CMSC 28100

Introduction to Complexity Theory

Autumn 2025
Instructor: William Hoza

Which problems

can be solved

through computation?

CLASSICAL

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

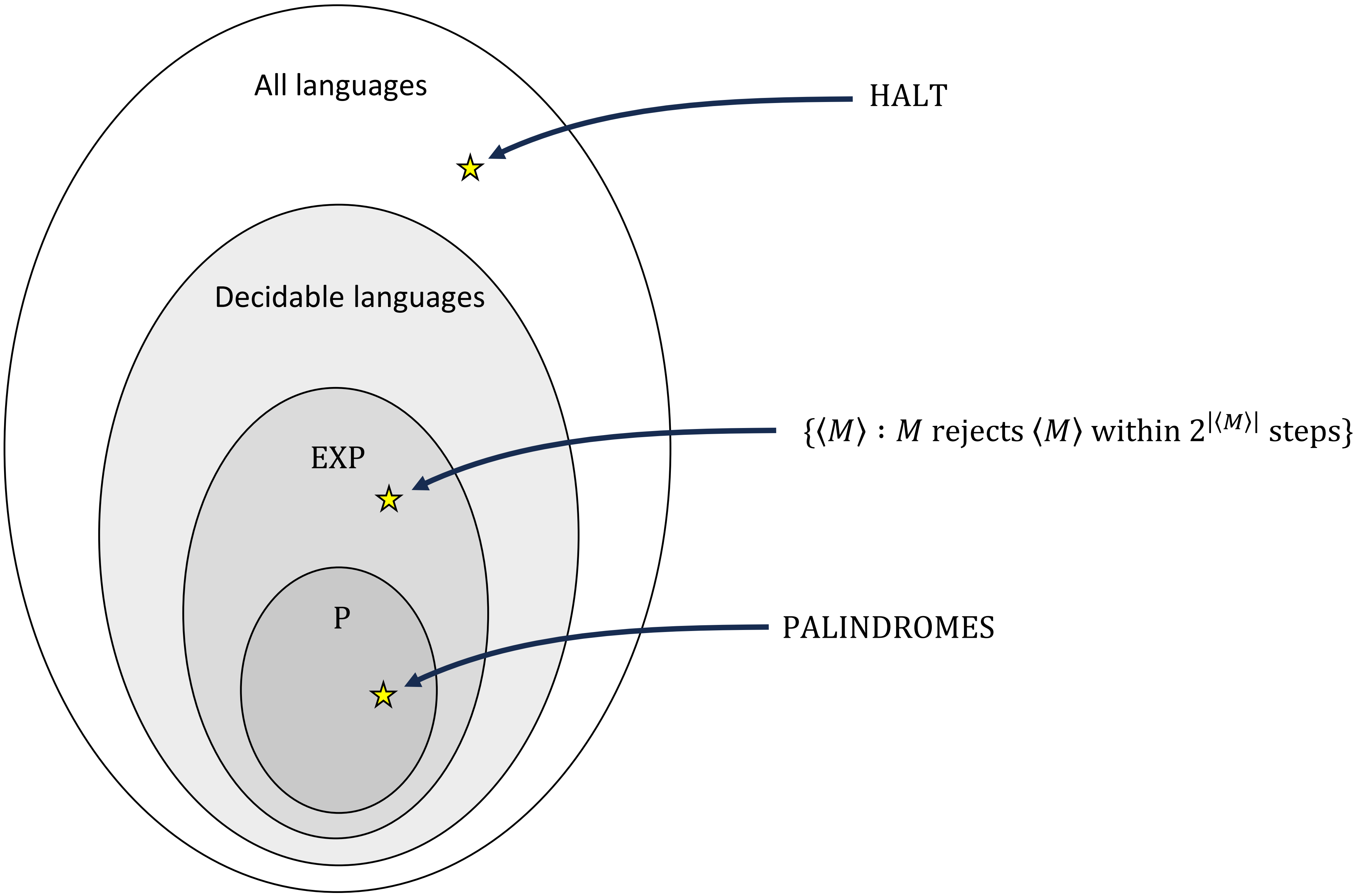
Which languages are not in $\mathbf{P}$?

