24 March 2025

SAT is HARD

a.k.a. The Cook-Levin Theorem

Plan

* Recall CNF-SAT
* Announcements
* Reductions TO SAT
  - ↳ IND SET $\leq_p$ CNF-SAT
  - ↳ CIRCUIT-SAT $\leq_p$ 3SAT

Boolean Satisfiability

Given: boolean formula φ in Conjunctive Normal Form

CNF $\varphi = (x_1 \vee \neg x_2 \vee x_5) \wedge (x_2 \vee x_3 \vee x_7 \vee \neg x_6) \wedge \dots \wedge (\neg x_1 \vee \neg x_{100})$

Question:

Does there exist an truth assignment to $(x_1 \dots x_n)$ that satisfies φ ?

Why study SAT?

Cook-Levin Theorem. SAT is NP-Complete.

Why study SAT?

Cook-Levin Theorem. SAT is NP-Complete.

↳ SAT is in NP.

Why study SAT?

Cook-Levin Theorem. SAT is NP-Complete.

↳ SAT is in NP.

Poly-time verifier for SAT.

$V(\varphi, \vec{a})$.

For each clause in φ

if $\vec{a}$ does not satisfy clause

Return $\perp$

Return ✓

Why study SAT?

Cook-Levin Theorem. SAT is NP-Complete.

- ↳ SAT is in NP.
- ↳ SAT is NP-Hard.

Why study SAT?

Cook-Levin Theorem. SAT is NP-Complete.

↳ SAT is in NP.

↳ SAT is NP-Hard.

$\Downarrow$

Every efficiently verifiable problem reduces to SAT!

Why study SAT?

Cook-Levin Theorem. SAT is NP-Complete.

↳ SAT is in NP.

↳ SAT is NP-Hard.

↓

Every efficiently verifiable problem reduces to SAT!

Solving SAT is hard!

Solving SAT is powerful!

Announcements

* HW6 ongoing

* Prelim #2
  - Thurs, Mar 27, 7:30-9p.
  - Review Session: Tues, Mar 25, 7-9p
  - Wed Lecture
    - Review of Topics

* Next Week: Spring Break!

Every efficiently verifiable problem reduces to SAT!

Solving SAT is hard!

Solving SAT is powerful!

Every efficiently verifiable problem reduces to SAT!

Solving SAT is hard!

Solving SAT is powerful!

Practical Algorithm design paradigm:

- Reduce problem to SAT
- Use optimized SAT SOLVER to solve the problem

(See Friday's Lecture)

