24 March 2025	SAT is	HARD
· · · · · · · · · · · · · · · · · · ·	a.k.a. The (ook-Levih
Plan	· · · · · · · · · · · ·	Theorem
* Recall CNF-S		· · · · · · · · · · · · · · · · ·
X Announcements		· · · · · · · · · · · · · · · · · ·
* Reductions To	SAT.	· · · · · · · · · · · · · · · · · · ·
L> INDSET <	$_{P}$ $CNF-SA$	
CIRCUIT-SAT	\leq_{P} 3SAT	. .
 		
· · · · · · · · · · · · · · · · · · ·		
· · · · · · · · · · · · · · · · · · ·		

Boolean Satisfiability Given: boolean formula ? in Conjunctive Normal Form $CNF = \left(\left(\begin{array}{c} x_{1} \\ x_{2} \end{array}\right) \times \left(\begin{array}{c} x_{2} \\ x_{3} \end{array}\right) \times \left(\begin{array}{c} x_{3} \end{array}\right) \times \left(\begin{array}{c} x_{3} \\ x_{3} \end{array}\right) \times \left(\begin{array}{c} x_{3} \end{array}\right) \times \left(\begin{array}{c} x_{3} \\ x_{3} \end{array}\right) \times \left(\begin{array}{c} x_{3} \\ x_{3} \end{array}\right) \times \left(\begin{array}{c} x_{3} \end{array}\right) \times \left($ Question. Does there exist an truth assignment to (x, . - . Xn) that satisfies P?

Why study SAT?												
Cook-Levin	Theorem.	SATis	NP-Complete.									
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · ·									
· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · ·										
· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · · · · ·									
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · · · ·									
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · ·									
· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·		. .									
· · · · · · · · · · · · · · · · · ·												
· · · · · · · · · · · · · · · · · · ·												

Why study SAT?												
Cook-Levin	Theorem.	SAT is NP-Complete.										
$\downarrow SAT$	is in NP	 										
. 										
	· · · · · · · · · · · · · · · · · · ·											
. .	. .											
	· · · · · · · · · · · · · · ·	.										

Why study SAT?
Cook-Levin Theorem. SAT is NP-Complete.
L> SAT is in NP.
Poly-time verifier for SAT. $V(\varphi, \bar{\alpha})$.
For each clause in P if ā does not satisfy clause
Return 1
Return V
· · · · · · · · · · · · · · · · · · ·

Why study	SAT T = 2
Cook-Levin	Theorem.	SAT is	NP-Complete.
\downarrow SAT	īs in N		. .
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$-\frac{1}{2} + \frac{1}{2} + 1$	$-\frac{1}{2}$. .
.
· ·		· · · · · · · · · · · ·	
· ·			
. .	· · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · ·

