CSE 421 Winter 2025
Lecture 23:
NP

Nathan Brunelle

http://www.cs.uw.edu/421

Polynomial Time Reduction

Defn: We write $A \leq_P B$ iff there is an algorithm for A using a 'black box' (subroutine or method) that solves B that

- uses only a polynomial number of steps, and
- makes only a polynomial number of calls to a method for B.

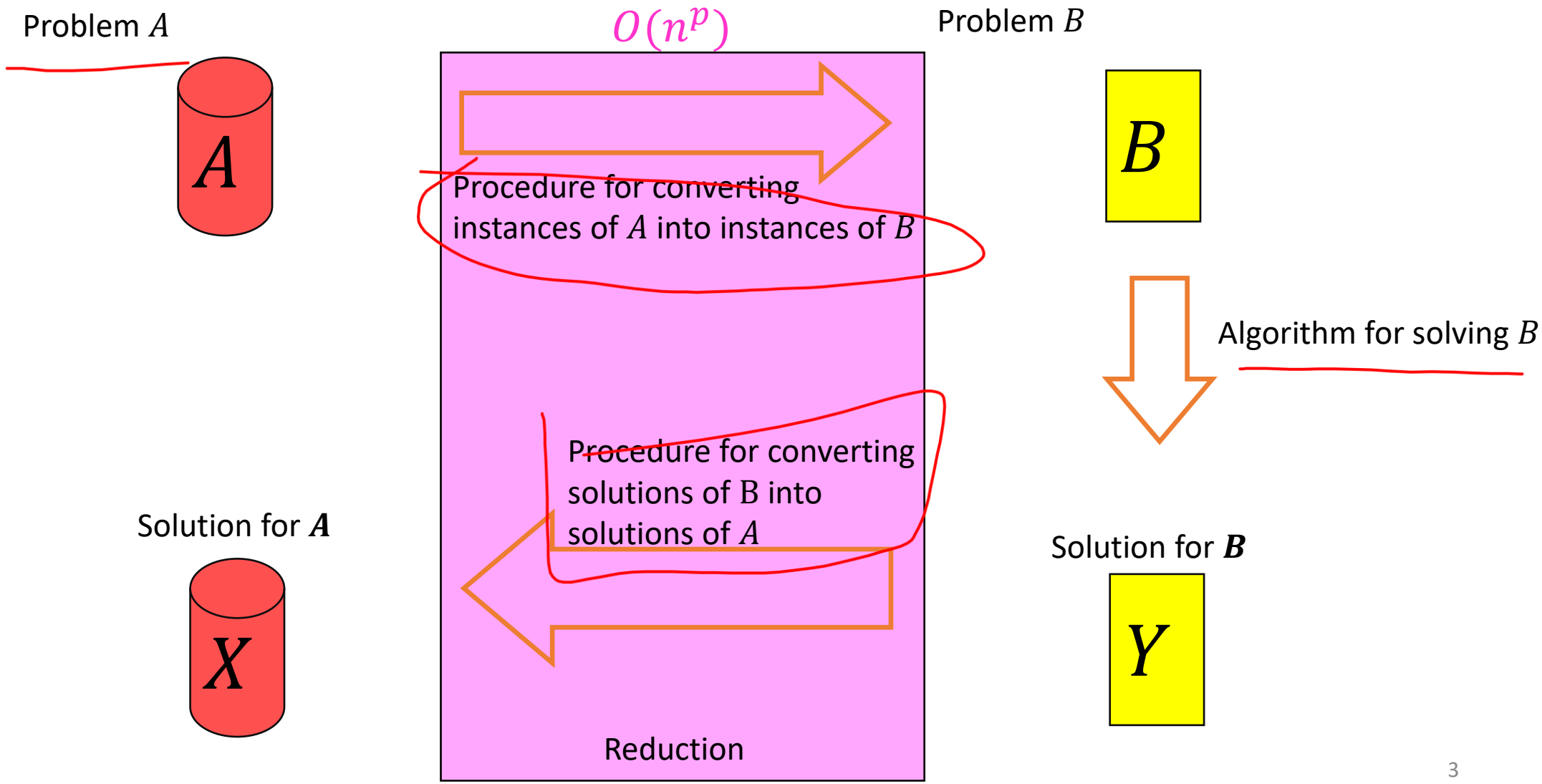
Theorem: If $A \leq_P B$ then a poly time algorithm for $B \Rightarrow$ poly time algorithm for A

Proof: Not only is the number of calls polynomial but the size of the inputs on which the calls are made is polynomial!

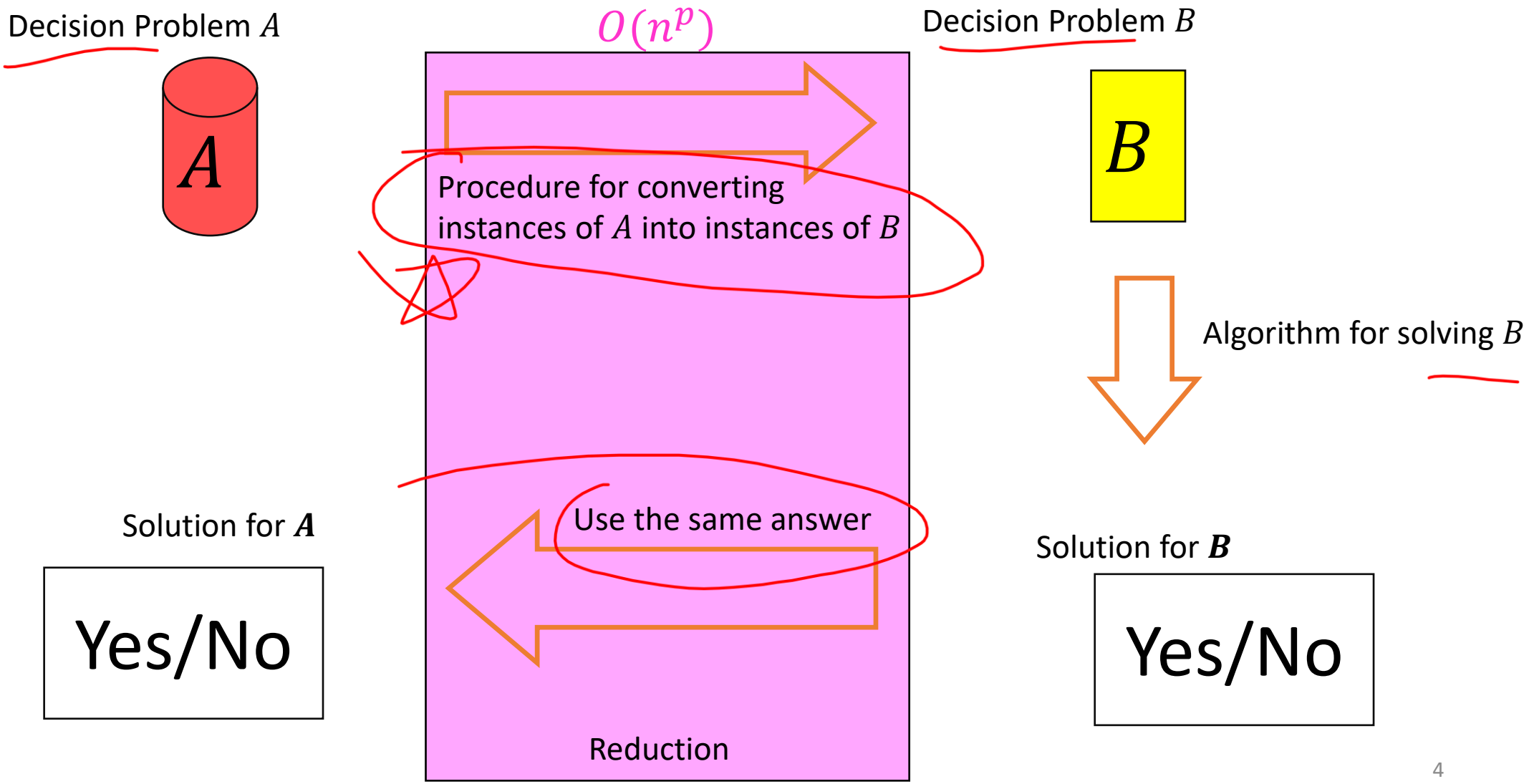
Corollary: If you can prove there is no fast algorithm for A, then that proves there is no fast algorithm for B.