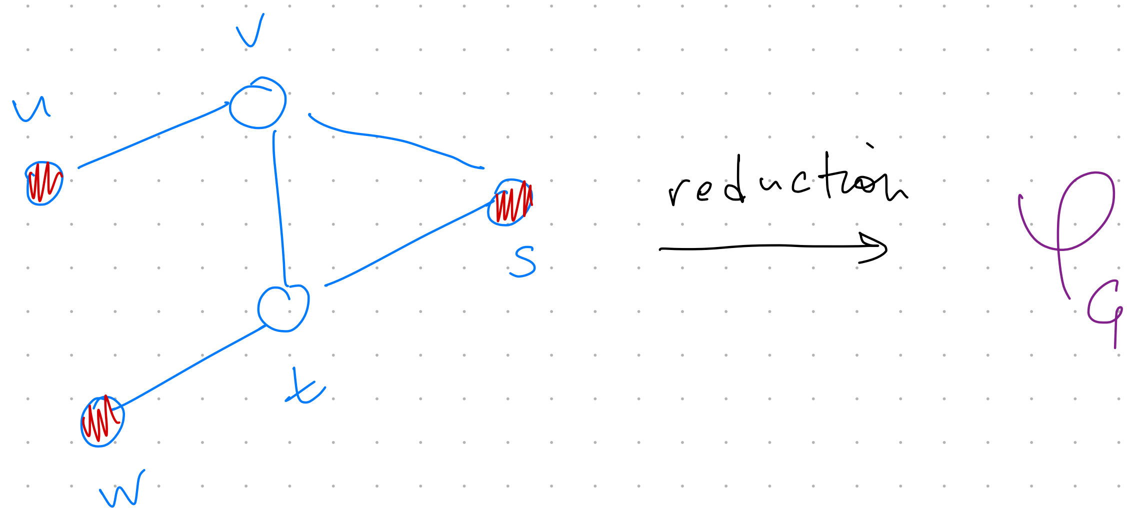
INDEPENDENT SET REDUCES TO CNF-SAT

↳ Given: Graph G, parameter k

Find: A subset $S \subseteq V$ of vertices $|S| \geq k$

such that no two vertices $u, v \in S$

share an edge $(u,v) \in E$

$G =$ 

φ_G satisfiable

$\Longleftrightarrow$

G has INDSET $\geq k$

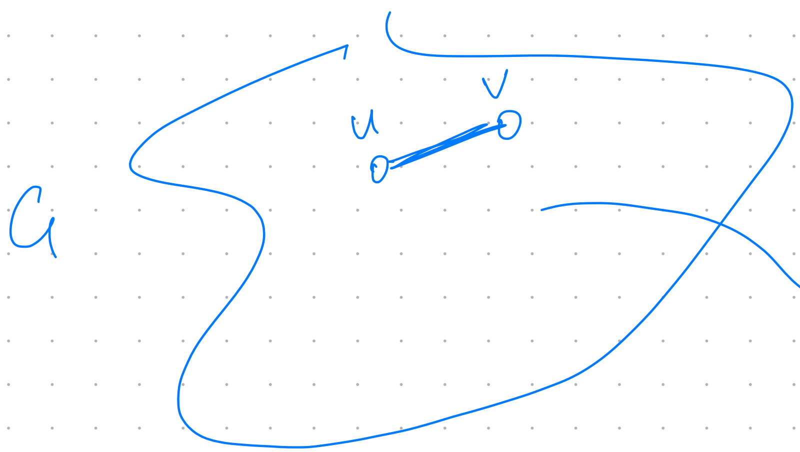
INDEPENDENT SET REDUCES TO CNF-SAT

↳ Given: Graph G, parameter k

Find: A subset $S \subseteq V$ of vertices $|S| \geq k$

such that no two vertices $u, v \in S$

share an edge $(u,v) \in E$



$\forall (u,v) \in E$

$\neg(u \in S) \vee \neg(v \in S)$

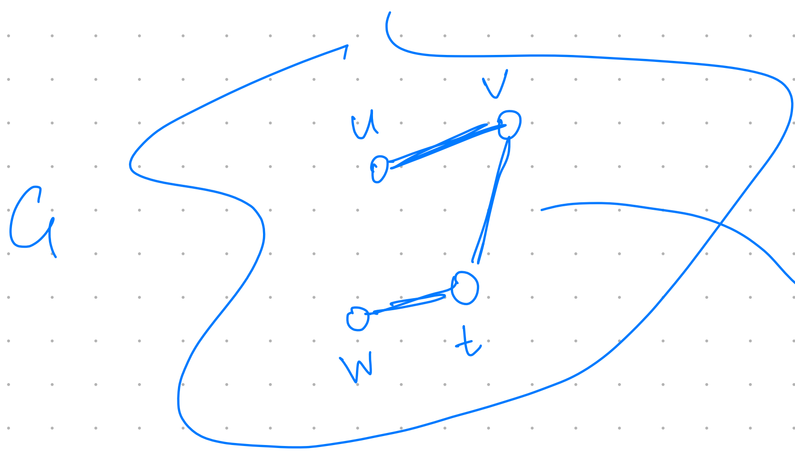
INDEPENDENT SET REDUCES TO CNF-SAT

↳ Given: Graph G, parameter k

Find: A subset $S \subseteq V$ of vertices $|S| \geq k$

such that no two vertices $u, v \in S$

share an edge $(u,v) \in E$



$\forall (u,v) \in E$

$$\neg\underbrace{(u \in S)}_{x_u} \vee \neg\underbrace{(v \in S)}_{x_v}$$

$$(\neg x_u \vee \neg x_v) \wedge (\neg x_v \vee \neg x_t) \wedge (\neg x_w \vee \neg x_t) \wedge \ldots \quad \forall e \in E$$

Given $G = (V, E)$

$$\phi_G \equiv (\neg x_{u_1} \vee \neg x_{v_1}) \wedge (\neg x_{u_2} \vee \neg x_{v_2}) \wedge \dots$$

$$\equiv \bigwedge_{(u,v) \in E} (\neg x_u \vee \neg x_v)$$

Given $G = (V, E)$

$$\phi_G \equiv (\neg x_{u_1} \vee \neg x_{v_1}) \wedge (\neg x_{u_2} \vee \neg x_{v_2}) \wedge \cdots$$

$$\equiv \bigwedge_{(u,v) \in E} (\neg x_u \vee \neg x_v)$$

Claim. ϕ_G is satisfiable iff G has an independent set.

Given $G = (V, E)$

$$\phi_G \equiv (\neg x_{u_1} \vee \neg x_{v_1}) \wedge (\neg x_{u_2} \vee \neg x_{v_2}) \wedge \cdots$$

$$\equiv \bigwedge_{(u,v) \in E} (\neg x_u \vee \neg x_v)$$

Claim. ϕ_G is satisfiable iff G has an independent set.

Problem?

INDEPENDENT SET REDUCES TO CNF-SAT

↳ Given: Graph G, parameter k

Find: A subset $S \subseteq V$ of vertices $|S| \geq k$

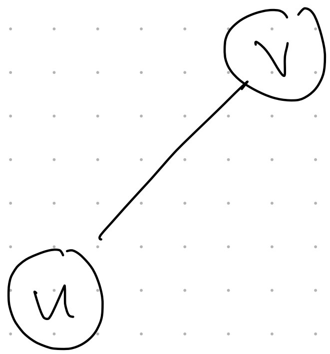
such that no two vertices $u, v \in S$

share an edge $(u,v) \in E$

Need some mechanism to count to k!

