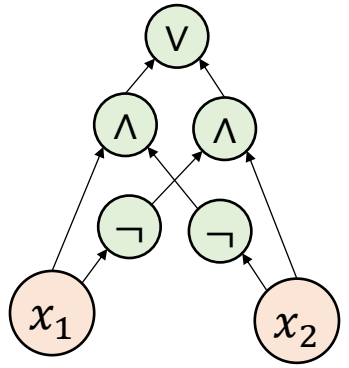
CMSC 28100

Introduction to Complexity Theory

Spring 2025
Instructor: William Hoza

Circuit satisfiability is $\mathbf{NP}$-complete



- Let $\text{CIRCUIT-SAT} = \{\langle C \rangle : C \text{ is a satisfiable circuit}\}$

Theorem: CIRCUIT-SAT is NP-complete.

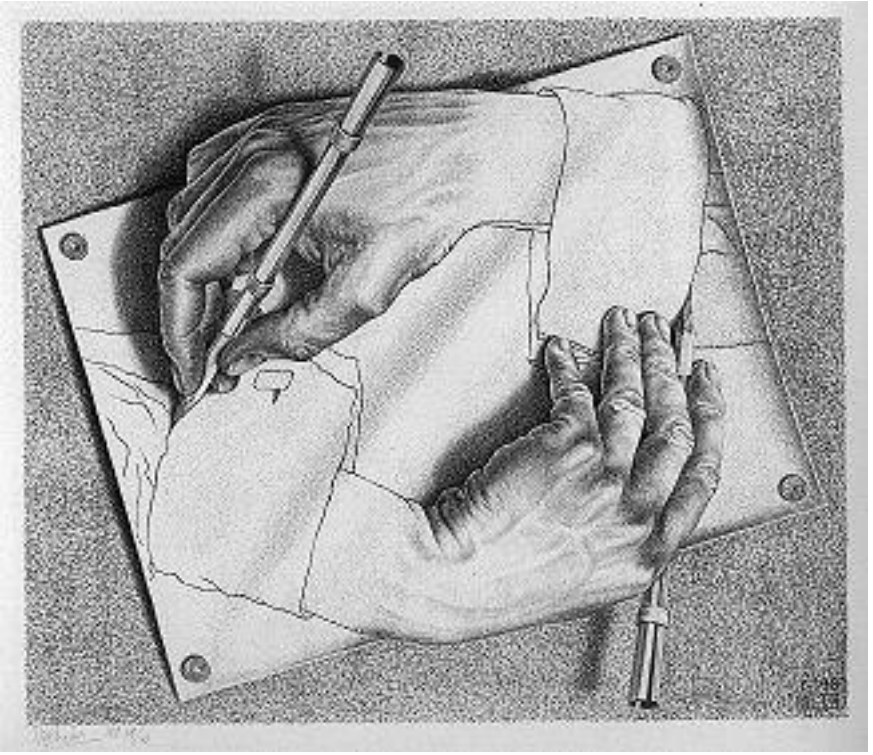
- Proof: Next 8 slides

Proof that $\mathrm{CIRCUIT\text{-}SAT} \in \mathrm{NP}$

- Given $\langle C \rangle$, where C is an n-input 1-output circuit:
  1. Pick $x \in \{0,1\}^n$ at random
  2. Check whether $C(x) = 1$ (recall $\mathrm{CIRCUIT\text{-}VALUE} \in \mathrm{P}$)
  3. Accept if $C(x) = 1$; reject if $C(x) = 0$

Code as data IV

- Let $Y \in \mathrm{NP}$
- To prove that CIRCUIT-SAT is NP-hard, we need to prove $Y \leq_{\mathrm{P}} \mathrm{CIRCUIT\text{-}SAT}$
- Given $w \in \{0,1\}^*$, we need to construct a circuit that is satisfiable if and only if $w \in Y$
- Idea: Build a "verification circuit"