Intuition for "$A \leq_P B$": "B is at least as hard* as A" *up to polynomial-time slop.

Polynomial Time Reductions



Polynomial Time Reductions (Decision Problems)



Let's do a reduction

4 steps for reducing (decision problem) A to problem B

1. Describe the reduction itself
   - i.e., the function that converts the input for A to the one for problem B.
   - i.e., describe what the top arrow in the pink box does
2. Make sure the running time would be polynomial
   - In lecture, we'll sometimes skip writing out this step.
3. Argue that if the correct answer (to the instance for A) is **YES**, then the input we produced is a **YES** instance for B.
4. Argue that if the correct answer (to the instance for A) is **NO**, then the input we produced is a **NO** instance for B.

Let's do a reduction

4 steps for reducing (decision problem) A to problem B

1. Describe the reduction itself
   - i.e., the function that converts the input for A to the one for problem B.
   - i.e., describe what the top arrow in the pink box does
2. Make sure the running time would be polynomial
   - In lecture, we'll sometimes skip writing out this step.
3. Argue that if the correct answer (to the instance for A) is **YES**, then the input we produced is a **YES** instance for B.
4. Argue that if the input we produced is a **YES** instance for B then the correct answer (to the instance for A) is **YES**.

Contrapositive

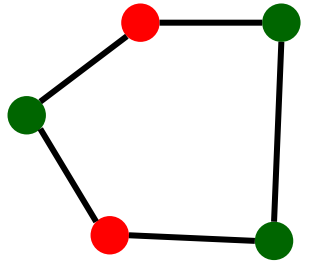
Reduce 2Color to 3Color

Defn: A undirected graph $G = (V, E)$ is k-colorable iff we can assign one of k colors to each vertex of V s.t. for $(u, v) \in E$, their colors, $\chi(u)$ and $\chi(v)$, are different.

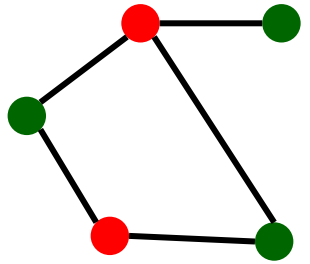
"edges are not monochromatic"

2Color: Given: an undirected graph G

Is G 2-colorable?



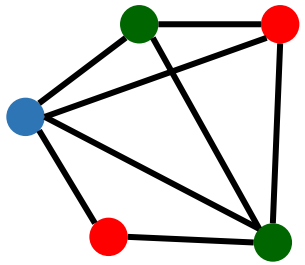
No



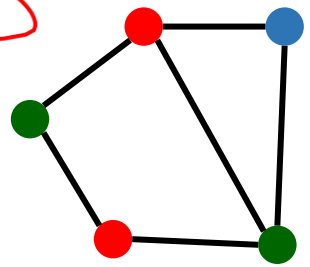
Yes

3Color: Given: an undirected graph G

Is G 3-colorable?



No



Yes

2Color $\leq_P$ 3Color

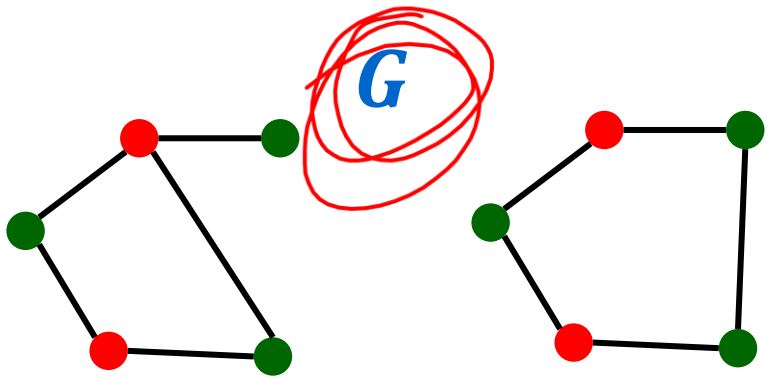
- Given a graph G figure out whether it can be 2-colored, by using an algorithm that figures out whether it can be 3-colored.

Usual outline:

- Transform G into an input for the **3Color** algorithm
- Run the **3Color** algorithm
- Use the answer from the **3Color** algorithm as the answer for G for **2Color**

Reducing 2Color to 3Color

2Color



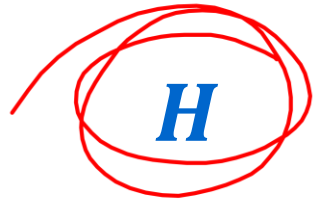
$O(n^p)$

Transform given graph G such that the output graph H was 3-colorable if and only if G was 2-colorable

Use the same answer

Reduction

3Color



Algorithm for solving 3Color

Solution for 2Color

Yes/No

Solution for 3Color

Yes/No

Reduction

If we just ask the **3Color** algorithm about G, if G is 3-colorable but not 2-colorable it will give the wrong answer because it has the 3rd color available.

Idea: Add extra vertices and edges to to **G** to force the 3rd color to be used there but not on G

Reduction f: Add one extra vertex v and attach it to **everything** in G.

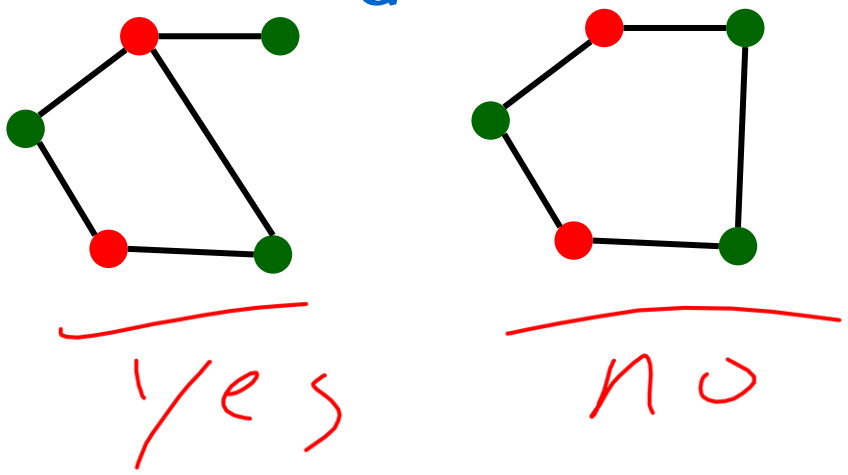
Write $H = f(G)$.

(f is polynomial time computable.)

Reducing 2Color to 3Color

2Color

$\bar{G}$



Solution for 2Color

Yes/No

$O(n^p)$

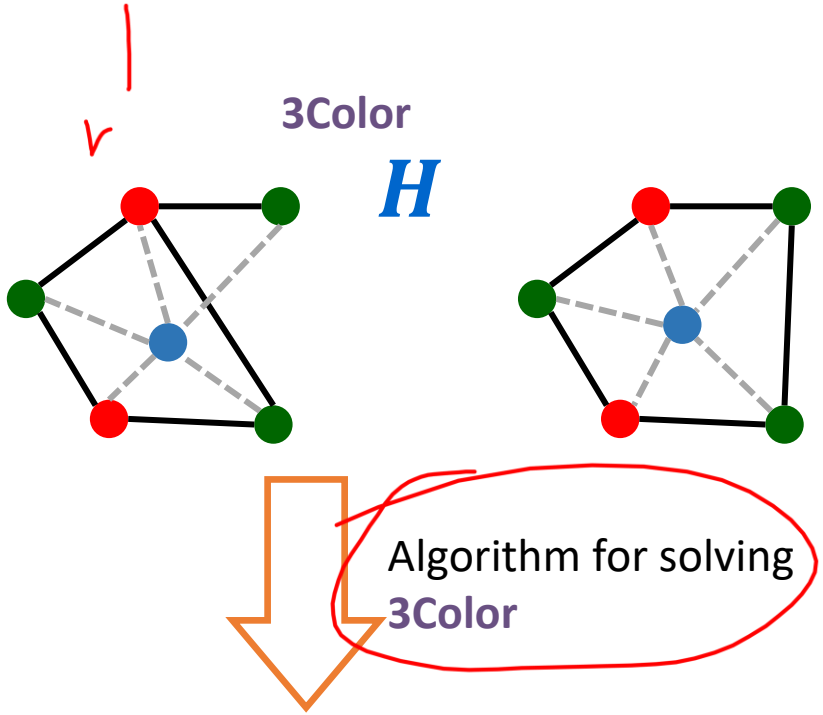
Add a new node to G, connect every node to it

Use the same answer

Reduction

3Color

H



Algorithm for solving 3Color

Solution for 3Color

Yes/No

Let's do a reduction

4 steps for reducing (decision problem) A to problem B

1. Describe the reduction itself
   - i.e., the function that converts the input for A to the one for problem B.
2. Make sure the running time would be polynomial
   - In lecture, we'll sometimes skip writing out this step.
3. Argue that if the correct answer (to the instance for A) is **YES**, then the input we produced is a **YES** instance for B.
4. Argue that if the input we produced is a **YES** instance for B then the correct answer (to the instance for A) is **YES**.

