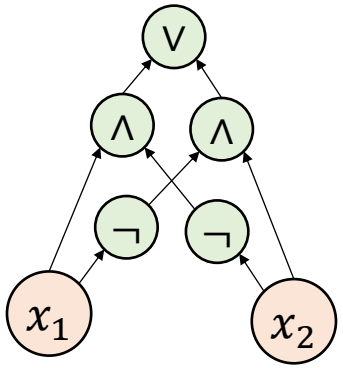
CMSC 28100

Introduction to Complexity Theory

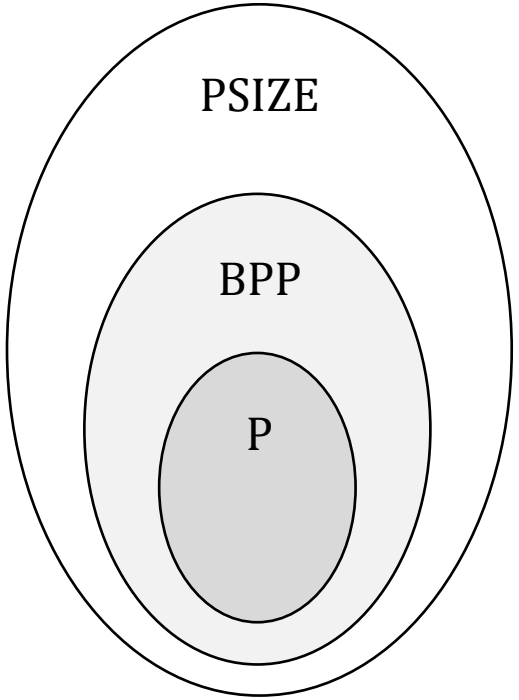
Spring 2025
Instructor: William Hoza

The complexity class $\mathbf{PSIZE}$

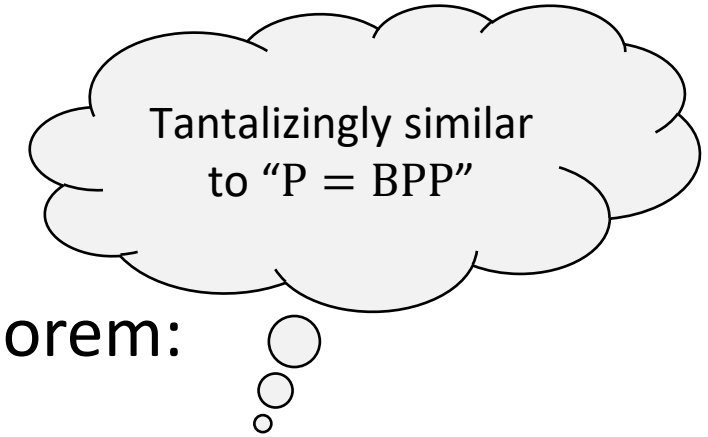


- Let $Y \subseteq \{0,1\}^*$
- By definition, $Y \in \mathrm{PSIZE}$ if for each n, there exists a $\mathrm{poly}(n)$-size circuit C_n that decides Y restricted to inputs of length n

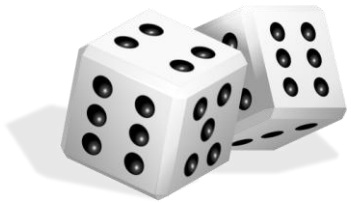
Adleman's theorem



- Last class: $\mathrm{P} \subseteq \mathrm{PSIZE}$



- Next, we will prove a stronger theorem:



Adleman's Theorem: $\mathrm{BPP} \subseteq \mathrm{PSIZE}$

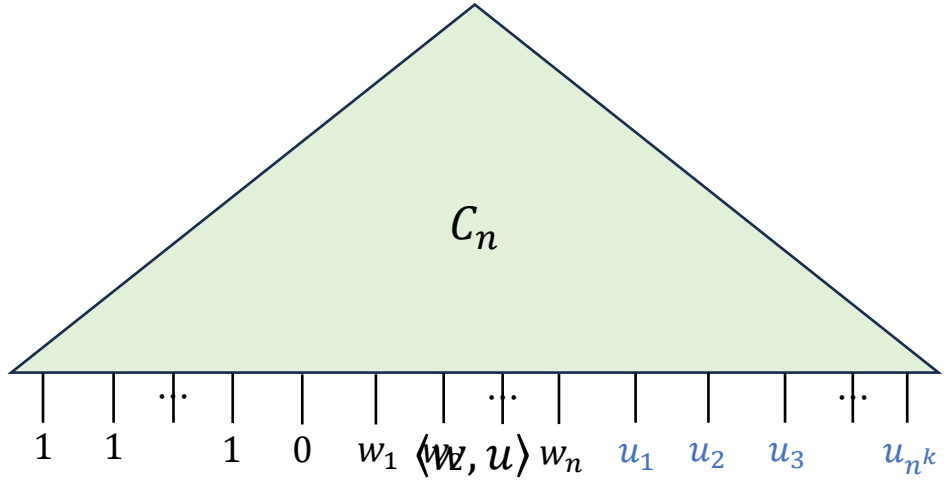
- Note: The circuit model is a deterministic model of computation!
- Proof of Adleman's theorem: Next 6 slides

Adleman proof step 1: Amplification

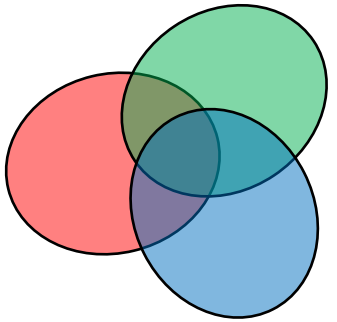
- Let $Y \in \mathrm{BPP}$
- By the amplification lemma, there exists a poly-time randomized Turing machine M such that for every $n \in \mathbb{N}$ and every $w \in \{0,1\}^n$:
  - If $w \in Y$, then $\Pr[M \text{ accepts } w] > 1 - 1/2^n$
  - If $w \notin Y$, then $\Pr[M \text{ accepts } w] < 1/2^n$

Adleman proof step 2: TM ⇒ Circuit

- Let $R = \{\langle w, u\rangle : M \text{ accepts when } w \text{ is on tape 1 and } u \text{ is on tape 2}\}$
  - Technical detail: Use the encoding $\langle w, u\rangle = 1^{|w|}0wu$
- Then $R \in \mathrm{P} \subseteq \mathrm{PSIZE}$
- Therefore, for every $n \in \mathbb{N}$, there exists a $\mathrm{poly}(n)$-size circuit C_n such that for every $w \in \{0,1\}^n$, if we pick $u \in \{0,1\}^{n^k}$ at random, then $\Pr[C_n(wu) \neq Y_n(w)] < 1/2^n$



Adleman proof step 3: The union bound



- Key fact from probability theory:

The Union Bound: For any events $E_1, E_2, \ldots, E_k$, we have

$$\Pr[E_1 \text{ or } E_2 \text{ or } \ldots \text{ or } E_k] \leq \Pr[E_1] + \Pr[E_2] + \cdots + \Pr[E_k]$$

- Example: If we pick two cards from a deck, then

$$\Pr[\text{card 1 is a queen or card 2 is a queen}] \leq \frac{1}{13} + \frac{1}{13} = \frac{2}{13}$$