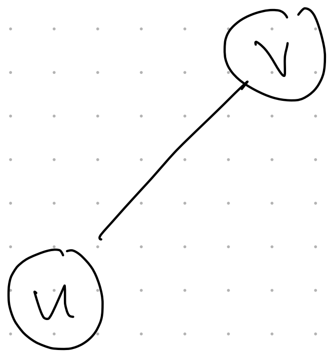
Otherwise $S = \emptyset$, i.e. $\vec{a} = \vec{0}$ satisfies φ_G

At most k vertices in S.



$X_u^{(1)} = 1 \iff$ u is the <u>first</u> vertex in S

At most k vertices in S.

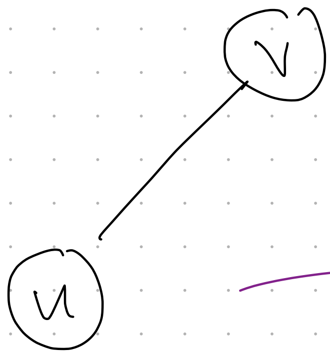


Idea. Order the vertices in $S \subseteq V$.

$X_u^{(1)} = 1 \iff u$ is the first vertex in S

At most k vertices in S.

<u>Idea</u>. Order the vertices in $S \subseteq V$.



$$\underbrace{x_u^{(1)} \quad x_u^{(2)} \quad \cdots \quad x_u^{(k)}}_{\text{k variables per vertex}}$$

$$x_u^{(i)} = 1 \iff u \text{ is the } i^{th} \text{ vertex in } S$$

Constraints

$$
\begin{array}{cccc}
X_1^{(1)} & X_1^{(2)} & \cdots & X_1^{(k)} \\
X_2^{(1)} & X_2^{(2)} & \cdots & X_2^{(k)} \\
\vdots & & & \\
X_n^{(1)} & X_n^{(2)} & \cdots & X_n^{(k)}
\end{array}
$$

$$
\begin{matrix}
x_1^{(1)} & x_1^{(2)} & \cdots & x_1^{(k)} \\
x_2^{(1)} & x_2^{(2)} & \cdots & x_2^{(k)} \\
\vdots & & & \\
x_n^{(1)} & x_n^{(2)} & \cdots & x_n^{(k)}
\end{matrix}
$$

Constraints

① For each $v \in V$

↳ At most 1 $x_v^{(i)} = 1$

① For all i, j $\quad (\neg x_u^{(i)} \vee \neg x_u^{(j)})$

$$\begin{array}{cccc} x_1^{(1)} & x_1^{(2)} & \cdots & x_1^{(k)} \\ x_2^{(1)} & x_2^{(2)} & \cdots & x_2^{(k)} \\ & \vdots & & \\ x_n^{(1)} & x_n^{(2)} & \cdots & x_n^{(k)} \end{array}$$

Constraints

1. For each $v \in V$

   ↳ At most 1 $x_v^{(i)} = 1$

1. For all i, j $\quad (\neg x_u^{(i)} \vee \neg x_u^{(j)})$

$$\phi_1 = \bigwedge_{u \in V} \bigwedge_{1 \le i, j \le k} (\neg x_u^{(i)} \wedge \neg x_u^{(j)})$$

$$\begin{array}{cccc} X_1^{(1)} & X_1^{(2)} & \cdots & X_1^{(k)} \\ X_2^{(1)} & X_2^{(2)} & \cdots & X_2^{(k)} \\ & \vdots & & \\ X_n^{(1)} & X_n^{(2)} & \cdots & X_n^{(k)} \end{array}$$

Constraints

1. For each $v \in V$

   ↳ At most 1 $x_v^{(i)} = 1$

2. For each $1 \le i \le k$

   ↳ Exactly 1 $x_v^{(i)} = 1$

For each i

$$\left(x_1^{(i)} \lor x_2^{(i)} \lor x_3^{(i)} \cdots \lor x_n^{(i)} \right)$$

At least one $u \in S$ is the i^{th} vertex

$$\begin{matrix} X_1^{(1)} & X_1^{(2)} & \cdots & X_1^{(k)} \\ X_2^{(1)} & X_2^{(2)} & \cdots & X_2^{(k)} \\ \vdots & & & \\ X_n^{(1)} & X_n^{(2)} & \cdots & X_n^{(k)} \end{matrix}$$

Constraints

1. For each $v \in V$
   $\hookrightarrow$ At most 1 $x_v^{(i)} = 1$

2. For each $1 \le i \le k$
   $\hookrightarrow$ Exactly 1 $x_v^{(i)} = 1$

For each i

$$\left(x_1^{(i)} \vee x_2^{(i)} \vee x_3^{(i)} \cdots \vee x_n^{(i)} \right)$$

For each u, v

$$\left(\neg x_u^{(i)} \vee \neg x_v^{(i)} \right)$$

At most 1 $u \in S$ is the i^{th} vertex

$$
\begin{array}{cccc}
X_1^{(1)} & X_1^{(2)} & \cdots & X_1^{(k)} \\
X_2^{(1)} & X_2^{(2)} & \cdots & X_2^{(k)} \\
\vdots & & \vdots & \\
X_n^{(1)} & X_n^{(2)} & \cdots & X_n^{(k)}
\end{array}
$$