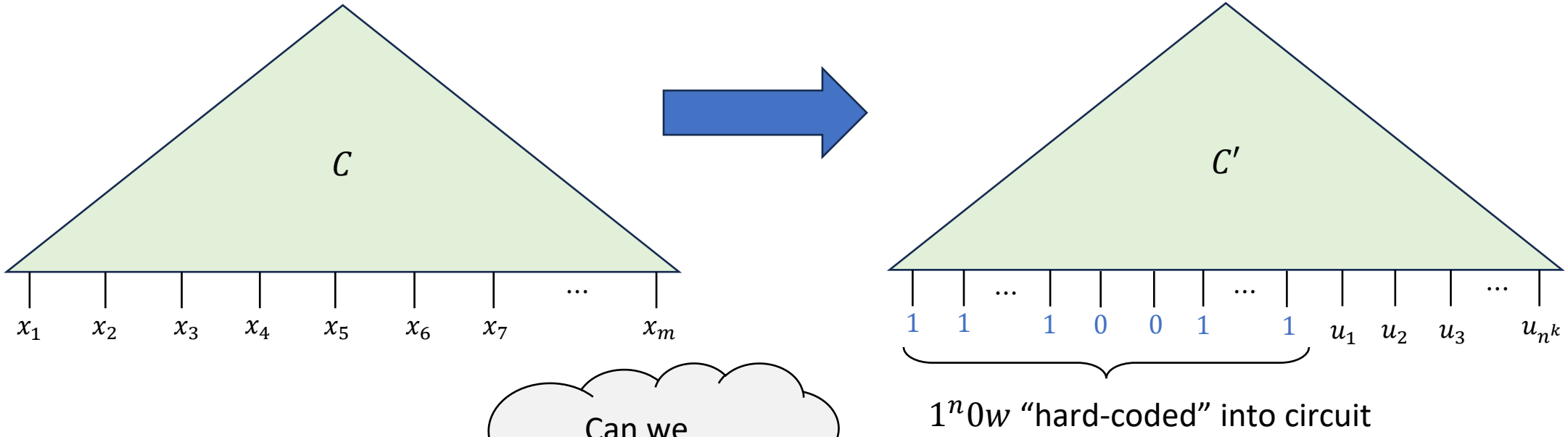


"Drawing Hands."
(1948 lithograph by M. C. Escher)

Constructing the verification circuit

- Let V be a poly-time verifier for Y, with certificates of length n^k
- Let $w \in \{0,1\}^n$
- $w \in Y$ if and only if there exists u such that $|u| \leq n^k$ and V accepts $\langle w, u \rangle$
  - Technical detail: Use the encoding $\langle w, u \rangle = 1^{|w|}0wu$
- $\mathrm{P} \subseteq \mathrm{PSIZE}$, so there is a poly-size circuit C that simulates V on inputs of length $m = 2n + 1 + n^k$

Constructing the verification circuit



Can we construct C in poly time?

- $w \in Y$ if and only if there exists u such that $C(\langle w, u \rangle) = 1$
- Reduction Ψ: Given w, produce $\langle C' \rangle$, where $C'(u) = C(\langle w, u \rangle)$