Correctness

Two statements to prove (two directions):

If G is a **YES** for **2Color** (G is 2-colorable) then H is a **YES** for **3Color** (H is 3-colorable)

Suppose G is 2-colorable: G has a 2-coloring χ so edges of G have different colored endpoints. We get a 3-coloring of H by using χ for all the copies of original vertices of G and a 3rd color for the extra vertex v. Original edges of G in H have different colored endpoints; the extra edges too. So H is 3-colorable.

If H is a **YES** for **3Color** (H is 3-colorable) then G is a **YES** for **2Color** on (G is 2-colorable)

Suppose H is 3-colorable: Consider a 3-coloring χ' of H. Consider the extra vertex v in H that was added to G. For every vertex u of G, we have an edge (u, v) so $\chi'(u) \neq \chi'(v)$. This means that every vertex u of G is colored with one of the two colors other than $\chi'(v)$. So we can use χ' as a 2-coloring of G since all those edges had different colored endpoints in H. So G is 2-colorable.

Write two separate arguments

The two directions we covered actually prove an if and only if.

To make sure you handle both directions, I **strongly** recommend:

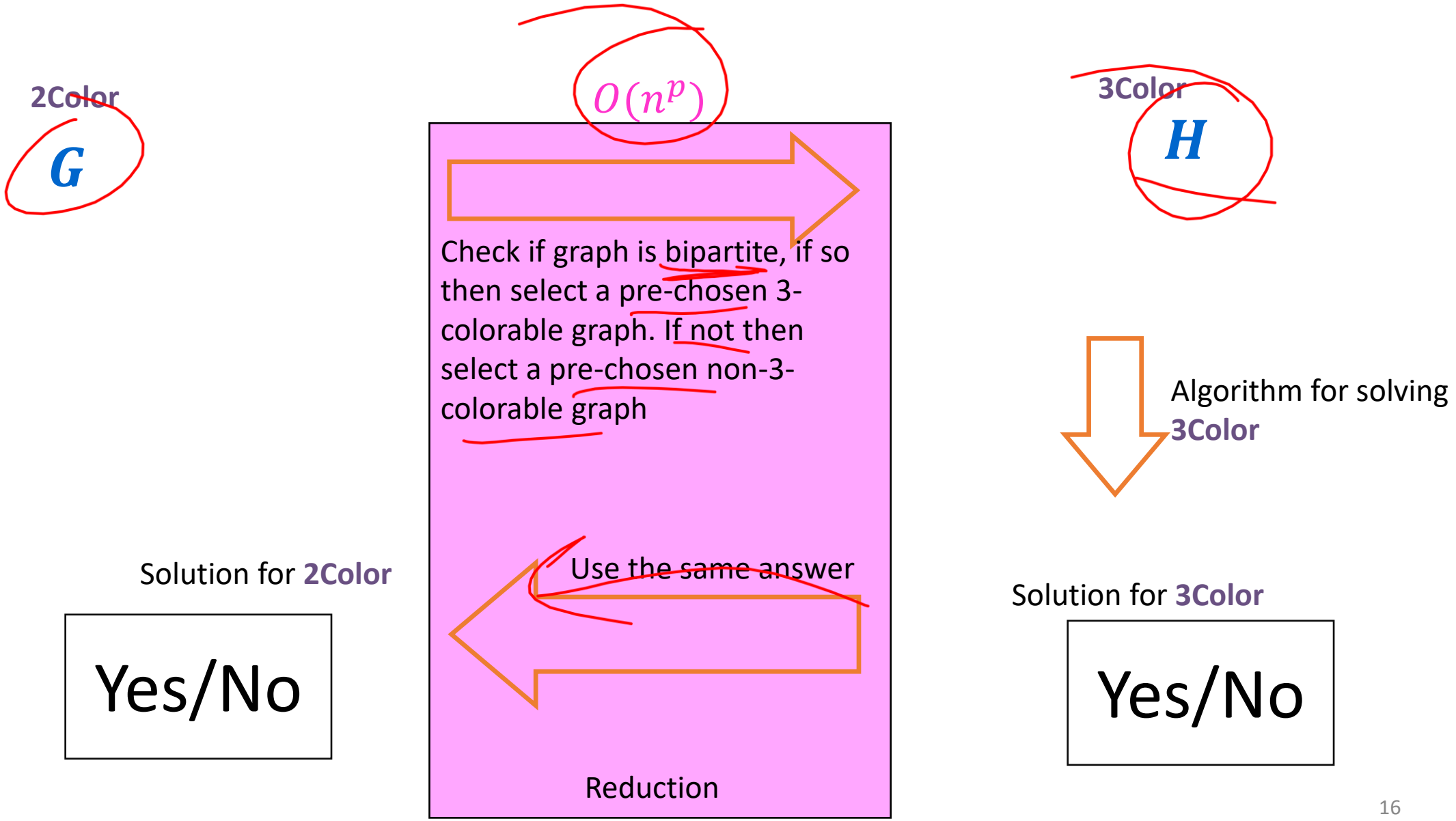
- Always do two separate proofs! (Don't try to prove both directions at once, don't refer back to the prior proof and say "for the same reason". There are usually subtle differences.)
- Don't use contradiction! (It's easy to start from the wrong spot and accidentally prove the same direction twice without realizing it.)

Another proof of 2Color $\leq_P$ 3Color

We had an $O(n+m)$ time algorithm for **2Color** based on BFS.

Simply solve the **2Color** problem without making any calls to a **3Color** method!

Reducing 2Color to 3Color



Two More Reductions

Independent-Set:

Given a graph $G = (V, E)$ and an integer k

Is there a $U \subseteq V$ with $|U| \geq k$ such that no two vertices in U are joined by an edge? (U is called an independent set.)

Clique:

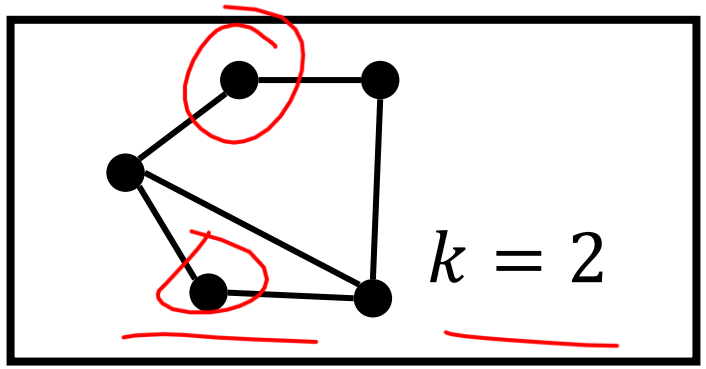
Given a graph $G = (V, E)$ and an integer k

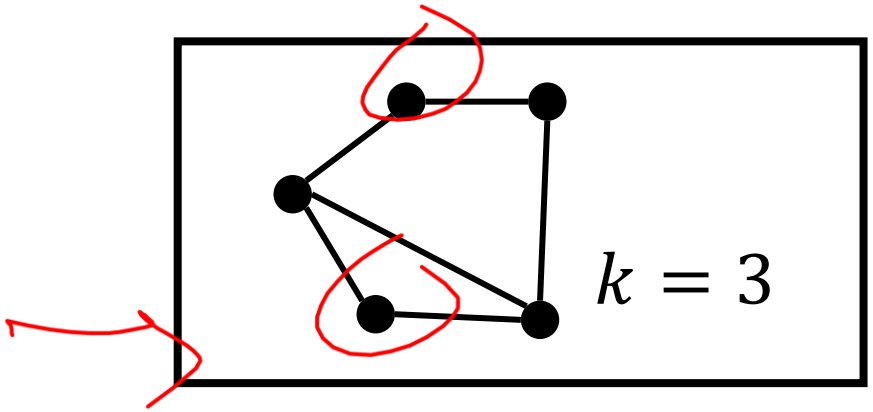
Is there a $U \subseteq V$ with $|U| \geq k$ such that every pair of vertices in U is joined by an edge? (U is called a clique.)