Intractability vs. undecidability

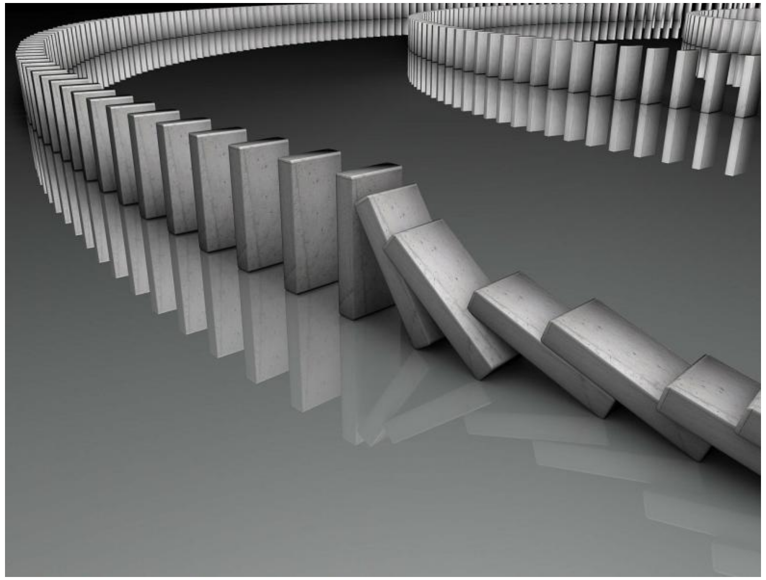
- Recall:

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

- Language: $Y = \{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } 2^{|\langle M \rangle|} \text{ steps}\}$
- Note: $Y \in \mathrm{EXP}$, so the theorem shows $\mathrm{P} \neq \mathrm{EXP}$
  - Some exponential-time algorithms cannot be converted into poly-time algorithms


All languages
HALT
Decidable languages
EXP
$\{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } 2^{|\langle M \rangle|} \text{ steps}\}$
P
PALINDROMES

Contrived vs. natural



- The language

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

is rather contrived

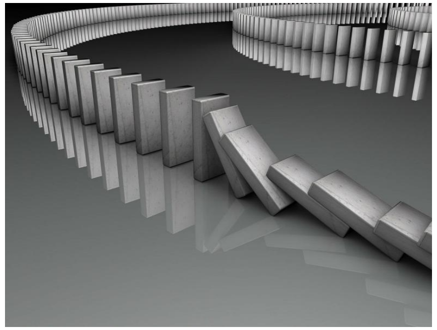
- Are there other examples of decidable languages outside P that are more interesting / natural / well-motivated?

The bounded halting problem

- Let $\text{BOUNDED-HALT} = \{\langle M, w, T \rangle : M \text{ halts on } w \text{ within } T \text{ steps}\}$
- Exercise: Can decide in time $O(|\langle M \rangle|^2 \cdot |w|^2 \cdot T^2)$
  - Pseudo-polynomial time
  - The input size is $n = |\langle M, w, T \rangle| \approx |\langle M \rangle| + |\langle w \rangle| + \log T$
- $\text{BOUNDED-HALT} \in \text{TIME}(n^4 \cdot 2^{2n}) \subseteq \text{EXP}$

Polynomial time?

The bounded halting problem



- $\text{BOUNDED-HALT} = \{\langle M, w, T \rangle : M \text{ halts on } w \text{ within } T \text{ steps}\}$

Theorem: $\text{BOUNDED-HALT} \notin \text{P}$

- Proof strategy: We'll show that if BOUNDED-HALT were in P, then it would follow that $\text{P} = \text{EXP}$

