1: Verification

Definition: Given a certificate (claim of the answer), need to verify its correctness is polynomial time for Decision Problem.

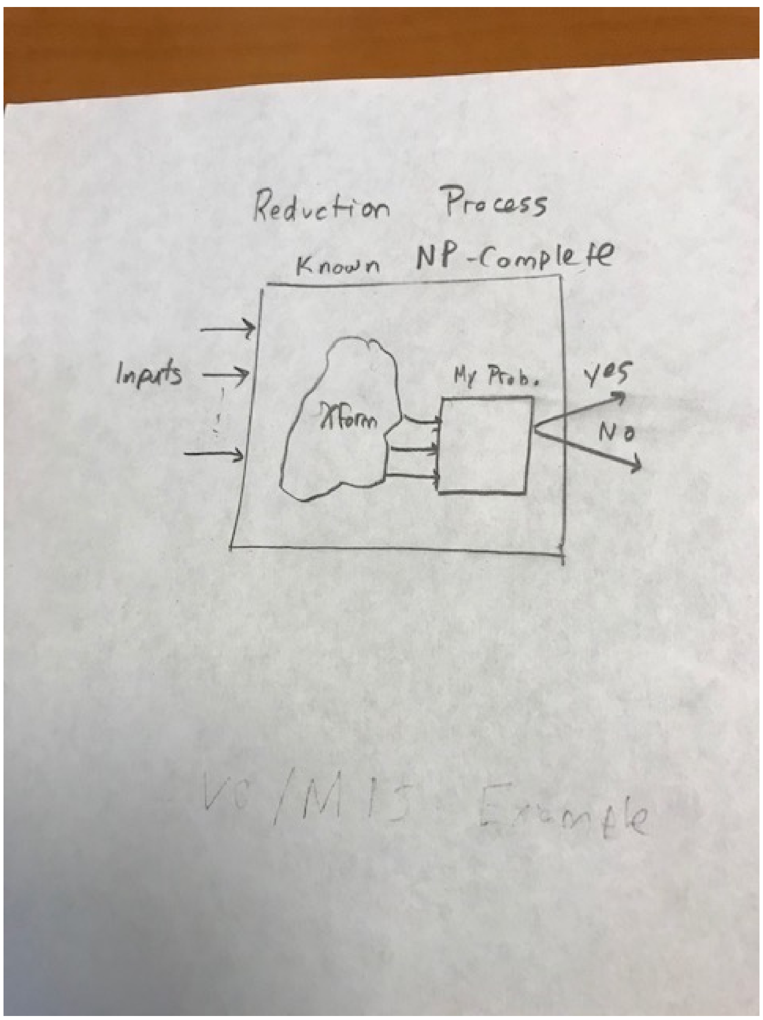
Co-NP (Complement of NP): For every certificate the answer is "No." Need to Prove that there is no certificate.

Formally speaking: A problem belongs to Co-NP if its complement is in NP.

Decision Version:

Given problem X (inputs): Is there a solution of size f(x) = k?

E.g. Shortest Path Complement version: No path exists of length k from source to destination.