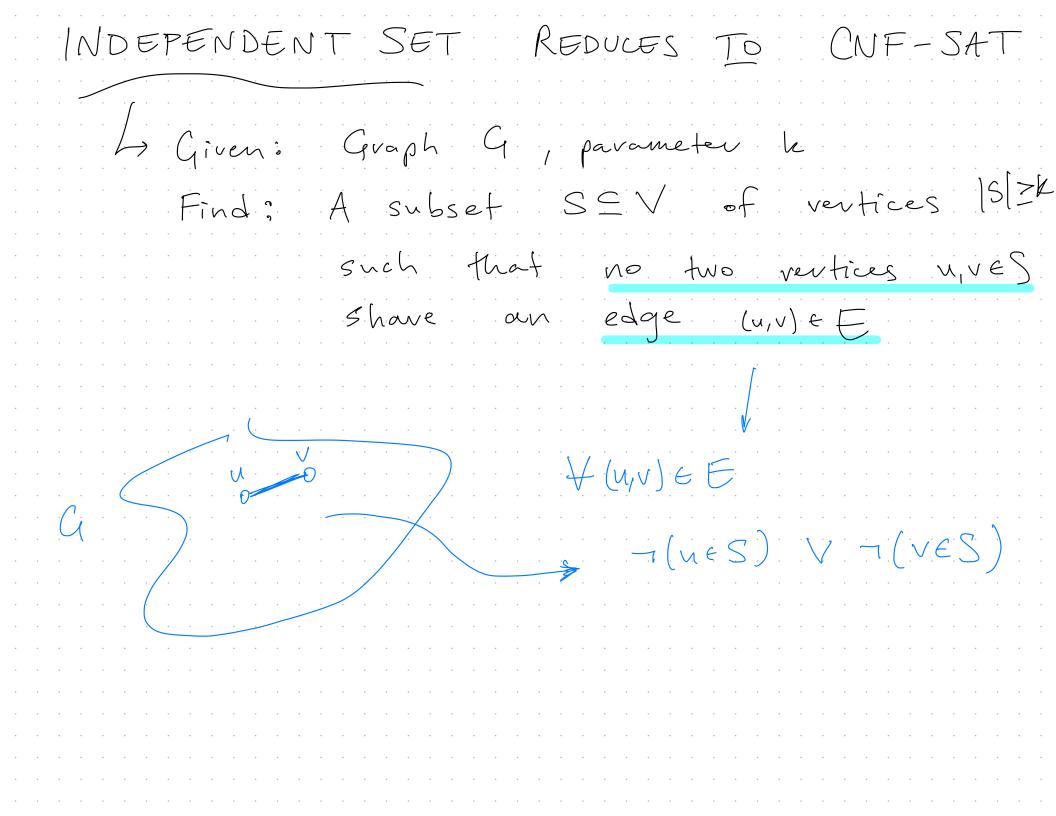
Why study SAT?	•
Cook-Levin Theorem. SAT is NP-Complete.	•
$L \gg SAT$ is in NP.	•
LD SAT is NP-Hard.	•
Every efficiently verifialde problem reduces to SAT! Solving SAT is hard! Solving SAT is powerful!	•

Announcements
XHW6 ongoing
* Prelim #2
- Thurs, Mar 27, 7:30-9p.
- Review Session: Tues, Mar 25, 7-9p
- Wed Lecture
· Review of Topics
X Next Week: Spring Break!
· ·
· · · · · · · · · · · · · · · · · · ·

Every	efficiently	verifialde	problem	reduces						
	plving SAT is	the second of the second secon		SAT1						
	lving SAT is	powerful	· · · · · · · · · · ·	· · · · · · · · · · · ·						
	· · · · · · · · · · · · ·									

Every efficiently verifiable problem reduces
Solving SAT is have! to SAT!
Solving SAT is powerful!
> Practical Aborithm Jesign paradigm:
- Reduce problem to SAT
- Use optimized SAT SOLVER to solve fue problem
(See Friday's Lecture)

INDEPENDEN7		REDUCES T	O CNF-SAT
			k F vertices
. .	such tha Shave a	t no two n edge	vertices $u, v \in S$ $(u, v) \in E$
		reduction	
. .	· · · · · · · · · ·		has INDSET ZK



INDEPENDENT SET REDUCES TO CNF-SAT La Given: Graph G, parameter le Find; A subset SEV of vertices ISIZK such that no two vertices $u, v \in S$ shave an edge $(u, v) \in E$ $\forall (u,v) \in E$ $\frac{1}{2} = \frac{1}{2} \left(u \in S \right) = \sqrt{1} = \frac{1}{2} \left(u \in S \right)$ $\left(\neg x_{v} \lor \neg x_{v}\right) \land \left(\neg x_{v} \lor \neg x_{t}\right) \land \left(\neg x_{v} \land \neg x_{v}\right) \land \left(\neg x_{v} \land \neg x_{v}\right) \land \left(\neg x_{v} \land \neg x_{v}\right) \land \left(\neg$ YeeE