TM ⇒ Circuit

- Recall proof that

  $\mathrm{P} \subseteq \mathrm{PSIZE}$

- Insight: The proof is

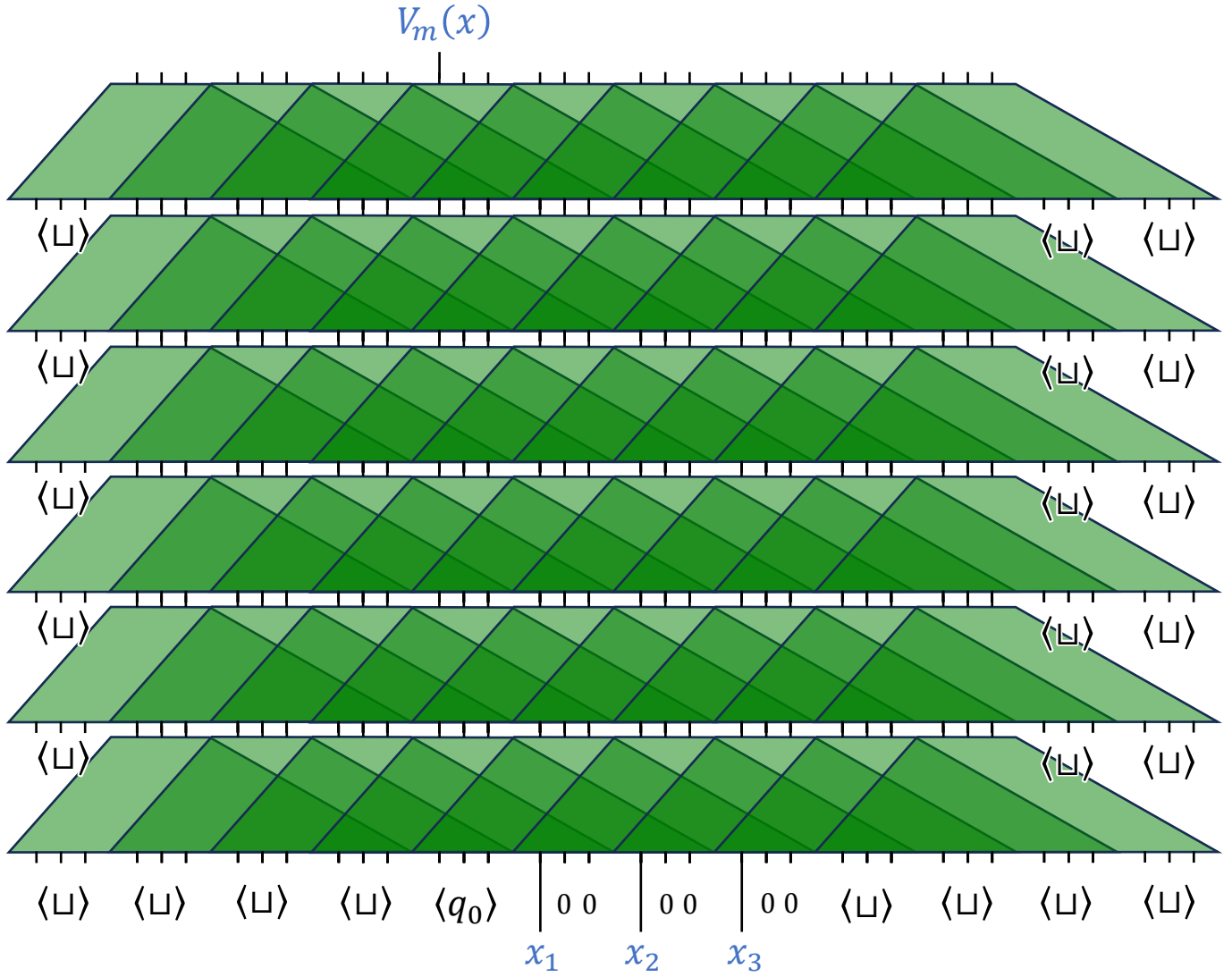
  constructive

- We can construct C in

  polynomial time

  - Copy and paste in a

    grid…



Proof that CIRCUIT-SAT is NP-hard

- Reduction Ψ: Given w, produce $\langle C' \rangle$, where $C'(\langle u \rangle) = C(\langle w, u \rangle)$ and C simulates the verifier V
- YES maps to YES:
  - If $w \in Y$, then exists a certificate $u \in \{0,1\}^{n^k}$ such that V accepts $\langle w, u \rangle$
  - Therefore, $C(\langle w, u \rangle) = 1$
  - Therefore, $C'(\langle u \rangle) = 1$, so C' is satisfiable ✔

Proof that CIRCUIT-SAT is NP-hard

- Reduction Ψ: Given w, produce $\langle C' \rangle$, where $C'(\langle u \rangle) = C(\langle w, u \rangle)$ and C simulates the verifier V
- NO maps to NO:
  - Suppose C' is satisfiable, i.e., there exists $u \in \{0,1\}^{n^k}$ such that $C'(u) = 1$
  - Then $C(\langle w, u \rangle) = 1$
  - Therefore, V accepts $\langle w, u \rangle$, so $w \in Y$ ✔