Constraints

① For each $v \in V$

↳ At most 1 $x_v^{(i)} = 1$

② For each $1 \le i \le k$

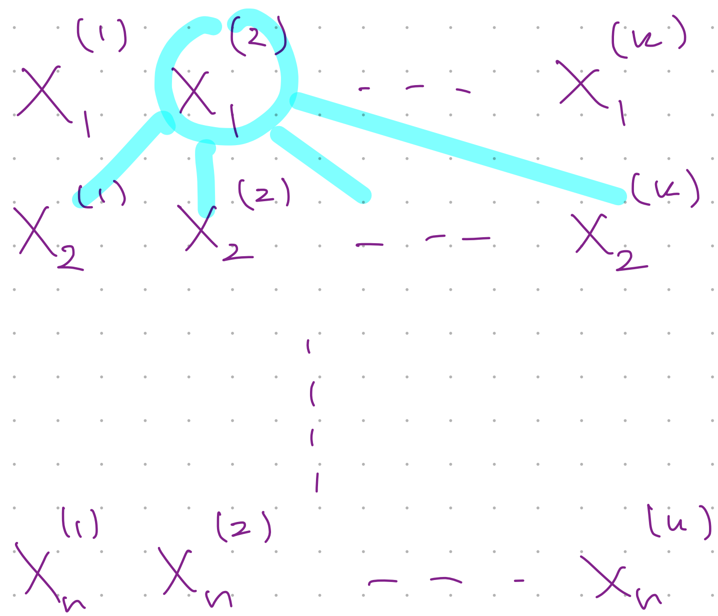
↳ Exactly 1 $x_v^{(i)} = 1$

For each i

$$(x_1^{(i)} \vee x_2^{(i)} \vee x_3^{(i)} \cdots \vee x_n^{(i)})$$

For each u, v $\quad (\neg x_u^{(i)} \vee \neg x_v^{(i)})$

$$\phi_2 \equiv \bigwedge_{1 \le i \le k} (x_1^{(i)} \vee x_2^{(i)} \vee \cdots \vee x_n^{(i)}) \wedge \bigwedge_{\substack{u \in V \\ v \in V}} (\neg x_u^{(i)} \vee \neg x_v^{(i)})$$



Constraints

① For each $v \in V$

$\hookrightarrow$ At most 1 $x_v^{(i)} = 1$

② For each $1 \le i \le k$

$\hookrightarrow$ Exactly 1 $x_v^{(i)} = 1$

③ For $(u,v) \in E$ for all i,j.

$\hookrightarrow$ $\neg x_u^{(i)} \vee \neg x_v^{(j)}$

ORIGINAL INDEPENDET SET CONSTRAINTS

$$\phi_{③} = \bigwedge_{(u,v) \in E} \; \bigwedge_{1 \le i,j \le k} \left(\neg x_u^{(i)} \vee \neg x_v^{(j)} \right)$$