· · ·	C	1 2	N	· · · · · · · · · · · · · · · · · · ·		1	· · ·		∨ , .	(†)	.)	· · ·	•	•	· · ·	•	•	· · ·	•	• •	· ·	•	· · ·	•	•	• •	•	· · ·	•	· · ·	•	•
· ·	· · ·		bg		· · ·	· ·	· · ·				⁄.	 	X_~)		•		م : م		· · ·	r V r	· · ·	۲۰۷	(~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	· · ·)		. —	· · ·		•
· ·	· ·	· ·	· ·	· · ·	· · ·				· ·			 1 X				•	, , , , , , ,)	• •	•	• •	•	•	• •	•	· ·	•	· ·	•	•
· ·	· · ·	· · ·	· · ·	•	· ·	(יי _ו ע	,) ∈ , , , , ,	Ę.	· ·	•	•	· ·	•	•	· ·	•	•	· ·	•	• •	· ·	•	· ·	•	•	• •	•	· ·	•	· ·	•	•
· ·	· ·	· ·	· ·	•	· · ·	· ·	· ·	•	· · ·	•	•	· ·	•	•	· · ·	•	•	· ·	•	• •	· ·	•	••••	•	•	• •	•	· ·	•	· ·	•	•
· ·	· ·	· ·	· ·	•	 		•••		· ·		•	· ·	•	•	· ·		•	· ·	•	• •	• •	•	· ·	•		• •	•	· ·	•	· ·	•	•
· ·	· ·		· · ·	•	• •		• •	•	• •	•	•	• •	•	•	• •	•	•	• •	•	• •	• •	•	• •	•	•	• •	•	• •	•	• •	•	•
· ·	• •	••••	• •	•				•				••••	•					•••		• •						• •	e e		•	• •	•	•
· ·	• •	•••	• •	•				•	• •		•	•••			•••			•••	•	•		•			•	• •	•		•	• •	•	•
• •	• •	• •	• •	•		•	• •		• •	•	•	• •	•	•	• •	•		• •	•	•	•	•	• •		•	• •	•	• •	•	• •	٠	

$G \sim$	ren G	$\frac{1}{2} = \frac{1}{2} \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ 2 \end{array} \right) \left(\begin{array}{c} 1 \end{array} \right) \left(\begin{array}{c} 1 \\ 2 \end{array} \right) \left(\begin{array}{c} 1 \end{array} \right) \left$	E)	· · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·	· · · ·
· · · · · · · ·			$\mathcal{L}_{\mathcal{L}} = \left\{ \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 &$			$ \begin{array}{c} \begin{array}{c} & & \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \end{array} \\ \begin{array}{c} \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \end{array} $	· · · ·
· · · · · · · ·		$(u,v) \in E$					· · · ·
	· · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · ·	· · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·	· · ·
· · · · (')· a	îm	the statis	sat	is fiable	ìff i		• • •
				isfiable Ghas		independent s	
. <th></th> <th>. </th> <th>G. has</th> <th></th> <th>Independent s</th> <th>· · · ·</th>		G. has		Independent s	· · · ·
. .	· · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · ·				Independent s	· · · · · · · · · · · · · · · · · · ·

Green	$C_{1} = (v_{1} \in v_{1})$
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	$= \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \\ -1 \times 1 & 1 \end{array} \right) \left(\begin{array}{c} -1 \times 1 & 1 \end{array}$
. .	$= \left(\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 $
Claim	for is satisfiable iff
· · · · · · · · · · ·	G has an independent set.
· · · · · · · · · · ·	
	problem ;
	· · · · · · · · · · · · · · · · · · ·

INDEPENDENT SET REDUCES TO CNF-SAT
Liven: Graph G, parameter le
Find; A subset SEV of vertices ISIZK
such that no two vertices u, v € S shave an edge (u, v) € E
Need some mechanism to count to k 1
Otherwise $S = \phi$, i.e. $\overline{a} = \overline{0}$ satisfies P_q

At	most	k	vertices		· · · · · · ·	· ·
· · · · · ·	· · · · · ·	$\overline{\mathbf{v}}$	· · · · · · · · · · ·			
. 		· · · · · ·		$\begin{array}{cccccccccccccccccccccccccccccccccccc$	- /	M is the first vertex ih S
· · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · · ·			
· · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · · ·			
· · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · · · ·			
 	· · · · · ·	· · · · ·	· · · · · · · · · ·	· · · · · · · ·	· · · · · · ·	. .
						. .