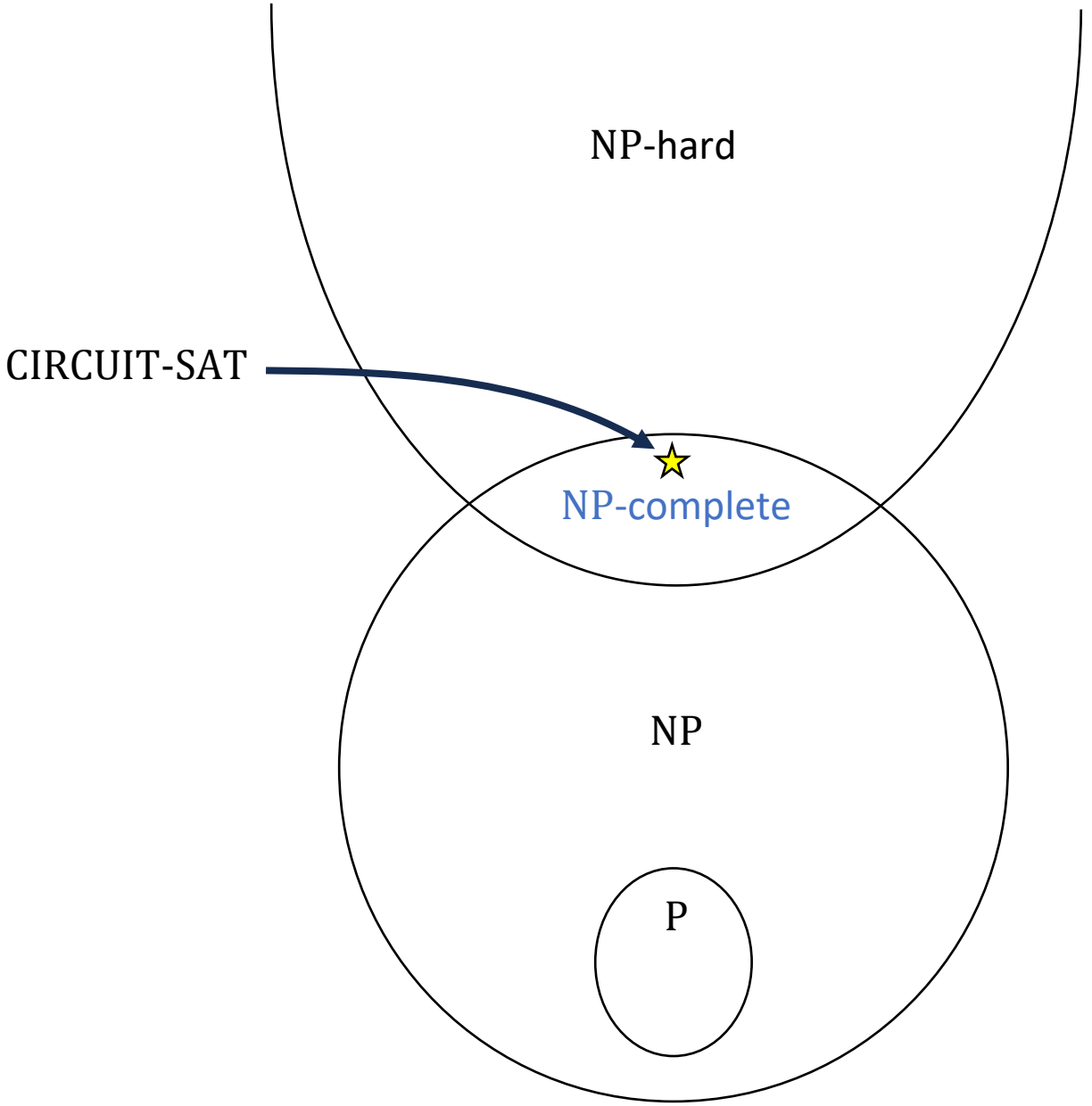
Proof that CIRCUIT-SAT is NP-hard

- Reduction Ψ: Given w, produce $\langle C' \rangle$, where $C'(\langle u \rangle) = C(\langle w, u \rangle)$ and C simulates the verifier V
- Time complexity:
  1. Compute $\langle C \rangle$ by copying and pasting in a grid
     - This takes $\text{poly}(m) = \text{poly}(n)$ time ✔
  2. Plug in $1^n 0 w$
     - This takes $\text{poly}(n)$ time ✔

Theorem: CIRCUIT-SAT is NP-complete.

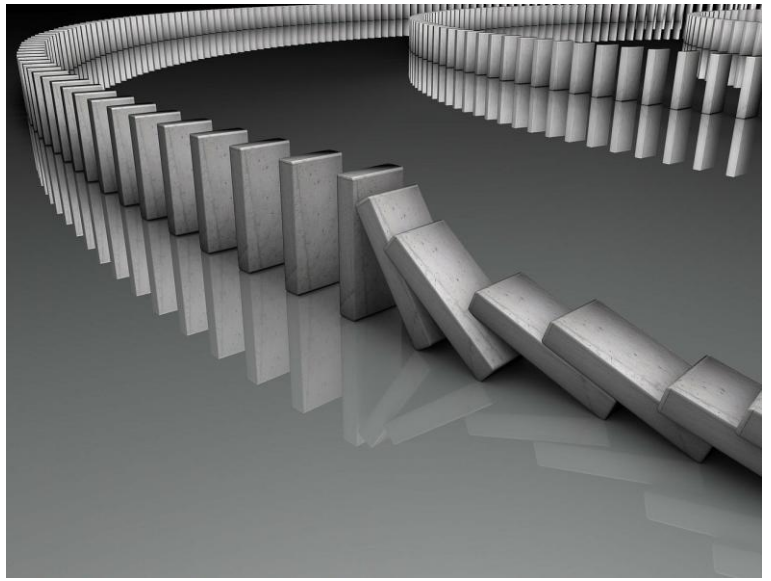
- Make sure you thoroughly understand this theorem and its proof!
- A ton of key concepts from this course are involved

