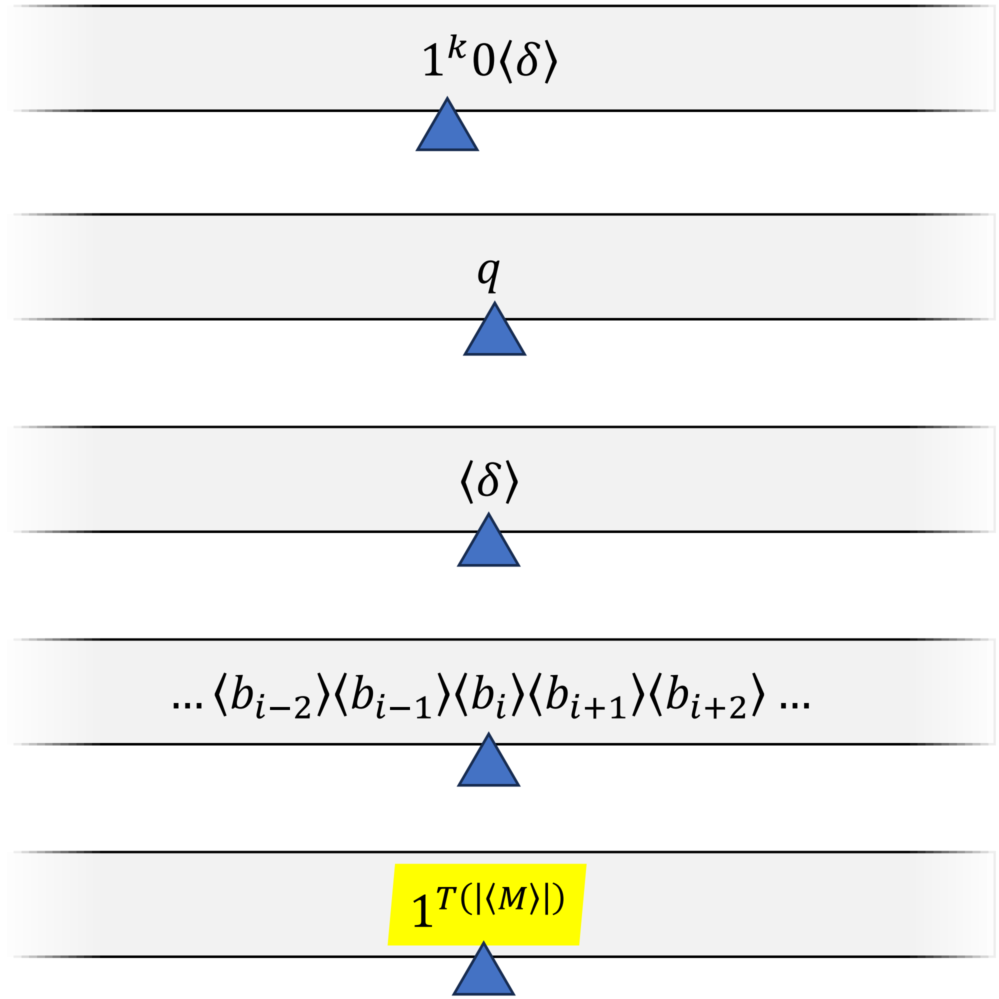
1. Simulate M on $\langle M \rangle$ for $T(|\langle M \rangle|)$ steps
2. If it rejects within that time, accept
3. Otherwise, reject

- Time complexity in the TM model?

Proof that $Y \in \mathrm{TIME}(T^4)$

$Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } T(|\langle M \rangle|) \text{ steps}\}$

- Let $n = |\langle M \rangle|$
- Each simulated step takes $O(n)$ actual steps
- Total time complexity of multi-tape machine: $O(T(n) \cdot n)$
- After converting to a one-tape machine: $O(T(n)^2 \cdot n^2) = O(T(n)^4)$



Time-constructible functions

- **Definition:** A function $T: \mathbb{N} \to \mathbb{N}$ is time-constructible if there exists a multi-tape Turing machine M such that
  - Given input 1^n, M halts with $1^{T(n)}$ written on tape 2
  - M has time complexity $O\big(T(n)\big)$
- Our proof that $Y \in \mathrm{TIME}(T^4)$ works assuming T is time-constructible
- All "reasonable" time complexity bounds (e.g., $5n$ or n^2 or 2^n) are time-constructible

Time Hierarchy Theorem

$Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } T(|\langle M \rangle|) \text{ steps}\}$

Time Hierarchy Theorem: For every time-constructible $T: \mathbb{N} \to \mathbb{N}$, there is a language $Y \in \mathrm{TIME}(T^4)$ such that $Y \notin \mathrm{TIME}\big(o(T)\big)$.

- We showed $Y \in \mathrm{TIME}(T^4)$
- We still need to show $Y \notin \mathrm{TIME}\big(o(T)\big)$

Proof that $Y \notin \mathrm{TIME}\big(o(T)\big)$

$Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } T(|\langle M \rangle|) \text{ steps}\}$

- Let R be a TM that decides Y, with time complexity $T': \mathbb{N} \to \mathbb{N}$
- Add dummy states! For infinitely many values of n, there exists a TM R_n such that R_n decides Y, R_n has time complexity T', and $|\langle R_n \rangle| = n$
- Each R_n must reject $\langle R_n \rangle$ after more than $T(n)$ steps
  - Otherwise, it would get trapped in a liar paradox
- Therefore, $T'(n) > T(n)$ for infinitely many values of n, hence T' is not $o(T)$