• •	At		ost	k	 V	evt	ce	ŝ	ĴΥ		5,	· ·	· · ·	· · ·	• •	· · ·	· · ·	· ·
• •	· · ·	· · ·	· ·			· · ·	· ·		· · ·	$\frac{1}{2}$	fec	 	Ore	Jer	th	e ve		و ک
• •	· · ·	· · · ·				· · · ·	· ·	· · · ·	· · · ·		••••	· · ·	· · · ·					· ·
• •	· · ·							(i) X								 	he	
	· · ·	· · ·						· · · ·							ist		rte	
• •	· · ·		· · ·	· · · ·	· · · ·									,) b		· 		
• •	· · ·	· · ·	· ·	· · ·	· · ·		· ·	· · ·	· · ·			· ·	· · ·		· ·	· · ·		
• •	· · ·	· · ·	· ·	· · ·	· · ·		· ·	· · ·	· · ·		• •	· ·	· · ·		· ·	· · ·		· ·
· ·	· · ·	· · ·	· ·	· · ·	· · ·	· · ·	· ·	· · ·	· · ·	· ·	· ·	• •	· · ·	· · ·	· ·	· · ·		· ·
• •	· · ·						• •								• •			• •
• •	· · ·						• •								• •			• •
• •	· · ·		• •	• • •			o o			• •	• •	• •	• • •		0 0	• • •	0 0 0	• •

At	most k	i vertic	es î	$\sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n} \sum_{i$	· · · · · · ·	· · ·	· · · · · · · ·
				Idea.	Order	the SS	verties EV
				 <td> . .</td> <td>· · · · · · · · ·</td>	 . .	· · · · · · · · ·
. 			· · · · · · ·		 	 	· · · · · · · · ·
. 		k va Per	viable verte		· · · · · · ·	· · · ·	· · · · · · · · ·
. .		$(z) = \frac{1}{2} + \frac{1}{2}$		vertex	the it		

$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$ \times + + + + + + + + + + + + + + + $	Constraints	
	$ X_{2}$		
.
$X_{n} = \left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right) \left(\begin{array}{c} 1 \\ 1 \\ 2 \end{array}\right) \left(\begin{array}{c} 1 \\ 1 \\ 2 \end{array}\right) \left(\begin{array}{c} 1 \end{array}\right) \left(\begin{array}{c} 1 \\ 2 \end{array}\right) \left(\begin{array}{c} 1 \\ 2 \end{array}\right) \left(\begin{array}{c} 1 \end{array}\right) \left(\begin{array}{c} 1 \\ 2 \end{array}\right) \left(\begin{array}{c} 1 \end{array}\right) \left(\left(\begin{array}{c} 1 \end{array}\right) \left(\end{array}\right) \left(\begin{array}{c} 1 \end{array}\right) \left(\left(\begin{array}{c}$	(u)	. .	
. .	· ·	· ·	· · · · · · · · · ·
. .	· ·	· ·	· · · · · · · · ·
	· · · · · · · · · · · · · · · · · ·		· · · · · · · · ·

$X_{1} = (1) + (2$		(1) For each ve V $f_{x_v}^{(i)} = 1$
(1) (2) (-7)	· · · · · · ·	$\left(\begin{array}{ccc} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot &$

$ \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2$	Constraints
$X_{2} = X_{2} = X_{2$	(i) For each ve V f = 1 f = 1
$X_{n} = X_{n} = X_{n}$	
$\frac{1}{1}$	$\left(\begin{array}{ccc} \ddots & \ddots $
$ \begin{array}{c} \cdot \cdot$	$ \begin{array}{c} (1, 1) \\ (2, 1) \\ (3, 2) \\ (3, $

