Def: Decision problem $Q$ is in $NP$ if

1. there is a polynomial time algorithm $VCI(I, X)$ s.t.
   1) if $I$ is a YES-instance of $Q$, then $\exists X$ with $1x1$ polynomial in $I$ such that $VCI(I, X) = YES$
   2) if $I$ is a NO-instance of $Q$, then $VCI(I, X) = NO \ \forall X$

Def: problem $Q$ is $NP$-hard if $\forall Q' \leq_p Q \ \forall Q' \in NP$

Def: problem $Q$ is $NP$-complete if $Q$ is $NP$-hard and $Q \in NP$.

Def: A many-one reduction from $A$ to $B$ is a function $f$ which takes arbitrary instances of $A$ and turns them into instances of $B$ s.t.

1) if $x$ is YES in $A$ then $f(x)$ is YES in $B$
2) If \( x \) No of A \( \Rightarrow f(x) \) No of B
3) \( f \) can be computed in polytime

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

Given boolean circuit with AND, OR, NOT gates, arbitrary fanout, 1 output. Is there a way of setting inputs so output = 1?

---

3-SAT: Given a Conjunctive normal form (CNF) formula over \( x_1, \ldots, x_n \), where each AND of ORs clause has \( \leq 3 \) variables. Is there an assignment to the variables that satisfies the formula?

\[
\text{Ex: } (x_1 \lor \overline{x}_2 \lor x_4) \land (x_2 \lor x_3 \lor x_5) \land (x_1 \lor x_4 \lor \overline{x}_6)
\]

**Thm:** 3-SAT is NP-complete

**PF:** In NP: \( \checkmark \)
**NP-hard:**

**Goal:** show \( \text{Circuit-SAT} \leq \text{3-SAT} \)

**First:** Change \( \text{Circuit-SAT} \) to only \( \text{NAND} \)

\[\begin{array}{c}
\text{AND} \Rightarrow \text{NAND} \\
\text{OR} \Rightarrow \text{NAND} \\
\text{XOR} \Rightarrow \text{NAND} \\
\end{array}\]

So given circuit \( C \), first transform it to only NANDs \( C' \)

**Input:** list of gates

\[g_1 = \text{NAND}(x_0, x_3) \quad g_3 = \text{NAND}(x_0, 1)\]
\[g_2 = \text{NAND}(x_0, x_4) \quad g_4 = \text{NAND}(x_5, x_2)\]

output gate \( g_m \)

\( n \) inputs \( x_0, \ldots, x_n \)

\( m \) gates \( g_0, \ldots, g_m \)
Many-one reduction to 3-SAT:
need to build 3CNF formula which preserves satisfiability of circuit

**Variables:**

\[ y_1, y_2, \ldots, y_n, y_{n+1}, y_{n+2}, \ldots, y_{n+m} \]

\[ \text{correspond to } x_i \text{'s} \quad \text{correspond to } g_i \text{'s} \]

**Clauses:**

Replace every

\[ y_i = \text{NAND}(y_j, y_k) \]

with:

\[(y_i \lor y_j \lor y_k) \quad \text{if } y_j = 0, y_k = 0 \Rightarrow y_i = 1
   \]

\[\land (y_i \lor \overline{y_j} \lor y_k) \quad \text{if } y_j = 1, y_k = 0 \Rightarrow y_i = 1
   \]

\[\land (y_i \lor y_j \lor \overline{y_k}) \quad \text{if } y_j = 0, y_k = 0 \Rightarrow y_i = 1
   \]

\[\land (\overline{y_i} \lor \overline{y_j} \lor \overline{y_k}) \quad \text{if } y_j = 1, y_k = 1 \Rightarrow y_i = 0
   \]

Add clause \((y_{n+m})\)

**Claim:** This is a many-one reduction.

**Proof:** poly-time \(\checkmark\)
Set C YES of Circuit-SAT

⇒ ∃ setting x of input s.t. \( g_m = 1 \)

⇒ ∃ assignment to \( Y_0 \ldots Y_m \) s.t.

\[
Y_i = x_i \text{ if } i \leq n \\
Y_i = g_m \text{ if } i > n
\]

All classes satisfied ⇒ \( f(C) \) YES of 3-SAT

Set \( f(C) \) YES of 3-SAT

⇒ ∃ setting \( x \) s.t. all classes satisfied

set \( x_i = Y_i \) \( \forall i \leq n \)

⇒ output of gate \( g_i = Y_i + n \) (by construction)

⇒ \( g_m = 1 \) (since \( (g_m) \) a clause)

⇒ YES of Circuit-SAT \( \checkmark \)

Graph Problems:

CLIQUE: Given \( G = (V, E) \), integer \( k \). Does \( G \) contain a clique of size \( \geq k \)?

\( S \subseteq V : \{ u \in S \land u \in S \} \land (u \neq v) \)

Then: CLIQUE is NP-complete
\textbf{NP-hard: Reduce 3-SAT to CLIQUE}

given 3-SAT instance $F$.

For every clause of $F$, create vertex for each satisfying assignment.

Edge between consistent assignments.

\textbf{Example: } $F = (x_1 \lor x_2 \lor \overline{x_4}) \land (\overline{x_3} \lor x_4) \land (\overline{x_2} \lor \overline{x_3})$ ...

Set \quad k = m
Claim: This is a many-one reduction.

poly time \(\checkmark\)

If \(F\) \(\text{YES}\) of \(3\)-SAT : \(C_k\) is not assigned

For each clause, choose vertex corresponding to \(k\).
\(\Rightarrow\) clique of size \(= m\)

If \(F\) \(\text{YES}\) of \(\text{CLIQUE}\):

\(\exists\) one vertex for each clause

\(\exists\) assignment to each variable consistent b/c clique

General method to prove \(Q\) is \(\text{NP-Complete}\):

1) Show \(Q\) is in \(\text{NP}\)

- can verify \(\text{YES}\)
- can catch false verification if \(\text{NO}\)

2) Find some \(\text{NP-hard}\) problem \(A\).

Reduce from \(A\) to \(Q\):

given instance \(I\) of \(A\), turn into
Independent set:

\[ \text{Def: } S \subseteq V \text{ independent set in } G = (V, E) \]
\[ \text{if } (u, v) \notin E \forall u, v \in S \]

**INDEPENDENT SET**: given \( G = (V, E) \), integer \( k \)

Does \( G \) have an independent set of size \( 2k \)?

**Thm**: INDEPENDENT SET is NP-complete

**Pf**: In NP: \checkmark

NP-hard:

Reduce from [CLIQUE]:

Given \( (G = (V, E), k) \) of [CLIQUE]

\[ \Rightarrow \text{ H complement of } G : \{ u, v \} \in E \iff \{ u, v \} \notin E(G) \]

\[ \Rightarrow \text{ H has IS of size } 2k \iff \]
A has clique of size $2k$

**Vertex Cover:**

**Def:** $S \subseteq V$ a vertex cover of $G = (V, E)$ if $S \cap \emptyset \neq \emptyset \subseteq E$

**Vertex Cover:** Given $G = (V, E)$, integer $k$.

Does $G$ have a vertex cover of size $\leq k$?

**Thm:** Vertex cover is NP-complete

**Pf:** In NP:

**NP-hard:**

Reduction from INDEPENDENT SET

Given $(G = (V, E), k)$ of IS

Let $(G, n-k)$ of VC.

If $G$ has IS $S$ of size $\geq k$:

$\Rightarrow V \setminus S$ a VC of size $\leq n-k$
If $\psi \in UC \ S$ of size $\leq n-k$

$\Rightarrow \psi \in IS$ of size $\geq k$