

The class NP is defined by "guess a witness and verify it quickly."

**SATISFIABILITY (SAT)** Instance: A Boolean formula  $\phi$  in variables  $x_1, \dots, x_n$  with connectives  $\wedge, \vee, \neg$  (or just NAND) allowed.

Question: Is there a 0-1 valued assignment  $\vec{a} = (a_1, a_2, \dots, a_n)$  that satisfies  $\phi$ , i.e. such that  $\phi(\vec{a}) = \text{true}$ ?

\* If the answer for  $\phi$  is yes, we can guess  $\vec{a}$  and quickly compute  $\phi(\vec{a})$  to verify that it comes out true.

[But note: if the answer is no, i.e. no satisfying assignment exists, all cases  $\vec{a} \in \{0,1\}^n$  we might not know until we have tried.]

Here  $|\vec{a}| = n < |\phi|$  because  $\phi$  includes symbols for  $n$  variables  $x_1, \dots, x_n$  and much else. But, OK to pretend  $|\vec{a}| = n$ .

Hence  $\text{SAT} \in \text{NP}$ .

TAU [T]  
Fact: so we can  
Defn:  
C, n-  
Examp  
If k is  
Define 3S  
In k-CNF, ver  
 $\phi(a) = 1$  means

verify it quickly."

**TAUTOLOGY (TAUT)** Inst: A Boolean formula  $\phi(x_1, \dots, x_n)$   
Ques: Is  $\phi(\vec{a}) = \text{true}$  for all  $\vec{a} \in \{0,1\}^n$ ?

Fact:  $\phi \in \text{TAUT} \Leftrightarrow \neg\phi$  is not satisfiable.  
so  $\phi \in \text{TAUT} \Leftrightarrow \neg\phi$  is satisfiable. Thus we can guess and verify for TAUT, so TAUT  $\in$  NP, so TAUT  $\in$  co-NP.

Defn:  $\phi$  is in conjunctive normal form (CNF) if  $\phi$  is a conjunction  $C_1 \wedge \dots \wedge C_m$  of clauses, where each  $C_j$  is a disjunction of literals  $x_i$  or  $\bar{x}_i$ .

Example:  $\phi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee x_4) \wedge (x_3 \vee \bar{x}_4)$ . Then  $|\phi| \approx k \cdot m$

If  $k$  is the max number of literals in any clause, then  $\phi$  is in  $k$ -CNF. ignoring  $O(\log n)$  length for variable labels  $x_1, \dots, x_n$ . Typically  $k$  is constant ( $k=3$ ) and  $m = O(n)$ , so then we really have  $|\phi| = O(n)$ , well

Define 3SAT: Inst: A  $\phi$  in 3CNF. Friday's lecture will show that 3SAT, and hence SAT, is NP-complete (under  $\leq_m$ ).  
In k-CNF, verifying Ques: Is  $\phi$  satisfiable? Note: 3SAT  $\leq_m$  SAT trivially "by restricted case". really  $\tilde{O}(n)$ .  
In k-CNF, verifying each clause, clearly  $O(m) = O(n)$  time.  $\therefore 3\text{SAT} \in \text{NLIN} = \text{TIME}[O(n)]$ .

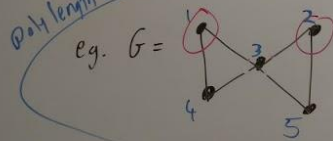
Diagram: A diamond-shaped graph with SAT at the top and TAUT at the top right. Below SAT is a diamond labeled NP. Below TAUT is a diamond labeled co-NP. A diamond labeled P is at the bottom, connected to both NP and co-NP.

Other Problems in NP: Big  $\exists$  quantifier over  $2^n$  possible subsets of  $V$ . Small quantifier over at most  $n^2$  possibilities.

INDEPENDENT SET: Inst: An undirected graph  $G=(V,E)$ , an integer  $k \geq 1$ .

Question: Does there exist a subset  $S \subseteq V, |S| \geq k$ , such that no two nodes in  $S$  are connected by an edge, i.e.  $\bigwedge_{u,v \in S} \neg E(u,v)$ ?

poly length witness and can we find  $(m, n)$



eg.  $G =$  (graph diagram)  
 Answer for  $\langle G, 1 \rangle$  is yes  $S = \{3\}$  (silly but it works)  
 Answer for  $\langle G, 2 \rangle$  is yes  $S = \{1, 2\}$  (or three other possibilities)  
 Answer for  $\langle G, 3 \rangle$  is no.

Anyway,  $|S| \leq n = \text{deg } |V|$  but we sometimes pretend  $n$  is the size of  $G$ .

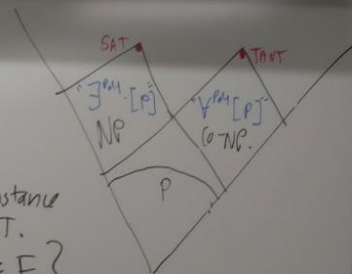
Verifying that  $S$  is independent takes time  $\approx O(|S|^2)$  going through each possible pair  $u,v$  from  $S$ . If  $G$  has  $m$  edges,  $|G|$  is better defined as  $\sim m$ , but often  $G$  is sparse meaning  $m = O(n)$  anyway.

Form is "Big  $\exists$  poly length on [poly time loop over  $u,v$ ]" so  $\in \text{NP}$ .

TAUTOLOG: Inst: A Boolean formula  $\phi(x_1, \dots, x_n)$

(TAUT)

Ques: Is  $\phi(a) = \text{true}$  for all  $a \in \{0,1\}^n$ ?  
 poly length  $a$



CLIQUE: Inst  $\langle G, k \rangle$  Same type of instance as for IND SET.

Ques: Is there  $S \subseteq V, |S| \geq k$ , such that  $\bigwedge_{u,v \in S} (u,v) \in E$ ?

$\therefore$  CLIQUE is in NP.  $\exists$  so  $|S| \leq |V|$  poly time (then  $S$  is called a clique in  $G$ )

In fact, CLIQUE is equivalent to IND SET on mapping  $G \mapsto G'$  = the complementary graph.

HAM CIRCUIT: Inst: Just a graph  $G=(V,E)$

Study: Why different from TAUT being in co-NP?

Question: Is there an ordering  $i_1, \dots, i_n$  of  $\{1, \dots, n\}$  st. for all  $j, (i_j, i_{j+1}) \in E$  and also  $(i_n, i_1) \in E$  to complete the circuit? Also in NP.