NP-completeness

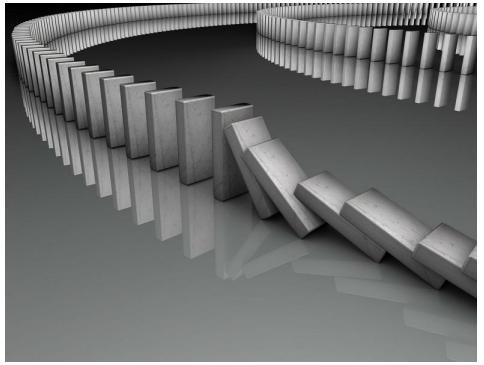


What else is NP-complete?

- We showed that CIRCUIT-SAT is NP-complete
- This will help us to prove that other problems, such as CLIQUE, are also NP-complete
- Idea: Chain reductions together



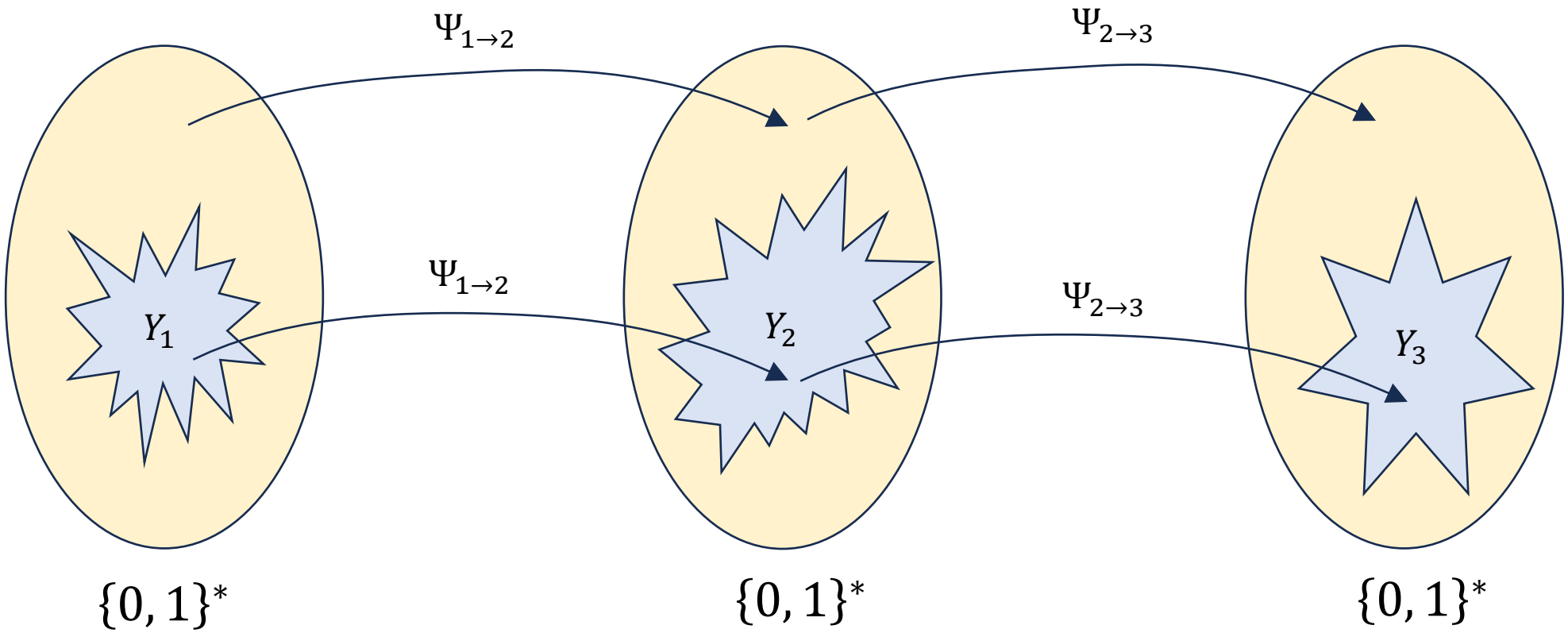
Chaining reductions together



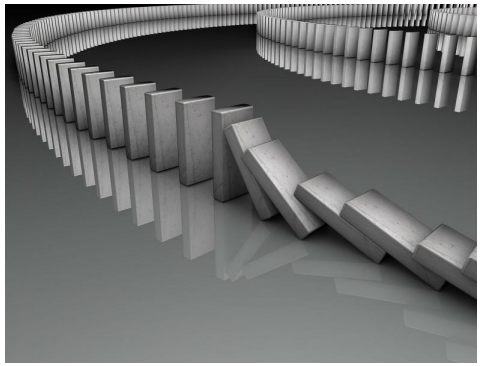
- **Claim:** If $Y_1 \leq_{\mathrm{P}} Y_2 \leq_{\mathrm{P}} Y_3$, then $Y_1 \leq_{\mathrm{P}} Y_3$
- **Proof:** Let $\Psi_{1\to2}$ and $\Psi_{2\to3}$ be the mapping reductions
- Reduction from Y_1 to Y_3: Given $w \in \{0,1\}^*$:
  1. Run $\Psi_{1\to2}$ on w to compute $w' \in \{0,1\}^*$
  2. Run $\Psi_{2\to3}$ on w' to compute $w'' \in \{0,1\}^*$
  3. Output w''

$|w'| \leq \mathrm{poly}(|w|)$, so the time complexity of step 2 is $\mathrm{poly}(|w|)$

Chaining reductions together

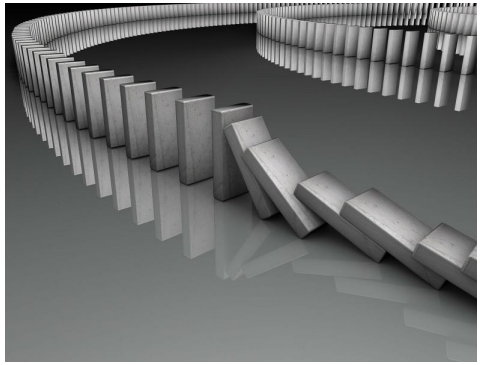


Chaining reductions together



- Let $Y_{\mathrm{OLD}}, Y_{\mathrm{NEW}} \subseteq \{0,1\}^*$