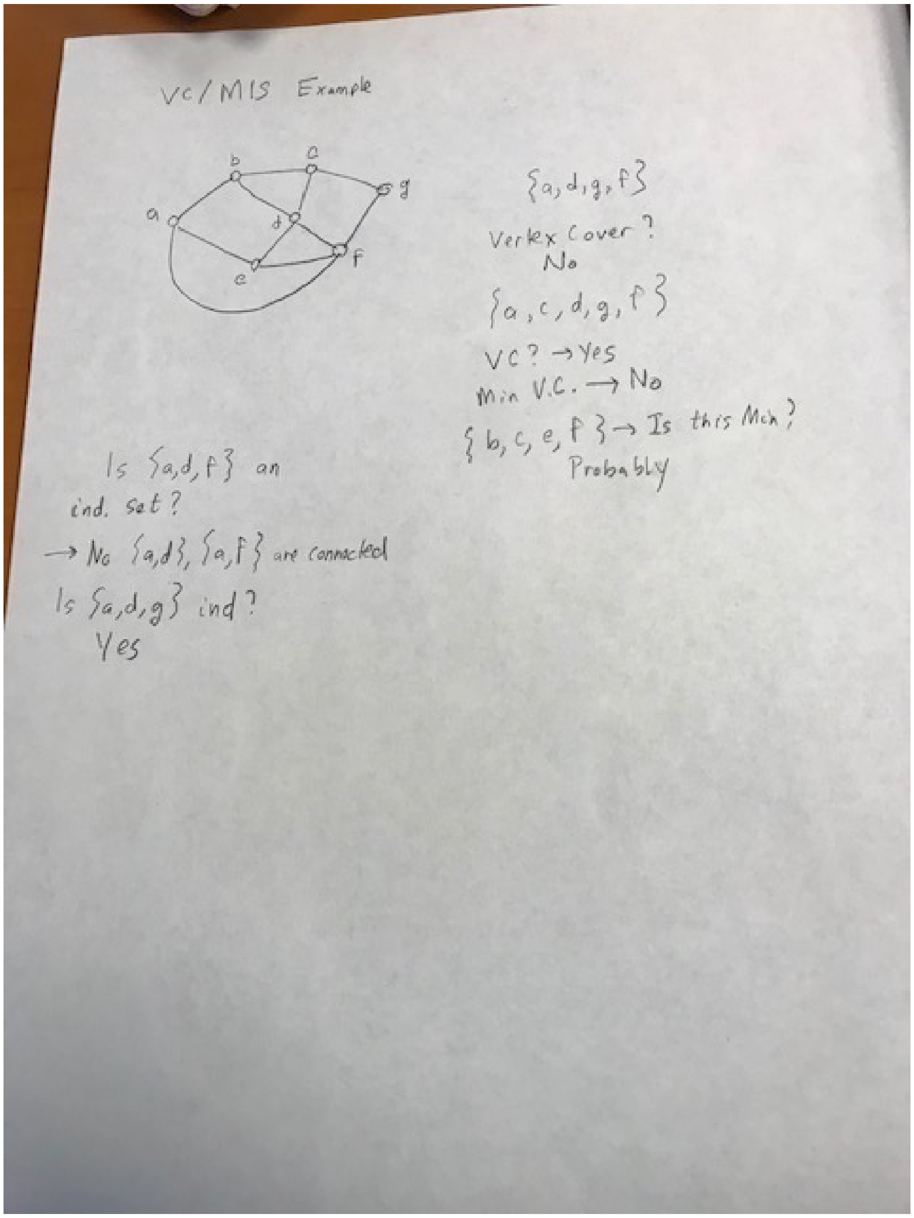


Problem in P - Can solve the optimization version in Polynomial Time:

- $P \subseteq$ Co-NP
- $P \subseteq NP$

If $P = NP \to$ Co-NP = NP = P

2: Proving NP-Complete (Reduction)



Vertex Cover

- G(V,E)
- Select the minimum number of vertices that hit all edges
- (Alternatively) Min s. s.t.
  - V(u,v) $\in$ V
  - Either $u \in S$ or $v \in S$

Maximum Independent Set

- G(V,E)
- Max $S \subseteq V$ s.t
  - $\forall u, v$
  - $u \notin S$ OR $v \notin S$
- Alternatively $\forall u \in S, v \in S$
  - (u,v) $\notin E$

2: Show Vertex Cover $\leq_p$ MIS

First Step:

Show $MIS \in NP$ (Verification)

Given an independent set (certificate), is this an independent set of size k?

Process :

- Check if $|S| = k$ $O(n)$
- $\forall (u, v) \in S$, check if (u,v) has an edge $O(n^2)$

Next step - Reduction (Use Decision Version)

MIS: Given (V,E), and k, does the graph have an independent set of size k?

Never Use Optimization Version!

2: Boolean Satisfiability $\in$ NP-Complete

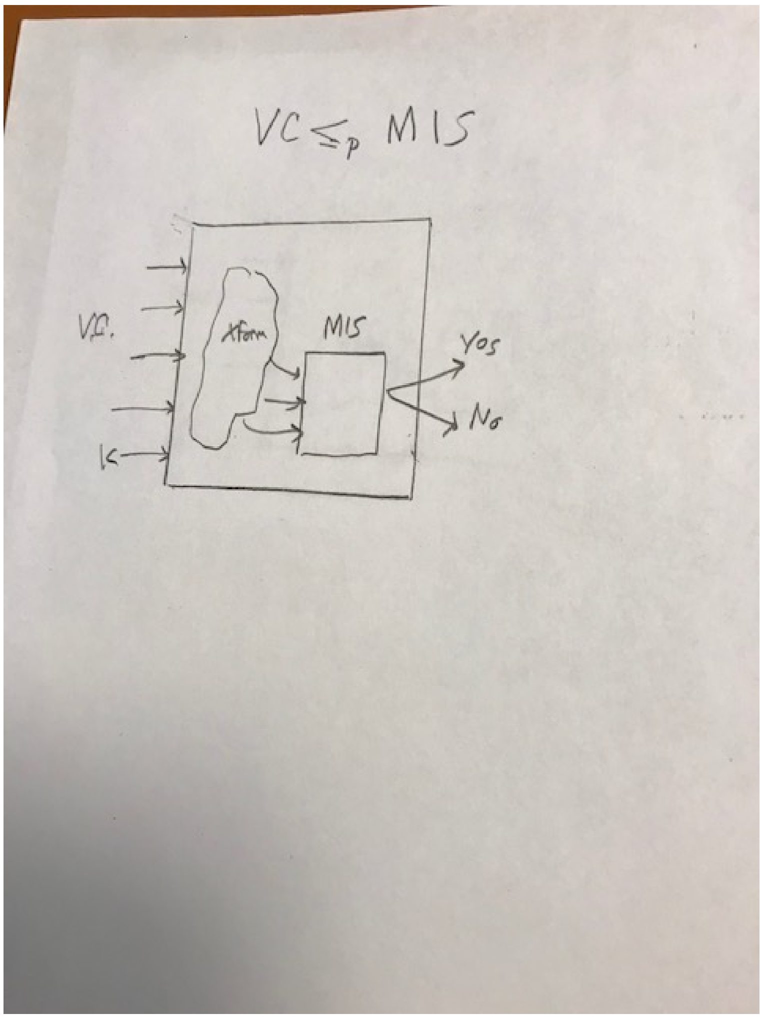
Proof: $\forall x \in NP$ Need to show:

$x \leq_P SAT$

Definition of SAT:

Given a set of variables (boolean values $v_1, v_2, ...v_n$), and a boolean statement, does there exist an assignment to $v_1, ..., v_n$ such that the statement evaluates to true?

E..g Consider $(v_1 \wedge v_2) \wedge (\bar{v_1} \wedge \bar{v_3}) \wedge (v_2 \wedge v_3)$ Does there exist an assignment to the variables that results in the formula being true?


$VC \leq_p MIS$
VC.
Xform
MIS
Yes
No
k