$(\tau) = (2)$	(\mathcal{W}^{\prime})	Constraints
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		() For each ve V
		$\rightarrow At most 1 x_v^{(i)} \equiv 1$
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		2) For each 15is K
$X_{n}^{(1)} = X_{n}^{(2)}$		$ \begin{array}{c} & \leftarrow \\ & \leftarrow $
For each i (i)	$(\tilde{\tau})$	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	X ₂	At least one uES
· · · · · · · · · · · · · · · · · ·		is the it vertex
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · ·	

$X = \left\{ \begin{array}{c} (1) \\ (2) $	Constraints
$X_{2} = X_{2} = X_{2$	(1) For each ve V
(1)	2 For each 15is K
$X_{n} = X_{n}$	$ \qquad \qquad$
For each i	· · · · · · · · · · · · · · · · · · ·
$(\dot{i}) = (\dot{i}) = ($	$\begin{array}{c} (i) \\ \chi_3 \\ \end{array} \\ \end{array} \bigvee \chi_3 \\ \end{array} $
For each w, v · · · · · · · · · · · · · · · · · ·	$\begin{pmatrix} \dot{c} \\ \dot{c} \end{pmatrix} = \begin{pmatrix} \dot{c} \\ \dot{c} \end{pmatrix} $
	At most 1 ues
	is the it vertex

$X = \left\{ \begin{array}{c} (1) \\ (2) \\ (2) \\ (3) \\ (4) $	Constraints
$X_{2} = X_{2} = X_{2}$	() For each ve V
	$(2) For each \leq i \leq k$
$X_{n}^{(1)} = X_{n}^{(2)} = X_{n}^{(2)}$	(2) For each $1 \leq n \leq n$ (2) For each $1 \leq n \leq n$ $f \neq f \leq x_a + (y) \leq 1$ $X_v = [$
For each i ((i)) ((i)) ((i)) (X_1) X_2)	$(i) \qquad \qquad$
For each v,v	$\neg (\tilde{i}) \rightarrow (\tilde{i}) \rightarrow$
$\begin{array}{c} \begin{array}{c} \end{array} \\ \end{array} $	$ \begin{array}{c} (\hat{z}) \\ (z$

(t) = (t) + (t)	· · · · · · · · · · · · · · · · · · ·	Constraints
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{c} \cdot \cdot$	(1) For each ve V
· · · · · · · · · · · · · · · · · · ·	· · · · · · ·	$A+i most 1 X_v = 1$
$X_{n} = X_{n} = X_{n}$	- X(a	
		$ \begin{array}{c} \\ $
· · · · · · · · · · · · · · · · · · ·	· · · · · · ·	(3) For $(u,v) \in E$ for all i,j . SET $\neg X_{u}^{(i)} \vee \neg X_{v}^{(j)}$
ORIGINAL IN CONSTR	NEPENDE'L AINTS	SET
$(v,v) \in C$ $I \leq c$	4]≤.h	$(\tilde{\mathbf{x}}) = (\tilde{\mathbf{x}}) = (\mathbf$
		· · · · · · · · · · · · · · · · · · ·

G has an independent set S of cardinality Zh G has an independent set $S = \{ u^{(1)}, u^{(2)}, \dots, u^{(2)} \}$ $\phi_{(1)}$ Λ $\phi_{(2)}$ Λ $\phi_{(3)}$ $\beta_{(3)}$ $\beta_{(3)$

G has an independent set S of cardinality Zh
S of cardinality Zh
G has an independent set
$S = \left\{ \begin{array}{c} (1) \\ (2) $
- polynomial -sized CNF
- each clause can be generated in poly-time.
\Rightarrow IND SET \leq_{p} CNF - SAT

n a construction of the second
 INDSET
T A S
\cdots

. NP. NDSET 7 SAT CIRCUIT SAT Theorem (Cook - Levin). Every problem in NP reduces to 35AT in polynomial - time

	$-SAT \leq_P 3SAT$
	Logical Circuit C: 20,13 ⁿ -> 20,13
Question	Does there exist XEZO,13h
· · · · · · · · · · · ·	S.t. $C(x) = 1$?
· · · · · · · · · · · ·	
· · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · ·	. .
	<pre>- · · · · · · · · · · · · · · · · · · ·</pre>
	· · · · · · · · · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · · · ·

CIRCUIT - SAT < BAT
Given: Logical Circuit C: 20,13 ⁿ -> 20,13
Question Does there exist $x \in \{0, 1\}^h$ s.t. $C(x) = 1$?
Note Circuit SAT ≤ BSAT is a key step in proof of Cook-Levin Theorem!
Intrition. Logical Circuits can implement any algorithm.