Adleman proof step 3: The union bound

Claim: For every n, there exists $u_* \in \{0,1\}^{n^k}$ such that

for all $w \in \{0,1\}^n$, we have $C_n(wu_*) = Y_n(w)$

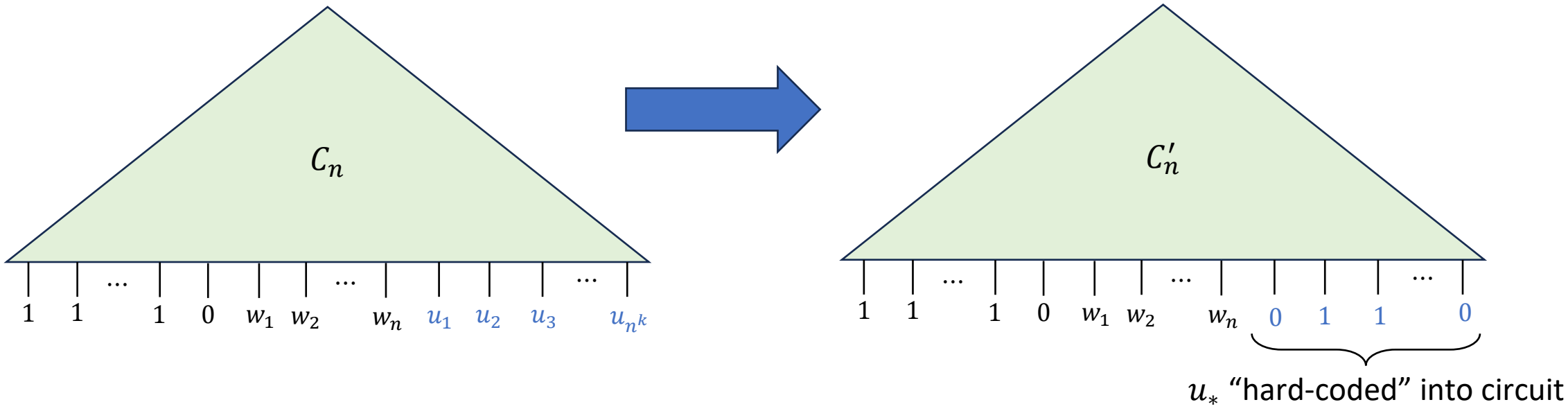
- **Proof:** Pick $u \in \{0,1\}^{n^k}$ uniformly at random. Then

Union Bound

$$\Pr\left[\begin{array}{c}\text{there exists } w \in \{0,1\}^n \\ \text{such that } C_n(wu) \neq Y_n(w)\end{array}\right] \leq \sum_{w \in \{0,1\}^n} \Pr[C_n(wu) \neq Y_n(w)] < 2^n \cdot \frac{1}{2^n} = 1$$

- The claim follows!

Adleman proof step 4: Hard-coding



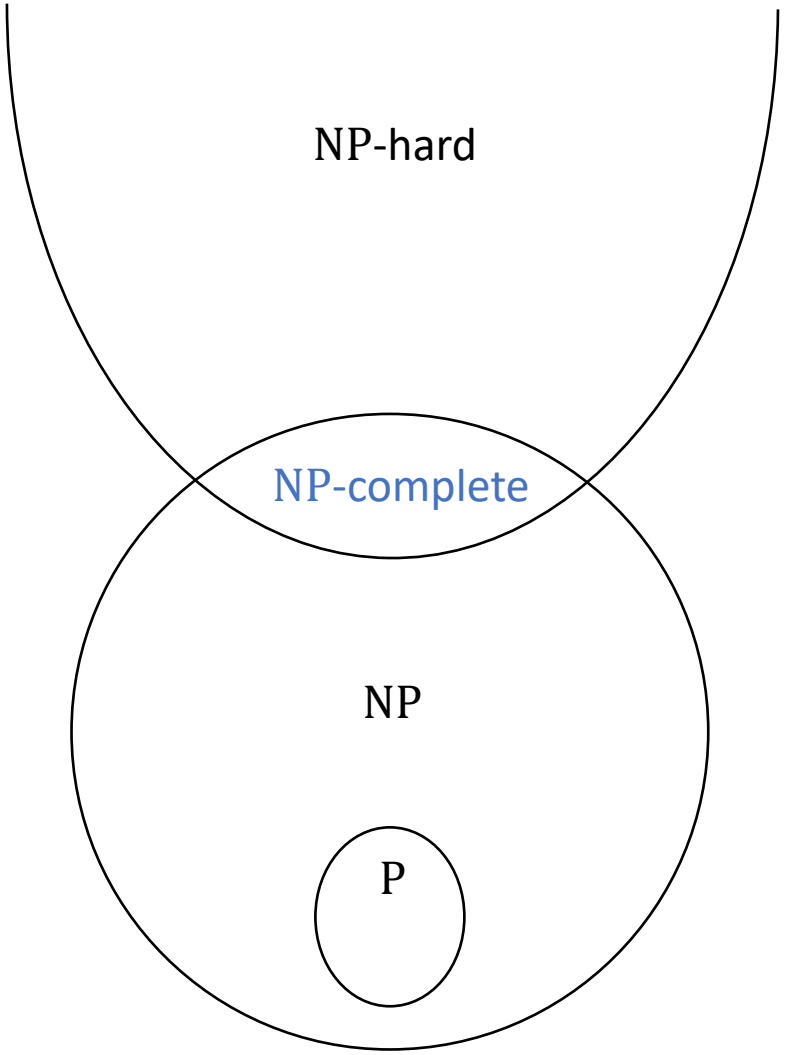
- C'_n computes Y_n and it has size $\mathrm{poly}(n)$
- Therefore, $Y \in \mathrm{PSIZE}$