- **Claim:** If Y_{OLD} is NP-hard and $Y_{\mathrm{OLD}} \leq_{\mathrm{P}} Y_{\mathrm{NEW}}$, then Y_{NEW} is NP-hard
- **Proof:** Let $Z \in \mathrm{NP}$
- Then $Z \leq_{\mathrm{P}} Y_{\mathrm{OLD}} \leq_{\mathrm{P}} Y_{\mathrm{NEW}}$
- Therefore, $Z \leq_{\mathrm{P}} Y_{\mathrm{NEW}}$

Roadmap



- We will define a language called “3-SAT”
- We will prove $\text{CIRCUIT-SAT} \leq_P \text{3-SAT} \leq_P \text{CLIQUE}$
- This will show that CLIQUE is NP-hard

k-CNF formulas

- Recall: A CNF formula is an "AND of ORs of literals"
- **Definition:** A k-CNF formula is a CNF formula in which every clause has at most k literals
- Example of a 3-CNF formula with two clauses:

$$\phi = (x_1 \vee \bar{x}_2 \vee \bar{x}_6) \wedge (x_5 \vee x_1 \vee x_2)$$

The Cook-Levin Theorem

- Define $k\text{-SAT} = \{\langle \phi \rangle : \phi \text{ is a satisfiable } k\text{-CNF formula}\}$

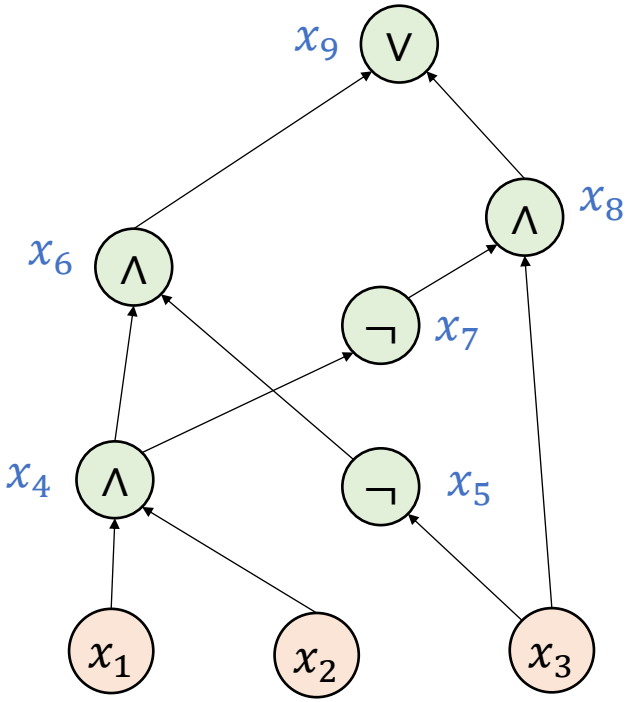
The Cook-Levin Theorem: 3-SAT is NP-complete