Claim: **Independent-Set** $\leq_P$ **Clique**

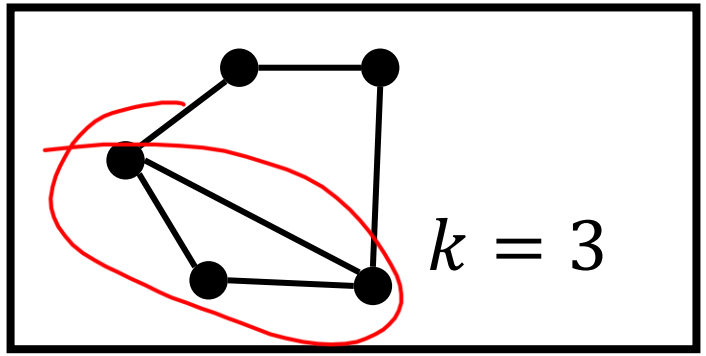
Examples

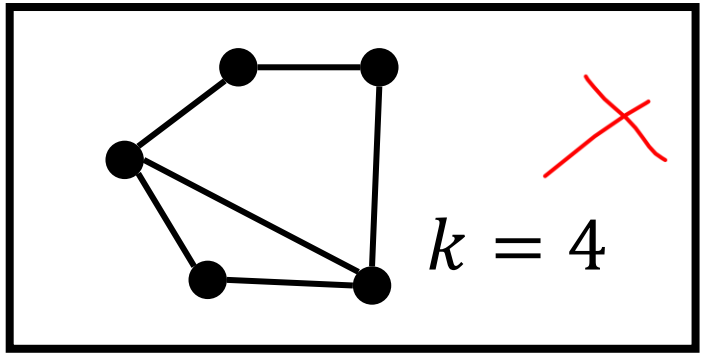
- Independent Set





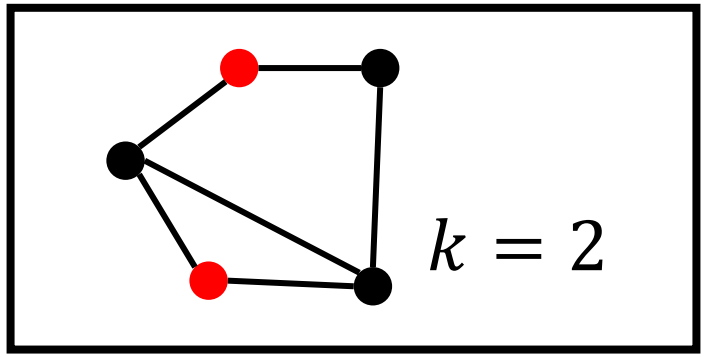
- Clique



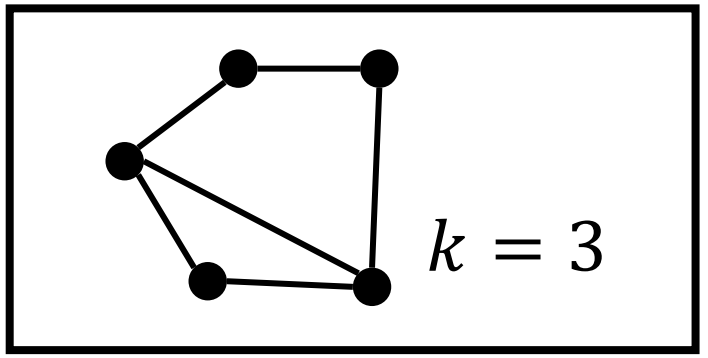


Examples

- Independent Set

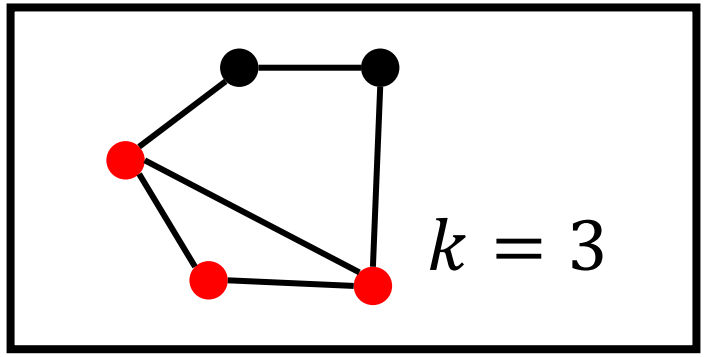


Yes

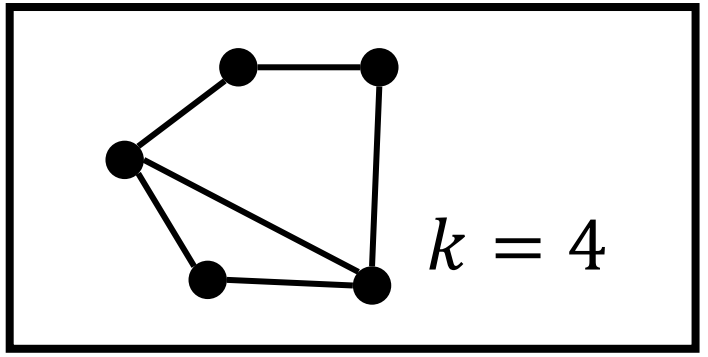


No

- Clique



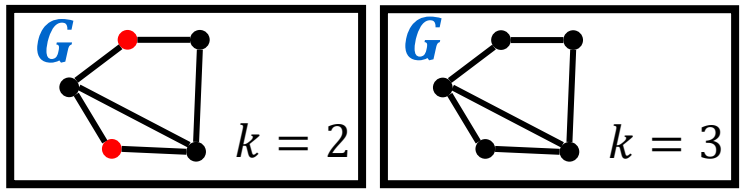
Yes



No

Reducing Independent Set to Clique

Independent Set



$O(n^p)$

Transform given graph G and number k into G' and k' such that G has an Independent Set of size k iff G' has a Clique of size k'

Use the same answer

Reduction

Clique

G', k'

Algorithm for solving **Clique**

Solution for **Independent Set**

Yes/No

Solution for **Clique**

Yes/No

Independent-Set $\leq_p$ Clique

Given:

- (G, k) as input to **Independent-Set** where $G = (V, E)$

Use function f that transforms (G, k) to (G', k') where

- $G' = (V, E')$ has the same vertices as G but E' consists of **precisely** those edges on V that are not edges of G.

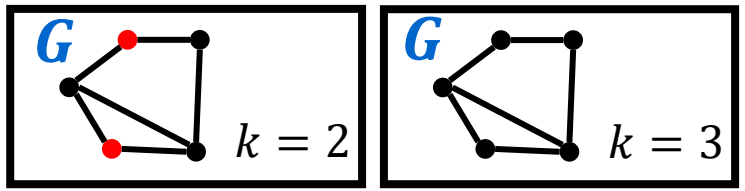
graph complement

From the definitions, U is an independent set in G

$\Leftrightarrow U$ is a clique in G'

Reducing Independent Set to Clique

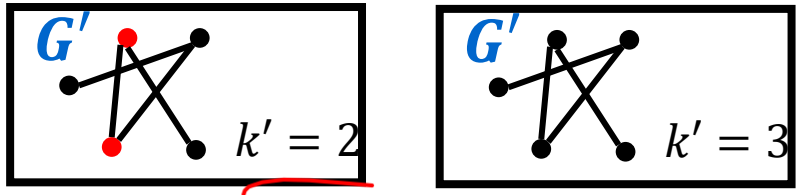
Independent Set



$O(n^p)$

Set G' to be the complement graph of G. Set $k' = k$

Clique



Algorithm for solving **Clique**

Solution for **Independent Set**

Yes/No

Use the same answer

Solution for **Clique**

Yes/No

Reduction

Clique $\leq_P$ Independent Set

Given:

- (G, k) as input to **Clique** where $G = (V, E)$

Use function f that transforms (G, k) to (G', k) where

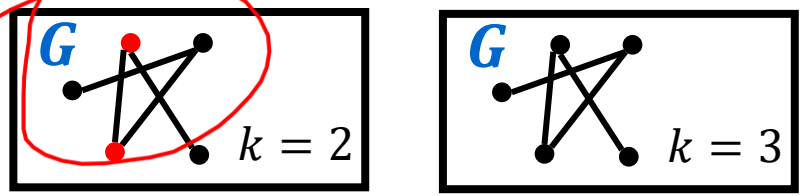
- $G' = (V, E')$ has the same vertices as G but E' consists of **precisely** those edges on V that are not edges of G.