Adleman's theorem and P vs. BPP

- Adleman's theorem makes "$\mathrm{P} = \mathrm{BPP}$" seem more plausible
- There is also more compelling evidence suggesting $\mathrm{P} = \mathrm{BPP}$
  - Beyond the scope of this course

Circuits and NP-completeness

- Why are we studying circuits?
  - It will help us prove that many interesting problems are NP-complete
  - E.g., CLIQUE
- Key idea: Code as Data



Code as data III

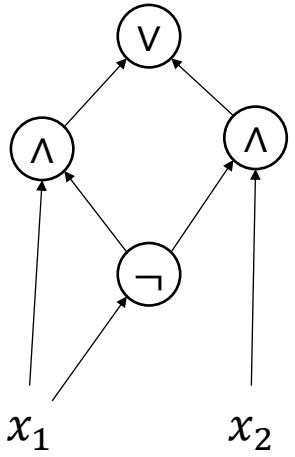
- Recall principle: A Turing machine M can be encoded as a string $\langle M \rangle$
  - M is an algorithm, but at the same time, $\langle M \rangle$ can be an input to another algorithm!
- Similar idea: A circuit C can be encoded as a string $\langle C \rangle$
  - C is an "algorithm," but at the same time, $\langle C \rangle$ can be an input to another algorithm!
  - You'll explore encoding details (Exercise 22)
  - What can we do with this idea?

Circuit value problem

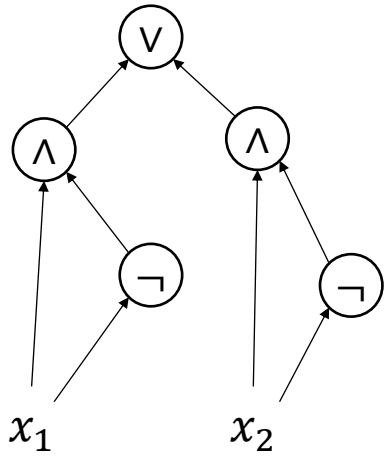
- Let $\text{CIRCUIT-VALUE} = \{\langle C, x\rangle : C \text{ is a circuit and } C(x) = 1\}$
- **Claim:** $\text{CIRCUIT-VALUE} \in \text{P}$
- **Proof sketch:** Suppose C has m nodes. To compute $C(x)$:
    1) Mark all the input nodes with their values
    2) While there is an unmarked node:
        a) For every gate g, find all the nodes that feed into g. If they are all marked with their values, then mark g with its value

Circuit satisfiability

- Let C be an n-input 1-output circuit
- We say that C is satisfiable if there exists $x \in \{0,1\}^n$ such that $C(x) = 1$



Satisfiable ✔



Unsatisfiable ✘

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.