G has an independent set S of cardinality $\geq k$

$$\Longleftrightarrow$$

G has an independent set

$$S = \{u^{(1)}, u^{(2)}, \dots, u^{(k)}\}$$

$$\Longleftrightarrow$$

$\phi_1 \wedge \phi_2 \wedge \phi_3$ is <u>satisfiable</u>

G has an independent set S of cardinality $\geq k$

$$\Longleftrightarrow$$

G has an independent set

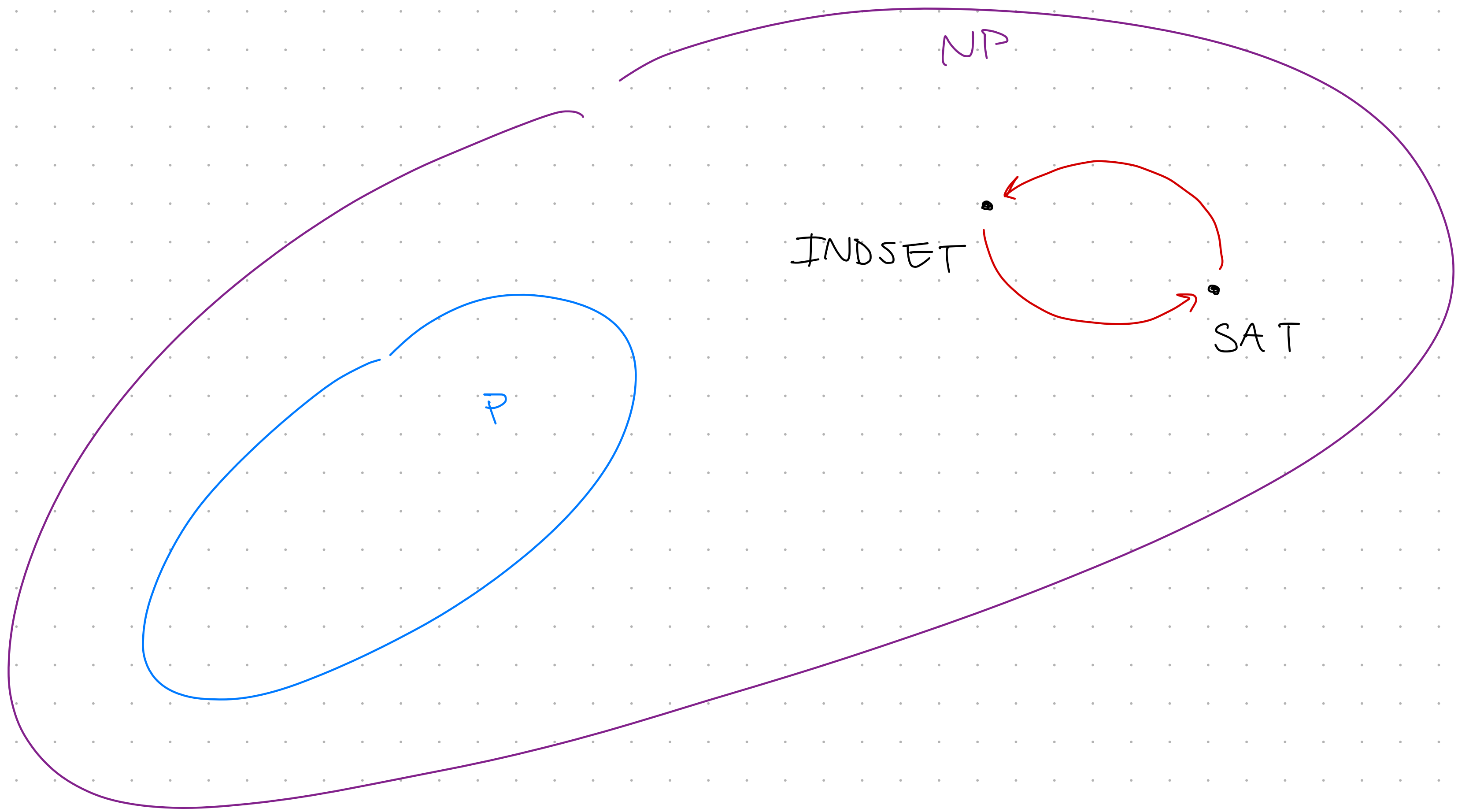
$$S = \{u^{(1)}, u^{(2)}, \ldots, u^{(k)}\}$$