- **Proof:** We need to show two things.

1. We need to show $3\text{-SAT} \in \text{NP}$. What is the certificate?

2. We need to show that 3-SAT is NP-hard. Reduction from CIRCUIT-SAT

Reduction step 1: Circuit → Instructions



Initial circuit C

- $x_4 \leftarrow x_1 \wedge x_2$
- $x_5 \leftarrow \neg x_3$
- $x_6 \leftarrow x_4 \wedge x_5$
- $x_7 \leftarrow \neg x_4$
- $x_8 \leftarrow x_7 \wedge x_3$
- $x_9 \leftarrow x_6 \vee x_8$
- Return x_9

Reduction step 2: Instructions → Formula

- $x_4 \leftarrow x_1 \wedge x_2$
- $x_5 \leftarrow \neg x_3$
- $x_6 \leftarrow x_4 \wedge x_5$
- $x_7 \leftarrow \neg x_4$
- $x_8 \leftarrow x_7 \wedge x_3$
- $x_9 \leftarrow x_6 \vee x_8$
- Return x_9

$$(x_4 = x_1 \wedge x_2)$$
$$\wedge\ (x_5 = \neg x_3)$$
$$\wedge\ (x_6 = x_4 \wedge x_5)$$
$$\wedge\ (x_7 = \neg x_4)$$
$$\wedge\ (x_8 = x_7 \wedge x_3)$$
$$\wedge\ (x_9 = x_6 \vee x_8)$$
$$\wedge\ (x_9)$$

A Boolean formula on 9 variables

using operations $\wedge$, $\vee$, $\neg$, and $=$

Reduc rmula

Let C be the initial circuit and let ϕ be the final 3-CNF formula. Which of the following is <u>false</u>?

A: C is satisfiable if and only if ϕ is satisfiable

B: $|\langle\phi\rangle| \leq \text{poly}(|\langle C\rangle|)$

C: The number of clauses in ϕ is $\Theta(\text{size of } C)$

D: C and ϕ compute the same Boolean function

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

$(x_4$

$\wedge\ (x_5$

$\wedge\ (x_6 = x_4 \wedge x_5)$

$\wedge\ (x_7 = \neg x_4)$

$\wedge\ (x_8 = x_7 \wedge x_3)$

$\wedge\ (x_9 = x_6 \vee x_8)$

$\wedge\ (x_9)$

A Boolean formula on 9 variables using operations $\wedge$, $\vee$, $\neg$, and $=$

$\vee\ \bar{x}_1 \vee \bar{x}_2)$

$\wedge\ (\bar{x}_6 \vee x_4) \wedge (\bar{x}_6 \vee x_5) \wedge (x_6 \vee \bar{x}_4 \vee \bar{x}_5)$

$\wedge\ (x_7 \vee \bar{x}_4) \wedge (\bar{x}_7 \vee x_4)$

$\wedge\ (\bar{x}_8 \vee x_7) \wedge (\bar{x}_8 \vee x_3) \wedge (x_8 \vee \bar{x}_7 \vee \bar{x}_3)$

$\wedge\ (x_9 \vee \bar{x}_6) \wedge (x_9 \vee \bar{x}_8) \wedge (\bar{x}_9 \vee x_6 \vee x_8)$