Proof that $\mathrm{BOUNDED\text{-}HALT} \notin \mathrm{P}$

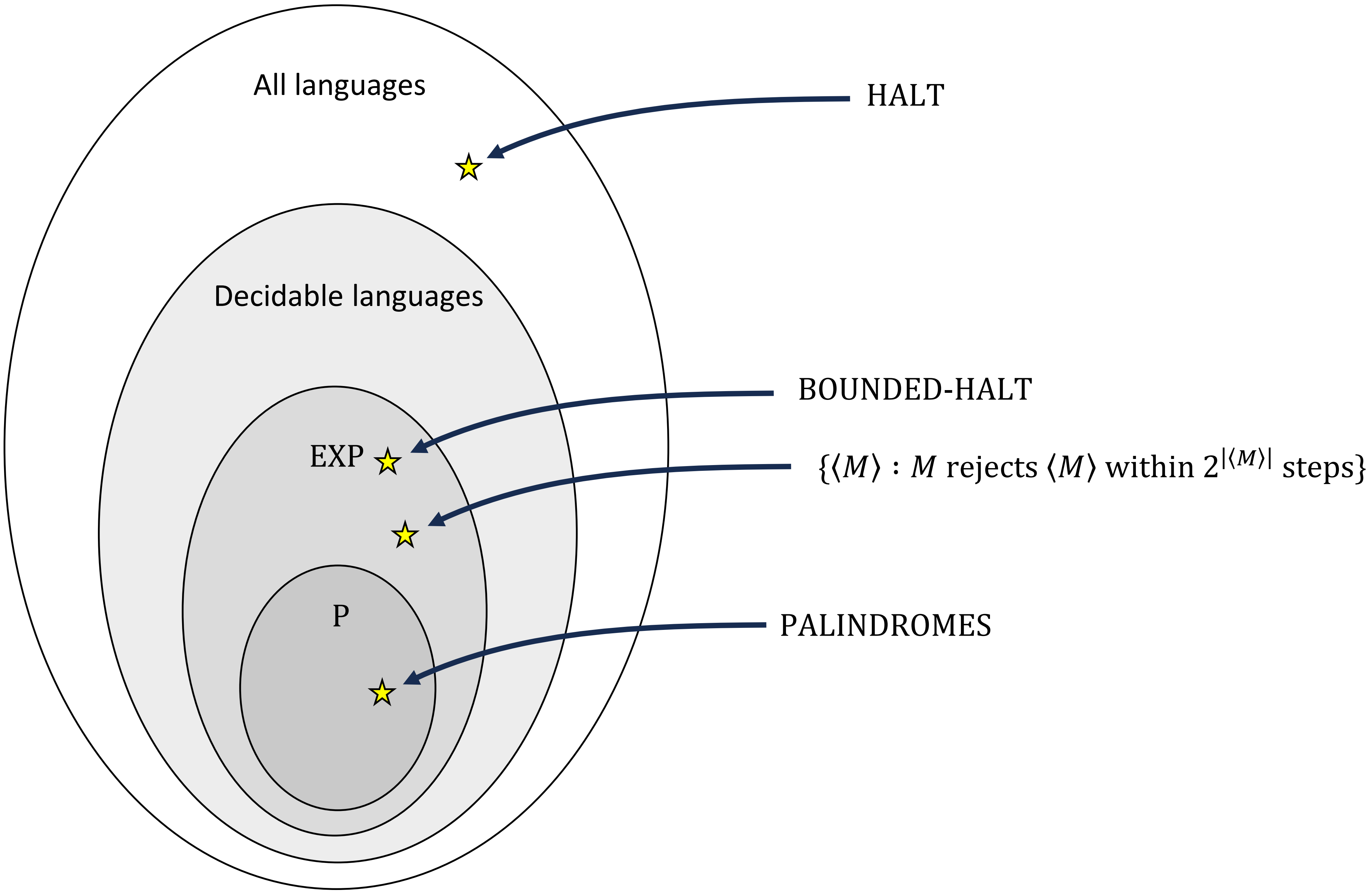
- Assume B is a poly-time TM deciding $\mathrm{BOUNDED\text{-}HALT}$
- Let $Y \in \mathrm{EXP}$. There is a TM M that $\begin{cases} \text{accepts } w \text{ within } 2^{|w|^k} \text{ steps} & \text{if } w \in Y \\ \text{loops} & \text{if } w \notin Y \end{cases}$
- We will construct a poly-time TM R that decides Y