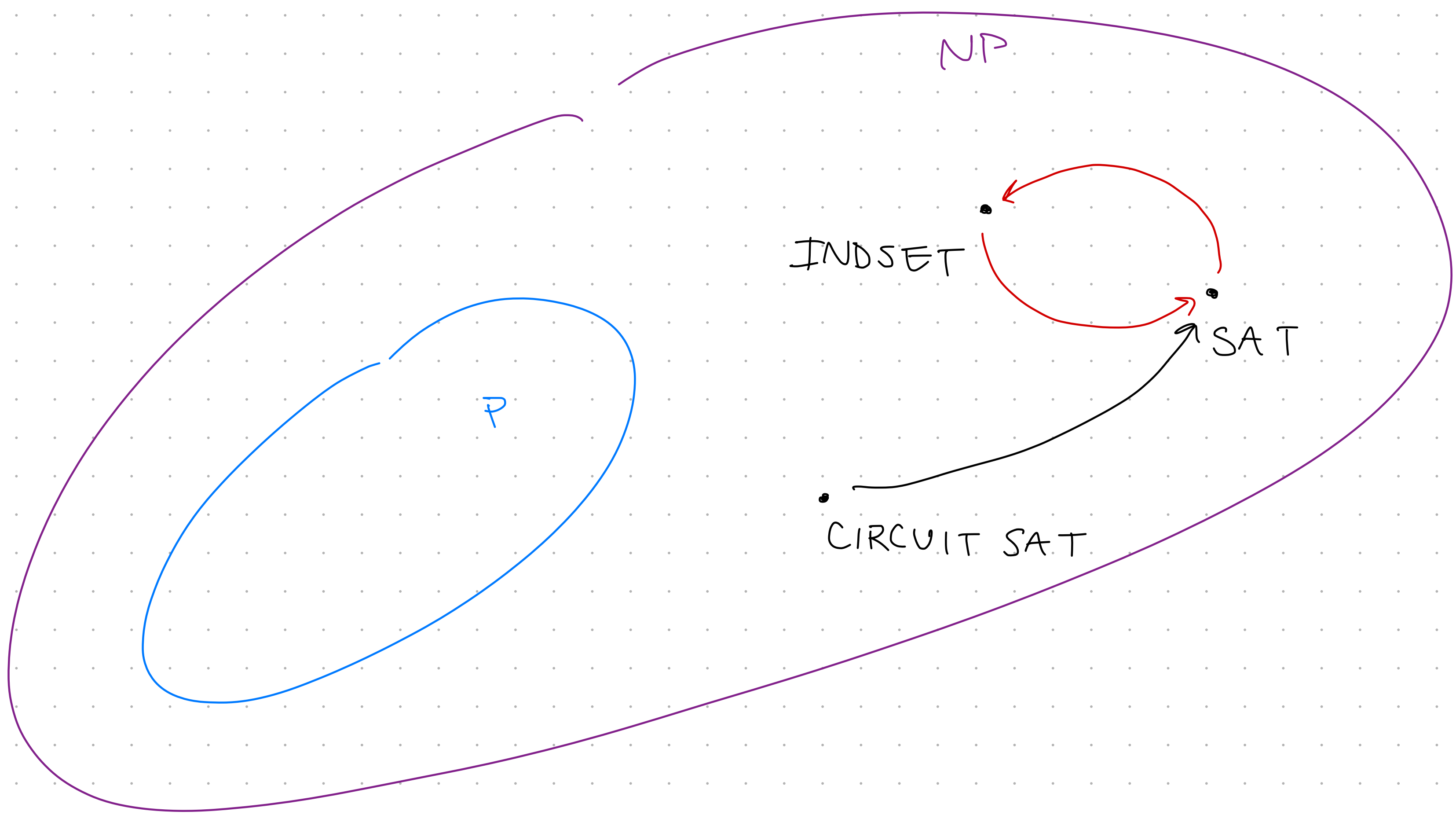
$$\Longleftrightarrow$$

$$\underbrace{\phi_1 \wedge \phi_2 \wedge \phi_3}$$ is satisfiable

- polynomial-sized CNF
- each clause can be generated in poly-time.

$\Longrightarrow$ IND SET $\leq_p$ CNF-SAT


NP
INDSET
SAT
P



Theorem (Cook-Levin).

Every problem in NP reduces to 3SAT in polynomial-time.

CIRCUIT-SAT $\leq_p$ 3SAT

<u>Given</u>: Logical Circuit $C : \{0,1\}^n \longrightarrow \{0,1\}$

<u>Question</u>.

Does there exist $x \in \{0,1\}^n$

s.t. $C(x) = 1$?

CIRCUIT-SAT $\leq_p$ 3SAT

Given: Logical Circuit $C : \{0,1\}^n \longrightarrow \{0,1\}$

Question.

Does there exist $x \in \{0,1\}^n$

s.t. $C(x) = 1$?

Note. CIRCUIT SAT $\leq_p$ 3SAT is a key step in proof of Cook-Levin Theorem!

Intuition. Logical Circuits can implement any algorithm.

CIRCUIT-SAT $\leq_p$ 3SAT

Given: Logical Circuit $C : \{0,1\}^n \longrightarrow \{0,1\}$

Question. Does there exist $x \in \{0,1\}^n$ s.t. $C(x) = 1$?

Note. CIRCUIT SAT $\leq_p$ 3SAT is a key step in proof of Cook-Levin Theorem!

Intuition. Logical Circuits can implement any algorithm.

Including poly-time Verifier for any NP problem!

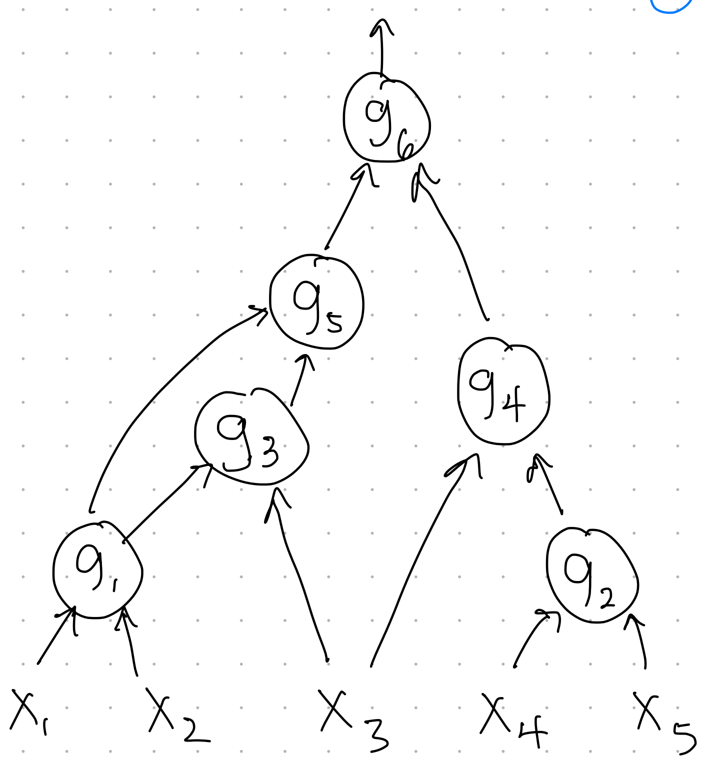
Circuits.

* Represented as a DAG
* Vertices ≡ "Gates"
* Edges ≡ "Wires"

// Each gate computes a boolean fn. on 2-variables

→ n total input wires to circuit

→ Output determined by evaluating each gate from bottom to top.



