* TAUT = $\{\phi \mid$ every assignment satisfies $\phi\}$

- We don't believe TAUT $\in$ NP
- $\exists$ easily verifiable certificate when $\varphi \notin$ TAUT

coNP : $L \in$ coNP if $\bar{L} \in$ NP

$L \in$ coNP if $\exists$ poly-time algorithm A that takes two inputs s.t $\forall x \in \{0,1\}^*$

* if $x \in L$, then $\forall y \in \{0,1\}^*$ s.t $|y| = |x|^c$ & $A(x,y) = 0$

* if $x \notin L$, then $\exists y \in \{0,1\}^*$ s.t $|y| = |x|^c$ & $A(x,y) = 1$

Theorem: (1) $P \subseteq NP$

(2) $P \subseteq$ coNP

Reductions & Completeness

For two languages A, B we write $A \leq B$ if $\exists$ poly-time algorithm for A that uses subroutine calls to B

APSP $\leq$ Matrix Multiplication
(unweighted undirected)

Theorem (Cook-Levin '71)

$\forall\ L \in NP,\quad L \leq$ CIRCUIT SAT

CIRCUITSAT is NP-complete

Poly-time reductions

We say that $A \leq B$ if $\exists$ poly-time computable function $f: \{0,1\}^* \to \{0,1\}^*$ s.t

$\forall\ x \in \{0,1\}^*\quad x \in A$ iff $f(x) \in B$

NP-completeness: A language $L \subseteq \{0,1\}^*$ is NP-complete if ① $L \in NP$

② $\forall\ L' \in NP,\ L' \leq L$

Examples of reductions

(1) IND-SET = $\{ (G, k) \mid G$ has an independent set of size $\geq k \}$

CLIQUE = $\{(G, k) \mid G$ has a clique of size $\geq k \}$

IND-SET $\leq$ CLIQUE

(G, k) : $f(G, k) = (\bar{G}, k)$

G has an independent set of size $\geq k$ iff $\bar{G}$ has a clique of size $\geq k$

CLIQUE $\leq$ IND-SET

(2) IND-SET $\leq$ VC = $\{(G, k) \mid G$ has a VC of size $\leq k \}$

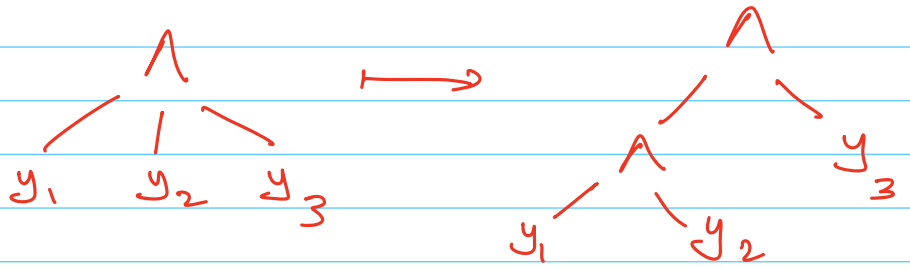
(G, k) : $f(G, k) = (G, n-k)$

If there are $\geq k$ vertices such that no edges are incident, then all the edges are incident on the remaining $n-k$ vertices. If $\exists$ VC of size $\leq n-k$, then there are no edges between the other $\geq k$ vertices

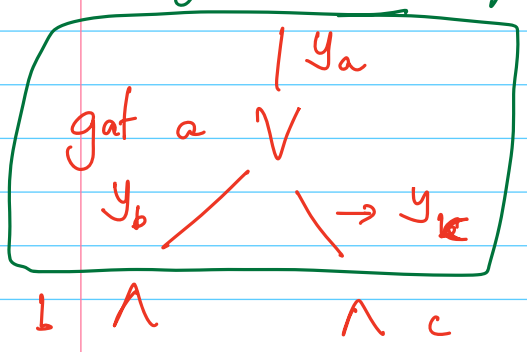
③ CIRCUITSAT $\leq$ 3SAT $= \{\varphi \mid \varphi$ is a CNF with ≤ 3 literals per clause$\}$

↓

C: Assume that every gate has fan-in ≤ 2



Every gate can be replaced by a conjunction of clauses with at most 3 literals



y_a	y_b	y_c	
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$(y_a \vee y_b \vee \bar{y}_c) \wedge (y_a \vee \bar{y}_b \vee y_c) \wedge (y_a \vee \bar{y}_b \vee \bar{y}_c)$
$\wedge (\bar{y}_a \vee y_b \vee y_c)$

↳ Do this conversion for every gate & take conjunction of all formulas to obtain φ