R:

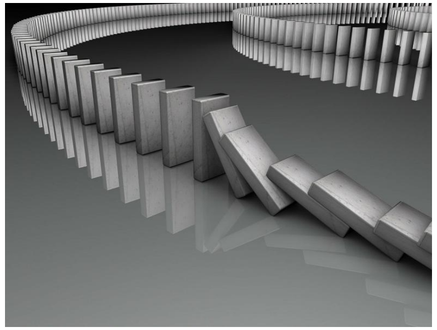
Given $w \in \{0,1\}^*$:

1. Simulate B on $\left\langle M, w, 2^{|w|^k} \right\rangle$
2. If B accepts, accept. If B rejects, reject.

- Polynomial time
- If $w \in Y$, then M accepts w within $2^{|w|^k}$ steps, so R accepts w
- If $w \notin Y$, then M loops on w, so R rejects w


All languages
Decidable languages
EXP
P
HALT
BOUNDED-HALT
$\{\langle M \rangle : M \text{ rejects } \langle M \rangle \text{ within } 2^{|\langle M \rangle|} \text{ steps}\}$
PALINDROMES

What about CLIQUE?



- $\mathrm{CLIQUE} = \{\langle G, k\rangle : G \text{ has a } k\text{-clique}\}$
- It seems likely that $\mathrm{CLIQUE} \notin \mathrm{P}$
- Can we prove it by doing a reduction from $\mathrm{BOUNDED\text{-}HALT}$?
- Answer: Probably not!
- To understand why, we need to go beyond “in P or not in P”

Beyond "it's not in P"

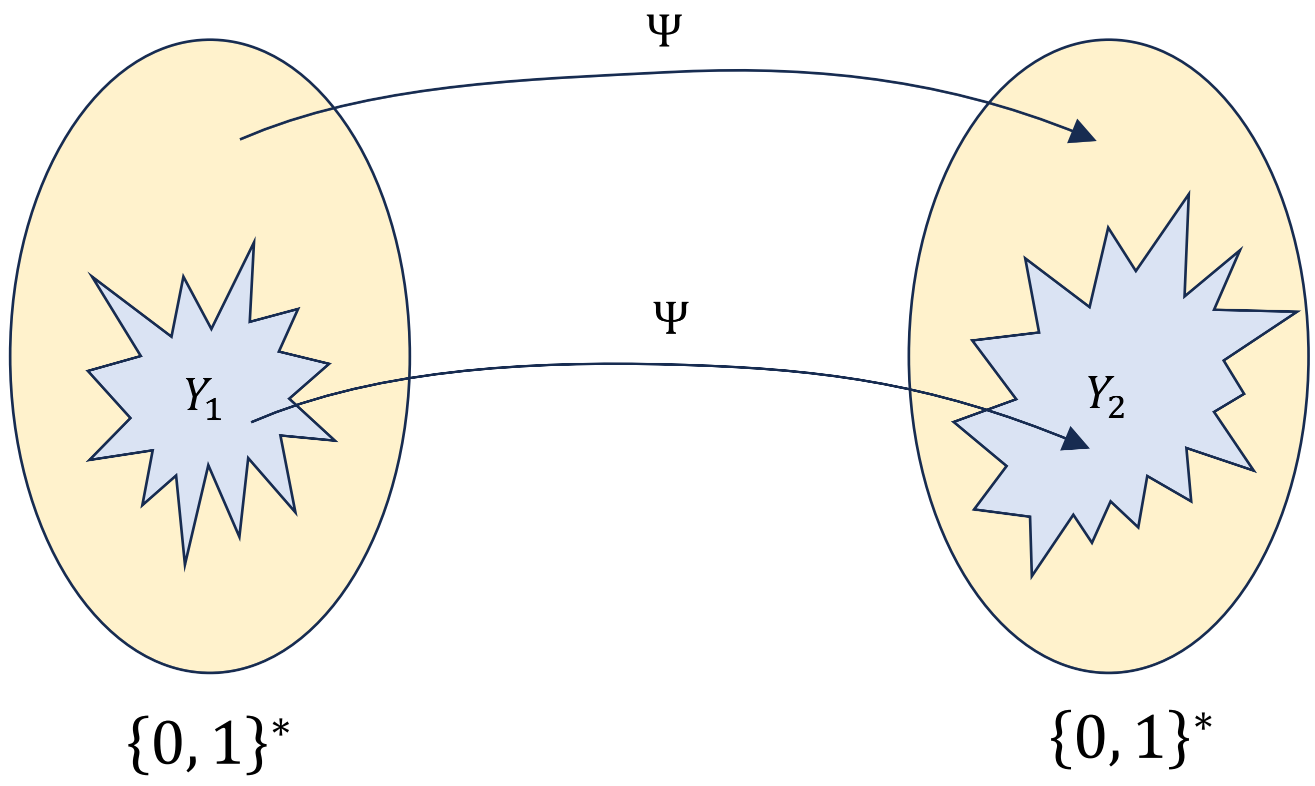
- We proved $\mathrm{BOUNDED\text{-}HALT} \notin \mathrm{P}$
- Insight: The proof gives us bonus information
  - "How far outside P is it?"
  - "Why is it outside P? What kind of hardness does it have?"
- The proof shows that every language in EXP reduces to $\mathrm{BOUNDED\text{-}HALT}$
- Furthermore, the reduction has a very specific structure