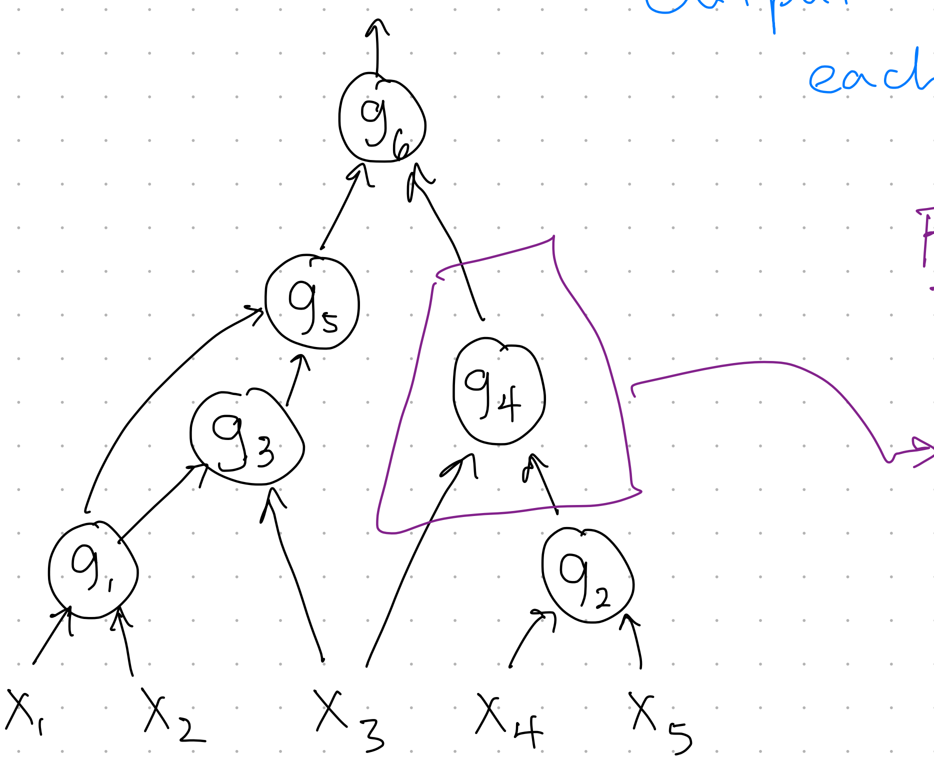
Circuits.

* Represented as a DAG
* Vertices $\equiv$ "Gates"
* Edges $\equiv$ "Wires"

// Each gate computes a boolean fn. on 2-variables

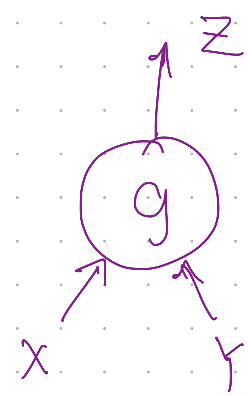
→ n total input wires to circuit

→ Output determined by evaluating each gate from bottom to top.



Reduction idea

For each gate

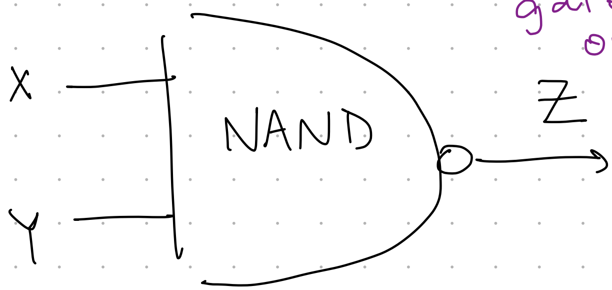


Check correctness

$$z \longleftrightarrow g(x, y)$$

Verify each gate

gate input



gate output

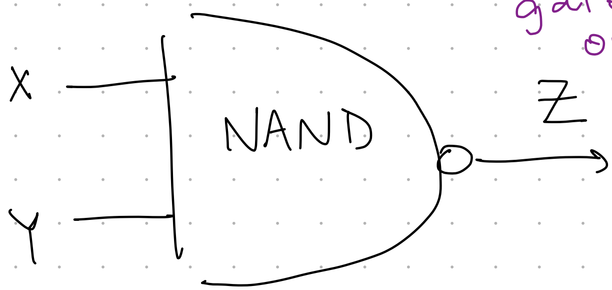
"Negated AND"

X	Y	Z = NAND(X, Y)
0	0	1
1	0	1
0	1	1
1	1	0

Note: NAND is Complete

Verify each gate

gate input



gate output

"Negated AND"