CIRCUIT - SAT < BAT
Given: Logical Circuit C: 20,13 ⁿ -> 20,13
Question Does there exist $x \in \{20, 1\}^{h}$ s.t. $C(x) = 1$?
Note. Circuit SAT is a key step in proof of Cook-Levin Theorem!
Intrition. Logical Circuits can implement any algorithm.
Encluding poly-time Verifier for any NP problem!

, des
· · ·

Civcuits
* Represented as a DAG
* Vertices = "Gates" // Each gate computes a * Edges = "Wires" boolean fr. on 2-variables
* Edges E Wires
, n total input wires to cirmit
\rightarrow Output determined by evaluating each gate from bottom to top.
Reduction idea and z
93 93 94 73 74 74 74 74 74 74 74 74 74 74 74 74 74
(9,) (9,) (1,)
$\begin{array}{cccccccccccccccccccccccccccccccccccc$

Verif	y ca	ch gate	· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · ·
				X + Z = 1	NAND(X,Y)
gate		A NAND NAND NAND	e		$\begin{array}{cccccccccccccccccccccccccccccccccccc$
	· · · · ·	"Negated ANO"		Note: NAND is	Complete
	• • • •				
	• • • •				
	• • • •				
	• • • •				

Verify	each gate	· · · · · · · · · · · · · · · · · · ·
	· · · · · · · · · · · · · ·	X Y Z = NAND(X, Y)
gate Tupnt		9^{ate} 1^{a} 0^{a} 1^{a} 1^{a} 0^{a} 1^{a} $1^$
· · · · · · · · ·	"Negated AND"	Note: NAND is Complete
GATE	GADGET.	Set of clause satisfied by any X,Y,Z s.t. Z=NAND(X,Y)
	$(X \land Y) \rightarrow (X \land$	
Z	$ \xrightarrow{A} \xrightarrow{A} \xrightarrow{A} \xrightarrow{A} \xrightarrow{A} \xrightarrow{A} \xrightarrow{A} \xrightarrow{A}$	$ \bigwedge_{i} = \frac{1}{2} \xrightarrow{i} \frac{1}{2} \longrightarrow_{i} \left(\left(X_{i} \wedge Y_{i} \right) \right) $
	$(\mathcal{A} \cap \mathcal{A} \cap$	$ \bigwedge_{i} \left(\begin{array}{c} i \not \not \not \not \not \not \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not \not \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not \not & i \end{pmatrix} \right) \left(\begin{array}{c} i \not & i \end{pmatrix} \right$

NAND 45 NAND ·G. 4 GI (NAND) NAND) $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1$ NANT poly-sized CNF (NAND) satisfiable iff 3 x e 20,138 s.t X, X2 X3 X4 X5 X6 X7 X8 C(x) = 1 $\begin{aligned} \varphi_{c} &= \varphi_{6} \wedge \left(\left(\neg \varphi_{1} \vee \neg \chi_{1} \vee \neg \chi_{2} \right) \wedge \left(\varphi_{1} \vee \chi_{1} \right) \wedge \left(\varphi_{1} \vee \chi_{2} \right) \right) \\ \wedge \left(\neg \varphi_{2} \vee \neg \chi_{4} \vee \neg \chi_{5} \right) \wedge \left(\varphi_{2} \vee \chi_{4} \right) \wedge \left(\varphi_{2} \vee \chi_{5} \right) \right) \end{aligned}$ (gate 1 gadget) (gate 2 gadaget) $(\neg G_6 \vee \neg G_4 \vee \neg G_5) \land (G_6 \vee G_4) \land (G_6 \vee G_5))$ (gate 6 gadget)