From the definitions, U is an clique in G

$\Leftrightarrow U$ is an independent set in G'

Reducing Clique to Independent Set

Clique



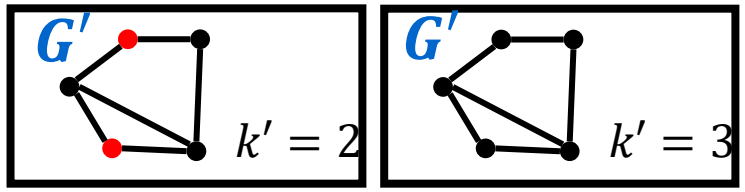
$O(n^p)$

Set G' to be the complement graph of G. Set $k' = k$

Use the same answer

Reduction

Independent Set



Algorithm for solving **Independent Set**

Solution for **Clique**

Yes/No

Solution for **Independent Set**

Yes/No

Another Reduction

Vertex-Cover:

Given a graph $G = (V, E)$ and an integer k

Is there a $W \subseteq V$ with $|W| \leq k$ such that every edge of G has an endpoint in W?

(W is a vertex cover, a set of vertices that covers E.)

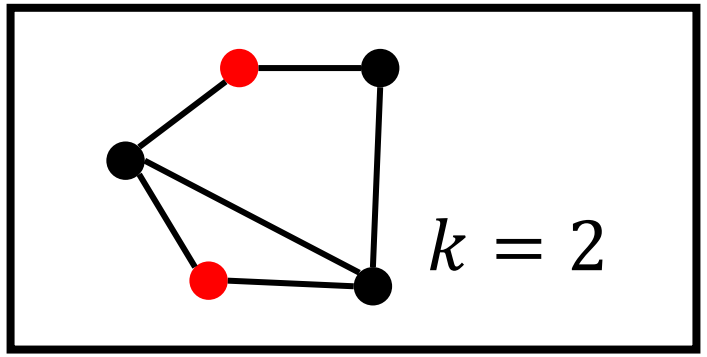
Claim: **Independent-Set $\leq_P$ Vertex-Cover**

Lemma: In a graph $G = (V, E)$ and $U \subseteq V$

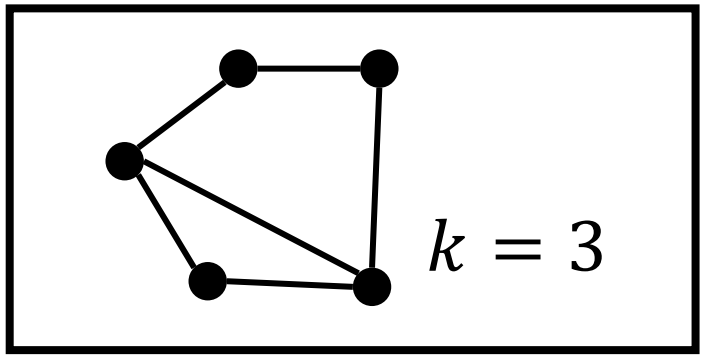
U is an independent set $\Leftrightarrow$ $V - U$ is a vertex cover

Examples

- Independent Set

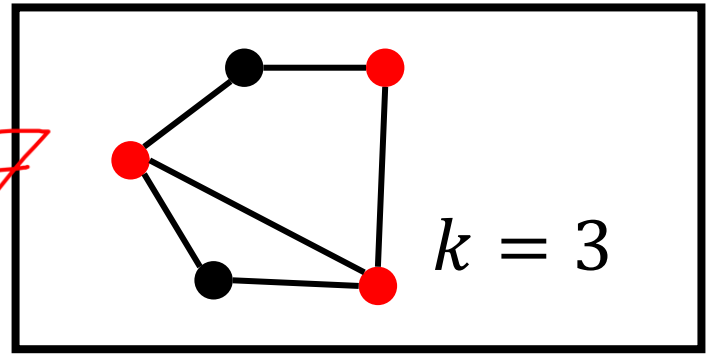


Yes

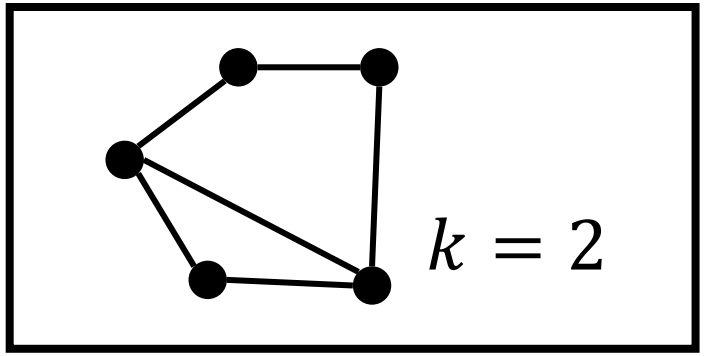


No

- Vertex Cover



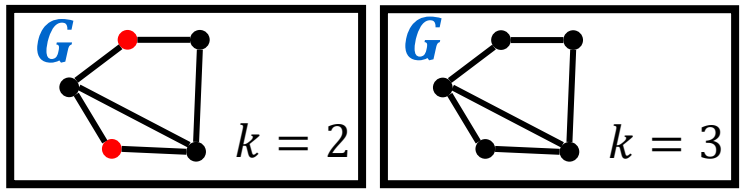
Yes



No

Reducing Independent Set to Vertex Cover

Independent Set



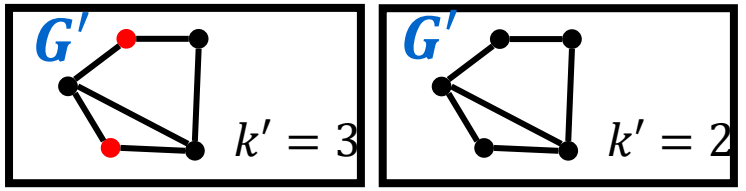
$O(n^p)$

Set $G' = G$. Set $k' = |V| - k$

Use the same answer

Reduction

Vertex Cover



Algorithm for solving **Vertex Cover**

Solution for **Independent Set**

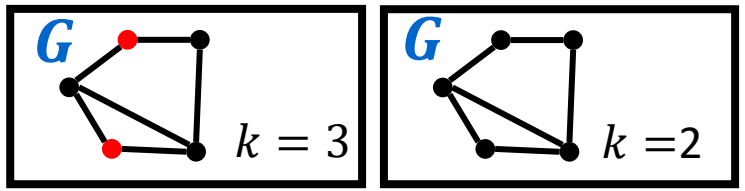
Yes/No

Solution for **Vertex Cover**

Yes/No

Reducing Vertex Cover to Independent Set

Vertex Cover



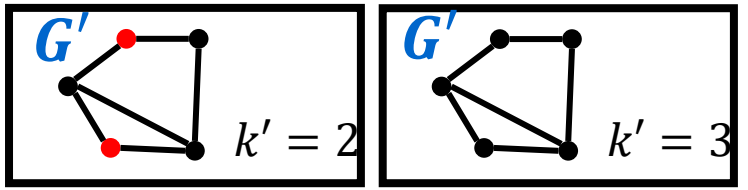
$O(n^p)$

Set $G' = G$. Set $k' = |V| - k$

Use the same answer

Reduction

Independent Set



Algorithm for solving **Independent Set**

Solution for **Vertex Cover**

Yes/No

Solution for **Independent Set**

Yes/No

Reduction Idea

Lemma: In a graph $G = (V, E)$ and $U \subseteq V$

U is an independent set $\Leftrightarrow V - U$ is a vertex cover

Proof:

($\Rightarrow$) Let U be an independent set in G

Then for every edge $e \in E$,

U contains at most one endpoint of e

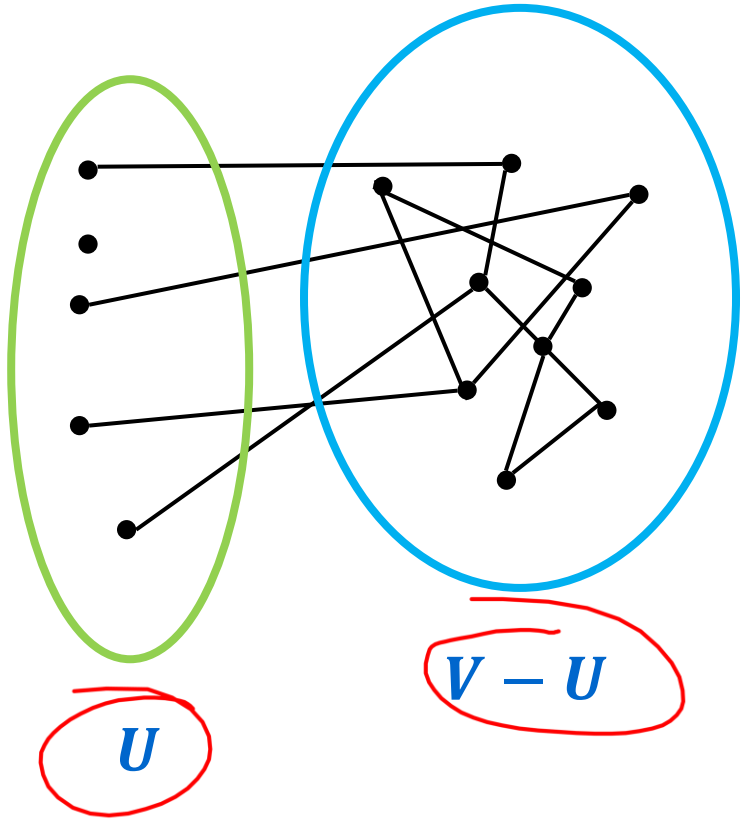
So, at least one endpoint of e must be in $V - U$

So, $V - U$ is a vertex cover

($\Leftarrow$) Let $W = V - U$ be a vertex cover of G

Then U does not contain both endpoints of any edge (else W would miss that edge)

So U is an independent set



Reduction for Clique $\leq_P$ Vertex-Cover

Clique:

Given a graph $G = (V, E)$ and an integer k

Is there a $U \subseteq V$ with $|U| \geq k$ such that every pair of vertices in U is joined by an edge?

(U is called a clique.)

Vertex-Cover:

Given a graph $G = (V, E)$ and an integer k

Is there a $W \subseteq V$ with $|W| \leq k$ such that every edge of G has an endpoint in W?

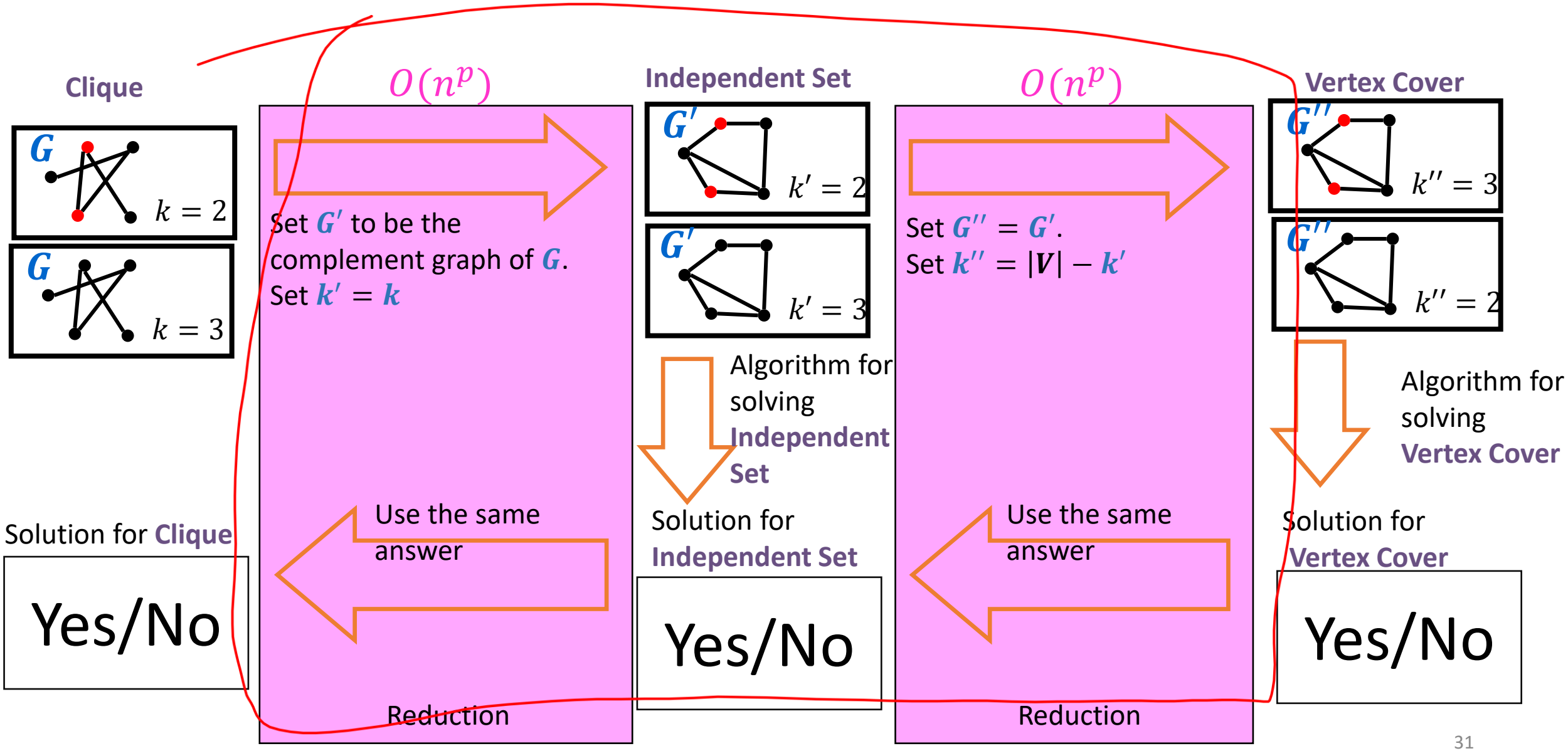
(W is a vertex cover, a set of vertices that covers E.)

Claim: **Clique $\leq_P$ Vertex-Cover**

Idea:

Use **Clique $\leq_P$ Independent-Set** and **Independent-Set $\leq_P$ Vertex-Cover**

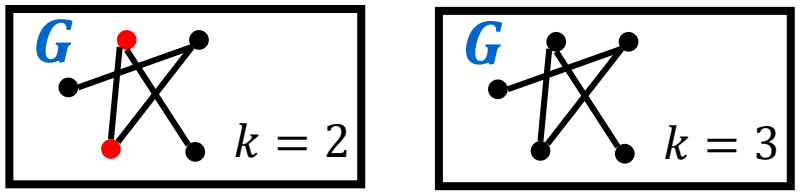
Reducing Clique to Vertex Cover



Reducing Clique to Vertex Cover

$(n^p)^q = n^{pq}$

Clique



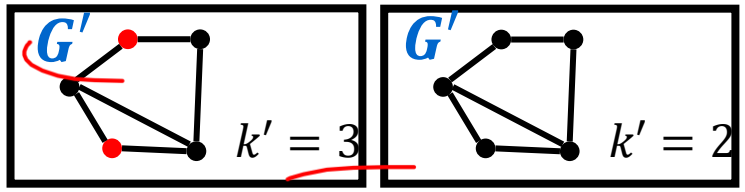
$O(n^p)$

Set G' to be the complement graph of G. Set $k' = |V| - k$

Use the same answer

Reduction

Vertex Cover



Algorithm for solving **Vertex Cover**

Solution for **Clique**

Yes/No

Solution for **Vertex Cover**

Yes/No

Polynomial time

Defn: Let **P** (polynomial-time) be the set of all decision problems solvable by algorithms whose worst-case running time is bounded by some polynomial in the input size.

