CIRCUIT SAT

**Input:** A boolean circuit $C$ with $n$ boolean inputs $(x_1, \ldots, x_n)$ and one output.

**Sol:** An input assignment $x$ such that output of $C = 1$.

**Thm:** Circuit SAT is NP-complete

Mother of all NP-completeness
Thm: CircuitSAT is NP-complete

Proof: 1) CircuitSAT ∈ NP : (convince)

2) For every problem $A \in$ NP

$$= \quad A \leq_p \text{CircuitSAT}$$

Fix $A = \text{FACTORIZATION}$
**Factorization**

Input: An n bit number N
Solution: p, q > 1 s.t. p · q = N

**Circuit SAT**

Input: Circuit C
Solution: A satisfying assignment

Diagram:
- **Number** N
- **Circuit** for Factorization
- **ALG for Circuit SAT**
  - Solution x
  - No solution
- Verification Circuit

Symbols: p, q
Factorisation $\in \text{NP}$

Verifying Circuit $\rightarrow$

Input: $N$

Solution: $P$, $Q$
**Thm:** CIRCUIT SAT

**INPUT:** A circuit $C$

**SOL:** A satisfying assignment $\lambda$

---

$$\text{3SAT} \leq_p \text{SAT}$$

**INPUT:** A 3SAT formula

**SOL:** A satisfying assignment.

---

**Variables:** $\{x_1, \ldots, x_n\}$

AND $\{w_1, \ldots, w_m\}$ = internal wires.

**Constraints:** 1) encode each gate

2) $(w_m \lor w_m \lor \neg w_m)$
3SAT is NP-complete

1) 3SAT ∈ NP

2) Every problem in NP

\[ A \leq_p 3SAT \]

\[ \therefore \text{CircuitSAT is NP-complete} \]

\[ A \leq_p \text{Circuit SAT} \leq_p 3SAT \]

Prop: \[ A \leq_p B \text{ and } B \leq_p C \]
then \[ A \leq_p C \]
To prove $A$ is NP-complete

1) $\{\text{3SAT, INDOSE, \ldots}\}$ one of them $\leq_P A$

2) $A \in \text{NP}$
Proof: 3SAT is NP-complete.

1) If the circuit C has an assignment \( \mathcal{a} \) such that \( (G) = 1 \)

\[ \Rightarrow \exists \text{ a satisfying assignment to 3SAT formula} \]

2) Given a satisfying assignment to formula

\[ \Rightarrow \text{ find a satisfying assignment} \]
\[ w_k = w_i \land w_j \]

\[ \begin{array}{ccc}
(w_i, w_j, w_k) & 1 & 0 & 1 \\
0 & 1 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0
\end{array} \]

\[ (\overline{w_i} \lor w_j \lor \overline{w_k}) \land \\
(w_i \lor \overline{w_j} \lor \overline{w_k}) \land \\
(w_i \lor w_j \lor \overline{w_k}) \land \\
(\overline{w_i} \lor \overline{w_j} \lor w_k) \]
3SAT: Input: A 3-SAT formula on variables $x_1, \ldots, x_n \in \{0,1\}$

Formula with $m$ clauses

$m$ clauses

Clause

Solution:

Goal: An assignment \{ $x_1 \rightarrow 0$, $x_2 \rightarrow 1$, \ldots \} that satisfies all clauses.
**3SAT**

**INPUT:** A 3SAT formula

**SOL:** A satisfying assignment

**INDEPENDENT SET**

**INPUT:** Graph $G = (V,E), K$

**SOL:** An independent set of size $K$

\[
(x \lor y \lor z) \land \\
(\overline{y} \lor \overline{z} \lor \overline{w}) \land \\
(\overline{w} \lor x \lor t) \land \\
\text{Satisfying assignment}
\]

\[
x = 1, y = 0, z = 0, w = 1, t = 0
\]