X	Y	Z = NAND(X, Y)
0	0	1
1	0	1
0	1	1
1	1	0

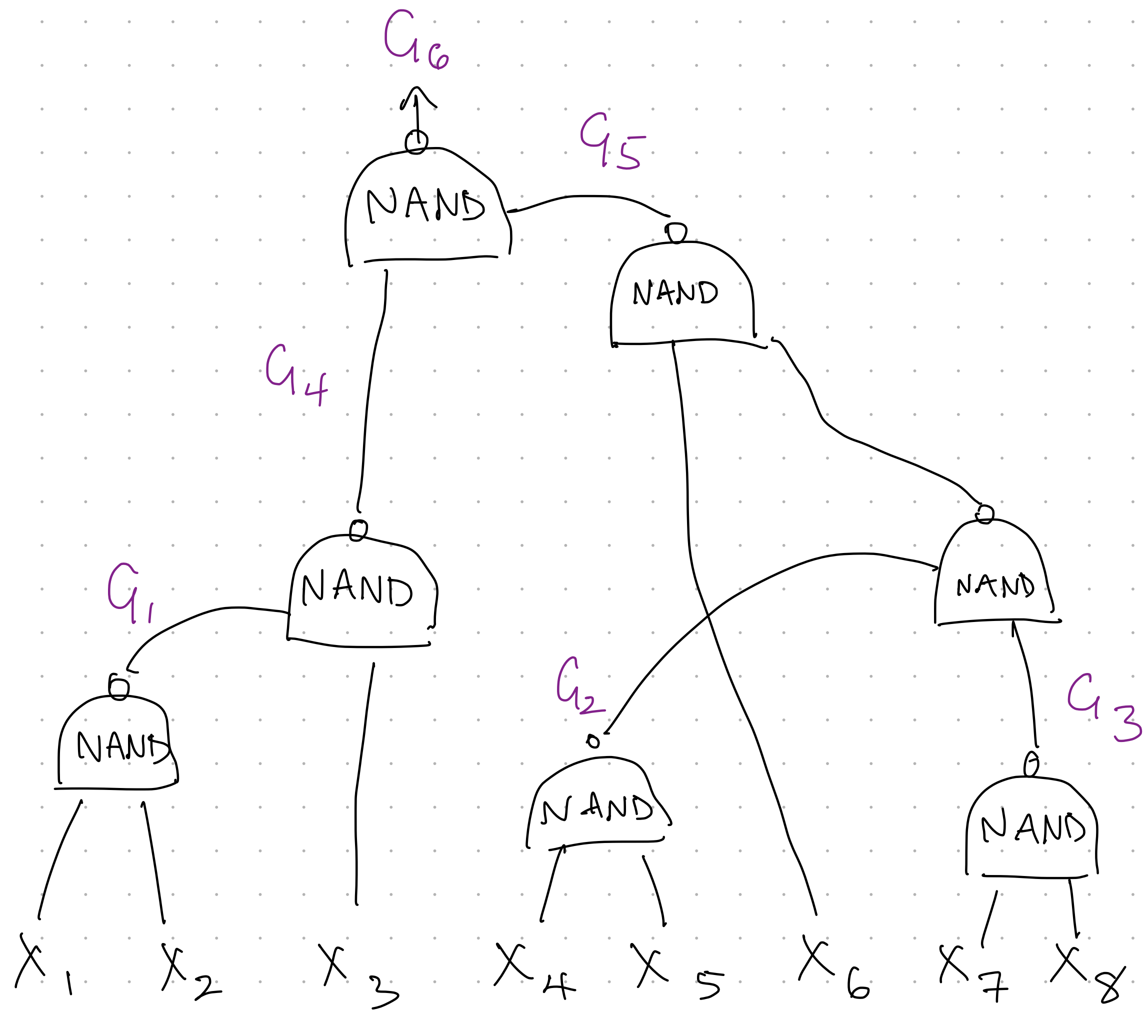
Note: NAND is Complete

GATE GADGET. $\longrightarrow$ Set of clause satisfied by any X, Y, Z s.t. Z = NAND(X, Y)

$$Z \leftrightarrow \neg(X \wedge Y)$$

$$\Leftrightarrow \quad \underbrace{Z \to \neg(X \wedge Y)}_{(\neg Z \vee \neg X \vee \neg Y)} \quad \wedge \quad \underbrace{\neg Z \to (X \wedge Y)}_{(Z \vee X) \wedge (Z \vee Y)}$$

$$(\neg Z \vee \neg X \vee \neg Y) \wedge (Z \vee X) \wedge (Z \vee Y)$$



poly-sized CNF satisfiable iff $\exists\ x \in \{0,1\}^8$ s.t. $C(x) = 1$.

$$\varphi_C = G_6 \wedge \Big[(\neg G_1 \vee \neg x_1 \vee \neg x_2) \wedge (G_1 \vee x_1) \wedge (G_1 \vee x_2)$$ (gate 1 gadget)

$$\wedge (\neg G_2 \vee \neg x_4 \vee \neg x_5) \wedge (G_2 \vee x_4) \wedge (G_2 \vee x_5)$$ (gate 2 gadget)

$$\vdots$$

$$\wedge (\neg G_6 \vee \neg G_4 \vee \neg G_5) \wedge (G_6 \vee G_4) \wedge (G_6 \vee G_5) \Big]$$ (gate 6 gadget)