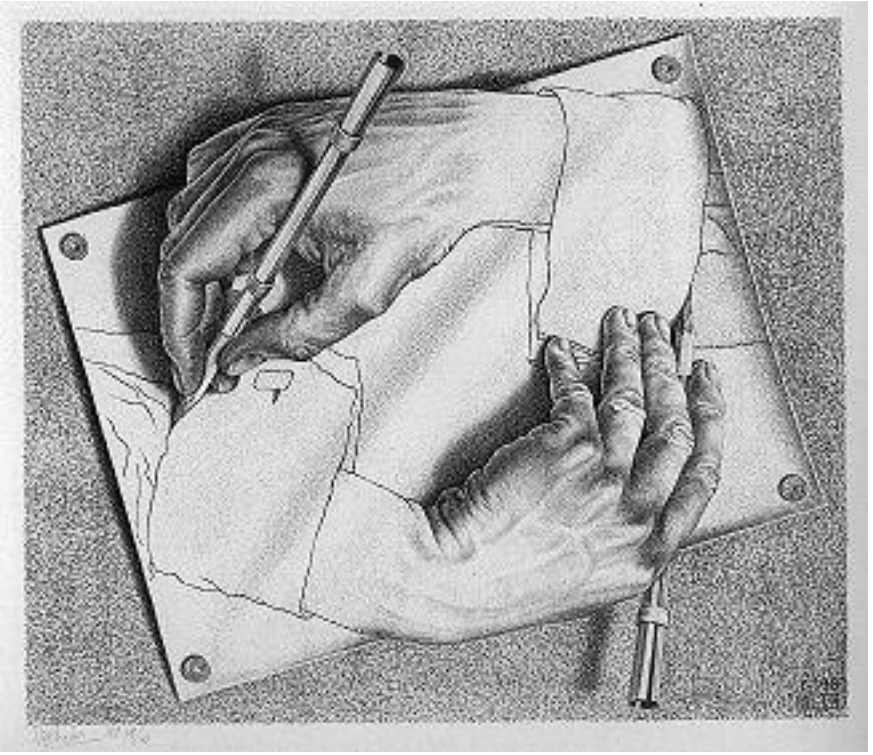
- Proof: Next 8 slides

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"

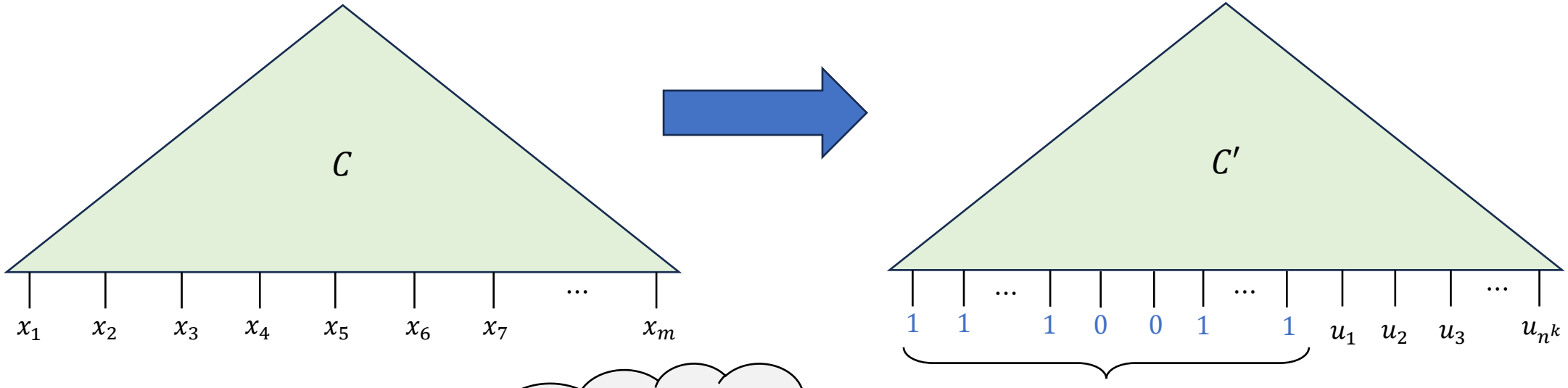


"Drawing Hands."
(1948 lithograph by M. C. Escher)

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 $C'(u) = C(\langle w, u \rangle)$