$\wedge\ (x_9)$

Final 3-CNF formula ϕ

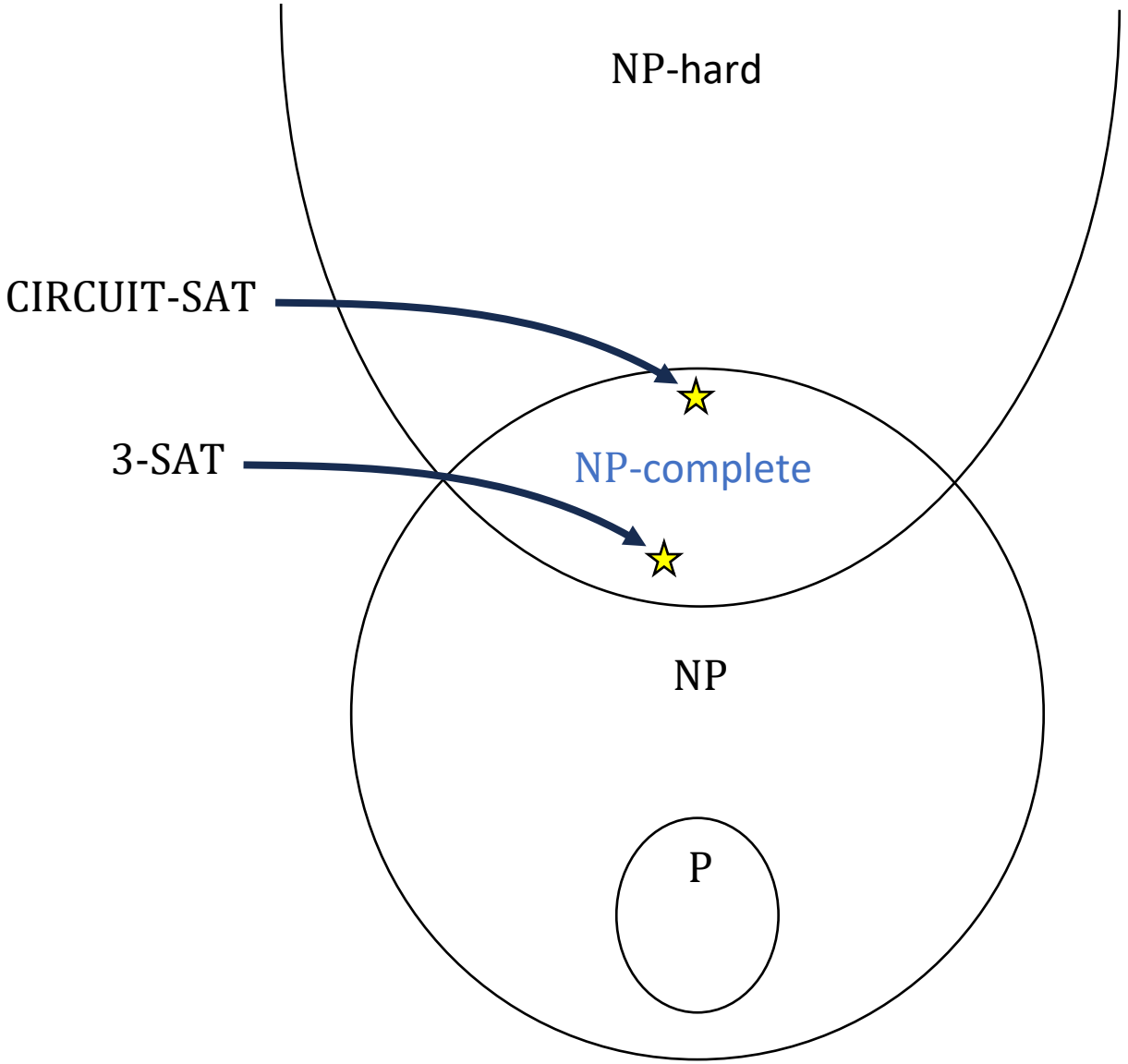
Every Boolean function has a CNF representation!

Reduction correctness

- Let the gates of C be $g_1, \ldots, g_m$ (topological order)
- **Claim:** C is satisfiable if and only if ϕ is satisfiable
- **Proof:** $(\Rightarrow)$ Suppose $C(x_1, \ldots, x_n) = 1$
- Let $x_{n+i} = g_i(x_1, \ldots, x_n)$
- Then $\phi(x_1, \ldots, x_{n+m}) = 1$

Reduction correctness

- Let the gates of C be $g_1, \ldots, g_m$ (topological order)
- **Claim:** C is satisfiable if and only if ϕ is satisfiable
- **Proof:** ($\Leftarrow$) Suppose $\phi(x_1, \ldots, x_{n+m}) = 1$
- Then $x_{n+i} = g_i(x_1, \ldots, x_n)$ for every i by induction
- Furthermore, $x_{n+m} = 1$
- Therefore, $C(x_1, \ldots, x_n) = 1$


NP-hard
CIRCUIT-SAT
3-SAT
NP-complete
NP
P