This is the class of decision problems whose solutions we have called "efficient".

Polynomial Time Reduction

Defn: We write $A \leq_P B$ iff there is an algorithm for A using a 'black box' (subroutine or method) that solves B that

- uses only a polynomial number of steps, and
- makes only a polynomial number of calls to a method for B.

Theorem: If $A \leq_P B$ then $B \in \mathbf{P} \Rightarrow A \in \mathbf{P}$

Proof: Not only is the number of calls polynomial but the size of the inputs on which the calls are made is polynomial!

Corollary: If $A \leq_P B$ then $A \notin \mathbf{P} \Rightarrow B \notin \mathbf{P}$.

Theorem: If $A \leq_P B$ and $B \leq_P C$ then $A \leq_P C$

Proof: Compose the reductions: Plug in "the algorithm for B that uses C" in place of B.

Relationship among the problems so far

Using polynomial time reductions we have found:

- 2Color $\leq_P$ 3Color
- Independent-Set $\leq_P$ Clique
- Clique $\leq_P$ Independent-Set
- Vertex-Cover $\leq_P$ Independent-Set
- Independent-Set $\leq_P$ Vertex-Cover
- Clique $\leq_P$ Vertex-Cover
  - By composing the reductions for Clique $\leq_P$ Independet-Set and Independent-Set $\leq_P$ Vertex-Cover

- We could also conclude Vertex-Cover $\leq_P$ Clique
- Because we can reduce any of Independent-Set, Vertex-Cover, and Clique to any other:
  - If any one of those belongs to class P then all of them do.
  - In any one of those does not belong to class P then none of them do

Beyond $\mathbf{P}$?

Independent-Set, **Clique**, **Vertex-Cover**, and **3Color** are examples of natural and practically important problems for which we don't know any polynomial-time algorithms.

There are many others such as...

DecisionTSP:

Given a weighted graph G and an integer k,

Is there a simple path that visits all vertices in G having total weight at most k?

and...

Satisfiability

- Boolean variables $x_1, \ldots, x_n$
  - taking values in $\{0, 1\}$. 0=false, 1=true
- Literals
  - x_i or $\neg x_i$ for $i = 1, \ldots, n$. ($\neg x_i$ also written as $\overline{x_i}$.)
- Clause
  - a logical OR of one or more literals
  - e.g. $(x_1 \vee \neg x_3 \vee x_7 \vee x_{12})$
- CNF formula
  - a logical AND of a bunch of clauses
- k-CNF formula
  - All clauses have exactly k variables

Satisfiability

CNF formula example:

$$(x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_4 \vee x_3) \wedge (x_2 \vee \neg x_1 \vee x_3)$$

Defn: If there is some assignment of 0's and 1's to the variables that makes it true then we say the formula is satisfiable

- $(x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_4 \vee x_3) \wedge (x_2 \vee \neg x_1 \vee x_3)$ is satisfiable: $x_1 = x_3 = 1$
- $x_1 \wedge (\neg x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge \neg x_3$ is not satisfiable.

3SAT: Given a CNF formula F with exactly 3 variables per clause, is F satisfiable?

Common property of these problems

- There is a special piece of information, a short certificate or proof, that allows you to **efficiently verify** (in polynomial-time) that the **YES** answer is correct. This certificate might be very hard to find.

  - **3Color**: the assignment of a color to each node.
  - **Independent-Set, Clique**: the set of vertices
  - **Vertex-Cover**: the set of vertices
  - **Decision-TSP**: the path
  - **3SAT**: a truth assignment that makes the CNF formula true.

The complexity class **NP**

NP consists of all decision problems where

- You can **verify** the **YES** answers efficiently (in polynomial time) given a short (polynomial-size) ***certificate***

and

- **No fake certificate** can fool your polynomial time verifier into saying **YES** for a **NO** instance

More precise definition of **NP**

A decision problem **A** is in **NP** iff there is

- a polynomial time procedure **VerifyA**(.,.) and
- a polynomial p

s.t.

- for every input x that is a **YES** for **A** there is a string t with $|t| \leq p(|x|)$ with **VerifyA**(x, t) = **YES**

  and

- for every input x that is a **NO** for **A** there does not exist a string t with $|t| \leq p(|x|)$ with **VerifyA**(x, t) = **YES**

- A string t on which **VerifyA**(x, t) = **YES** is called a ***certificate*** for x or a ***proof*** that x is a **YES** input

Verifying the certificate is efficient

3Color: the coloring

- Check that each vertex has one of only 3 colors and check that the endpoints of every edge have different colors

Independent-Set, **Clique**: the set U of vertices

- Check that $|U| \geq k$ and either no (**IS**) or all (**Clique**) edges on present on U

Vertex-Cover: the set W of vertices

- Check that $|W| \leq k$ and W touches every edge.

Decision-TSP: the path

- Check that the path touches each vertex and has total weight $\leq k$.

- **3-SAT**: a truth assignment α that makes the CNF formula F true.
  - Evaluate F on the truth assignment α.

Keys to showing that a problem is in **NP**

1. Must be decision probem (**YES**/**NO**)
2. For every given **YES** input, is there a certificate (i.e., a hint) that would help?
   - OK if some inputs don't need a certificate
3. For any given **NO** input, is there a fake certificate that would trick you?
4. You need a polynomial-time algorithm to be able to tell the difference.

Solving **NP** problems without hints

There is an obvious algorithm for all **NP** problems:

Brute force:

Try all possible certificates and check each one using the verifier to see if it works.

Even though the certificates are short, this is exponential time

- 2^n truth assignments for n variables
- $\binom{n}{k}$ possible k-element subsets of n vertices
- $n!$ possible TSP tours of n vertices
- etc.

What We Know

- Every problem in $\mathbf{NP}$ is in exponential time
- Every problem in $\mathbf{P}$ is in $\mathbf{NP}$
  - You don't need a certificate for problems in $\mathbf{P}$ so just ignore any hint you are given
- Nobody knows if all problems in $\mathbf{NP}$ can be solved in polynomial time; i.e., does $\mathbf{P = NP?}$
  - one of the most important open questions in all of science.
  - huge practical implications
- Most CS researchers believe that $\mathbf{P \neq NP}$
  - $1M prize either way
  - but we don't have good ideas for how to prove this ...

$\mathbf{NP}$-hardness & $\mathbf{NP}$-completeness

Notion of hardness we **can** prove that is useful unless $\mathbf{P} = \mathbf{NP}$:

Defn: Problem B is $\mathbf{NP}$-hard iff **every** problem $A \in \mathbf{NP}$ satisfies $A \leq_P B$.

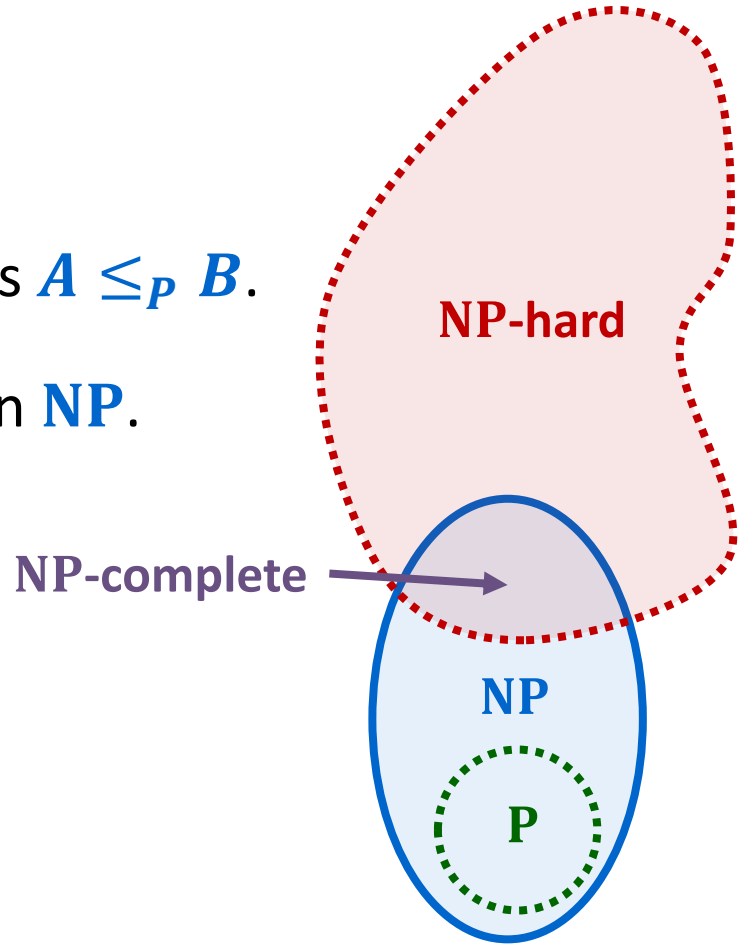
This means that B is at least as hard as every problem in $\mathbf{NP}$.