Mapping reductions

- Let $Y_1, Y_2 \subseteq \{0,1\}^*$
- **Definition:** We say Y_1 is poly-time mapping reducible to Y_2 if there exists $\Psi: \{0,1\}^* \to \{0,1\}^*$ and a poly-time TM M_Ψ such that for every $w \in \{0,1\}^*$:
  - If $w \in Y_1$, then $\Psi(w) \in Y_2$ — "YES maps to YES"
  - If $w \notin Y_1$, then $\Psi(w) \notin Y_2$ — "NO maps to NO"
  - M_Ψ halts on w with $\Psi(w)$ written on its tape — "Poly-time computable"
- Notation: $Y_1 \leq_{\mathrm{P}} Y_2$
  - Intuition: "Complexity of Y_1" $\leq$ "Complexity of Y_2"

Mapping reductions

- $Y_1 \leq_{\mathrm{P}} Y_2$ means there is an efficient way to convert questions of the form "is $w \in Y_1$?" into questions of the form "is $w' \in Y_2$?"



Mapping reduction example

- $\text{COMPOSITES} = \{\langle K \rangle : K \text{ is a composite number}\}$
- $\text{FACTOR} = \{\langle K, M \rangle : K \text{ has a prime factor } p \leq M\}$
- **Claim:** $\text{COMPOSITES} \leq_{\text{P}} \text{FACTOR}$
- **Proof:** $\Psi(\langle K \rangle) = \langle K, K - 1 \rangle$. Poly-time computable ✔
- If K is composite, then K has a prime factor less than K ✔
- If K is not composite, then K does not have a prime factor less than K ✔

Let $n = |w|$ and $m = |w'|$. What is the relationship between n and m?