Defn: Problem B is $\mathbf{NP}$-complete iff

- $B \in \mathbf{NP}$ and
- B is $\mathbf{NP}$-hard.

This means that B is a hardest problem in $\mathbf{NP}$.

Not at all obvious that any $\mathbf{NP}$-complete problems exist!



Cook-Levin Theorem

Theorem [Cook 1971, Levin 1973]: **3SAT** is **NP**-complete

Proof: See CSE 431.

Corollary: If **3SAT** $\leq_P$ **B** then **B** is **NP**-hard.

Proof: Let **A** be an arbitrary problem in **NP**.
Since **3SAT** is **NP**-hard we have **A** $\leq_P$ **3SAT.**

Then **A** $\leq_P$ **3SAT** and **3SAT** $\leq_P$ **B** imply that **A** $\leq_P$ **B**.

Therefore every problem **A** in **NP** has **A** $\leq_P$ **B**
so **B** is **NP**-hard.

Cook & Levin did the hard work.

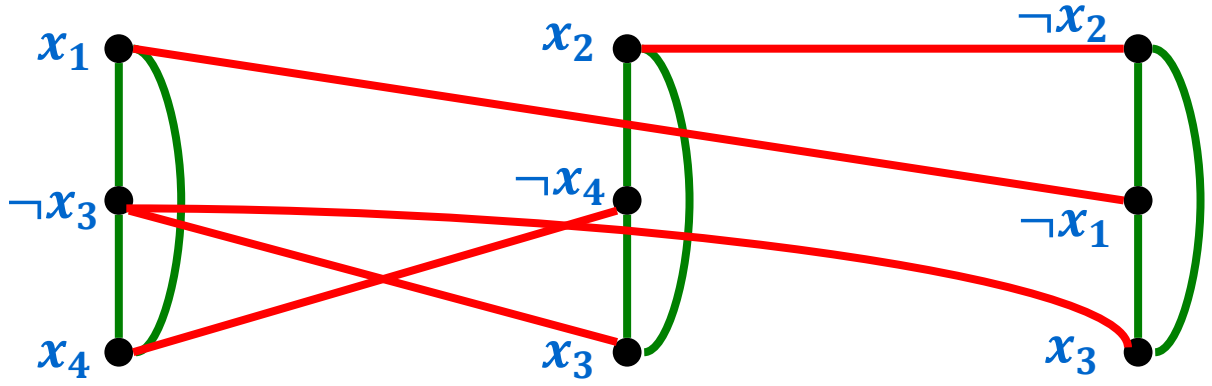
We only need to give one reduction to show that a problem is NP-hard!

Another **NP**-complete problem: 3SAT $\leq_P$ Independent-Set

1. The reduction:
   - Map CNF formula F to a graph G and integer k
   - Let m = # of clauses of F
   - Create a vertex in G for each literal occurrence in F
   - Join two vertices u, v in G by an edge iff
     - u and v correspond to literals in the same clause of F (green edges) or
     - u and v correspond to literals x and $\neg x$ (or vice versa) for some variable x (red edges).
   - Set $k = m$
2. Clearly polynomial-time computable

Another **NP**-complete problem: 3SAT $\leq_P$ Independent-Set

$\boldsymbol{F = (x_1 \vee \neg x_3 \vee x_4) \wedge (x_2 \vee \neg x_4 \vee x_3) \wedge (\neg x_2 \vee \neg x_1 \vee x_3)}$



$\boldsymbol{m = 3}$

$\boldsymbol{G}$ has both kinds of edges.
The color is just to show why the edges were included.

$\boldsymbol{k = m}$

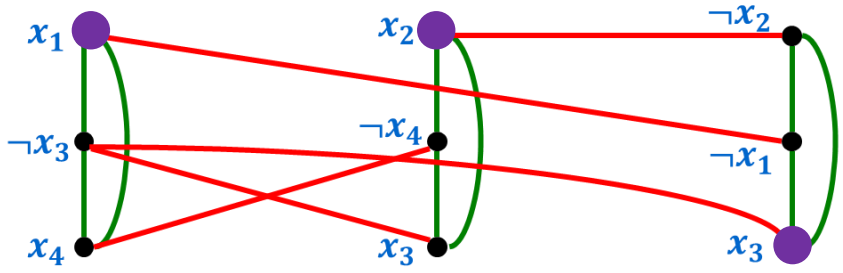
Correctness (⇒)

Suppose that F is satisfiable (**YES** for **3SAT**)

- Let α be a satisfying assignment; it satisfies at least one literal in each clause.
- Choose the set U in G to correspond to the **first satisfied literal in each clause**.
  - $|U| = m$
  - Since U has 1 vertex per clause, no green edges inside U.
  - A truth assignment never satisfies both x and $\neg x$, so no red edges inside U.
  - Therefore U is an independent set of size m

Therefore (G, m) is a **YES** for **Independent-Set**.

$$F = (x_1 \vee \neg x_3 \vee x_4) \wedge (x_2 \vee \neg x_4 \vee x_3) \wedge (\neg x_2 \vee \neg x_1 \vee x_3)$$



Satisfying assignment α:

$$\alpha(x_1) = \alpha(x_2) = \alpha(x_3) = \alpha(x_4) = 1$$

Set U marked in purple is independent.

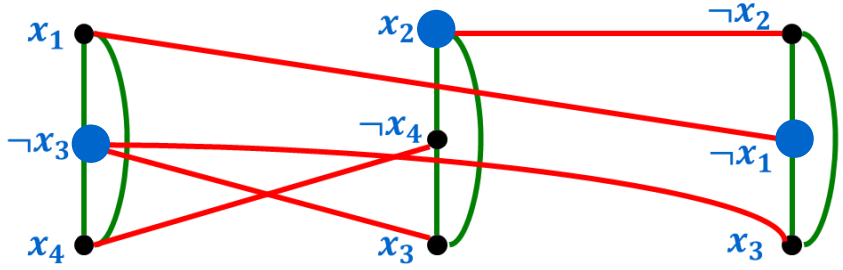
Correctness (⇐)

Suppose that G has an independent set of size m ((G, m) is a **YES** for **Independent-Set**)

- Let U be the independent set of size m;
- U must have one vertex per column (green edges)
- Because of red edges, U doesn't have vertex labels with conflicting literals.
- Set all literals labelling vertices in U to true
- This may not be a total assignment but just extend arbitrarily to a total assignment α.
  - This assignment satisfies F since it makes at least one literal per clause true.

Therefore F is satisfiable and a **YES** for **3SAT**.

$$F = (x_1 \vee \neg x_3 \vee x_4) \wedge (x_2 \vee \neg x_4 \vee x_3) \wedge (\neg x_2 \vee \neg x_1 \vee x_3)$$



Given independent set U of size m

Satisfying assignment α: Part defined by U:

$\alpha(x_1) = 0, \alpha(x_2) = 1, \alpha(x_3) = 0$

Set $\alpha(x_4) = 0$.

Many **NP**-complete problems

Since **3SAT** $\leq_P$ **Independent-Set**, **Independent-Set** is **NP**-hard.

We already showed that **Independent-Set** is in **NP**.

⇒ **Independent-Set** is **NP**-complete

Corollary: **Clique** and **Vertex-Cover** are also **NP**-complete.

Proof: We already showed that all are in **NP**.

We also showed that **Independent-Set** polytime reduces to all of them.

Combining this with **3SAT** $\leq_P$ **Independent-Set** we get that all are **NP**-hard.