A: $m \le \text{poly}(n)$

B: $n \le \text{poly}(m)$

C: $n = m$

D: Not enough information

Respond at PollEv.com/whoza or text “whoza” to 22333

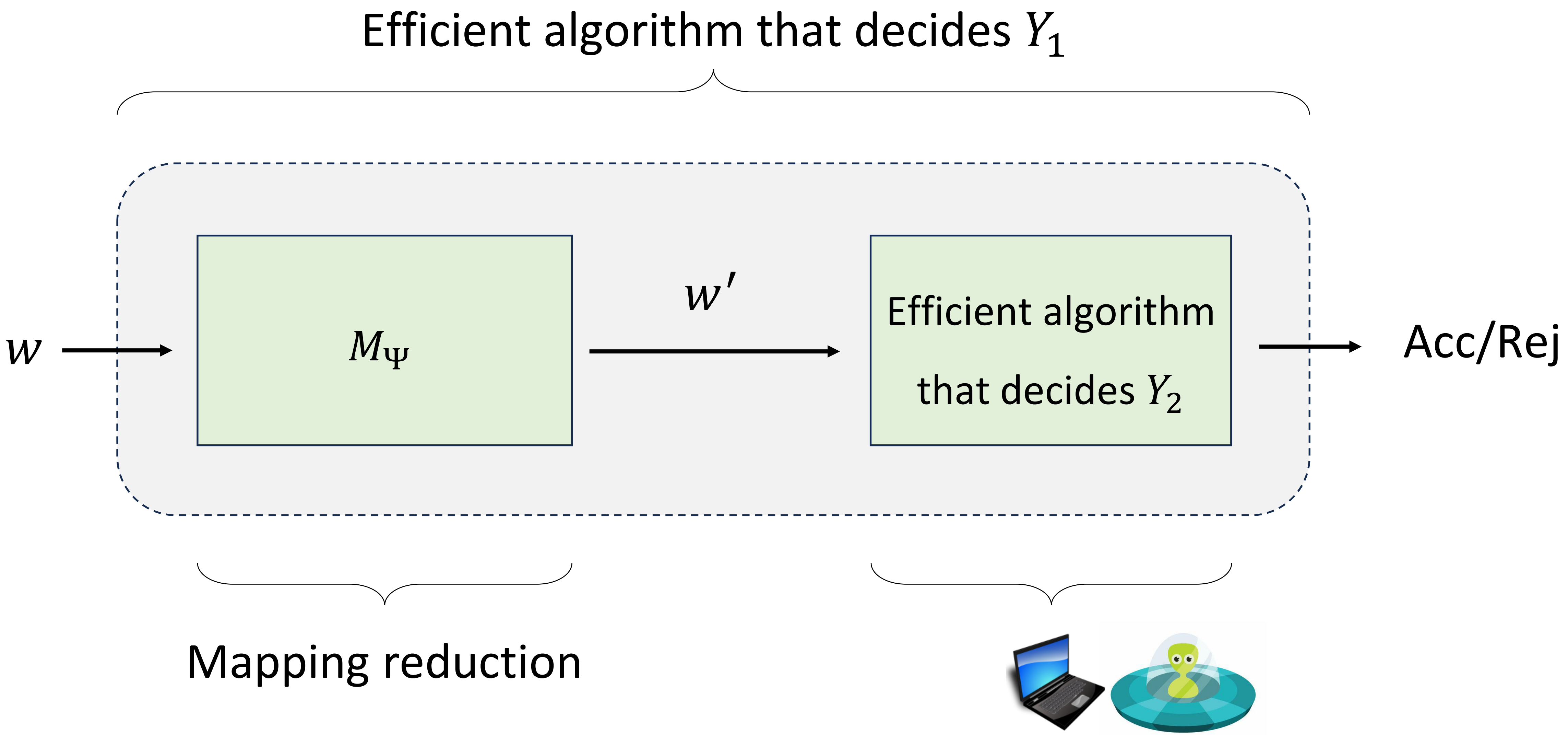
guage is in P

- **Proof:** Given $w \in \{0,1\}^*$:

1. Compute $w' = \Psi(w)$ (this takes $O(n^{k_1})$ time)
2. Check whether $w' \in Y_2$ (this takes $O(m^{k_2})$ time where $m = |w'|$)
3. If so, accept; otherwise, reject.

- $m \le O(n^{k_1})$, so the total time is $O(n^{k_1} + n^{k_1 \cdot k_2}) = \text{poly}(n)$

Reductions: Proving that a language is in P



Reductions: Proving that a language is not in P

- Let $Y_1, Y_2 \subseteq \{0,1\}^*$
- **Claim:** If $Y_1 \leq_{\mathrm{P}} Y_2$ and $Y_1 \notin \mathrm{P}$, then $Y_2 \notin \mathrm{P}$
- **Proof:** If Y_2 were in P, then Y_1 would also be in P