Lecture 19: NP-Completeness

Outline of this Lecture

- Polynomial-time reductions.
  CLRS pp.984-5

- The class $\mathcal{NPC}$.
  CLRS p. 986

- Proving that problems are $\mathcal{NPC}$.
  SAT, CLIQUE, INDEPENDENT SET, VERTEX COVER
  CLRS pp. 995-1007

- Optimization vs. Decision problems

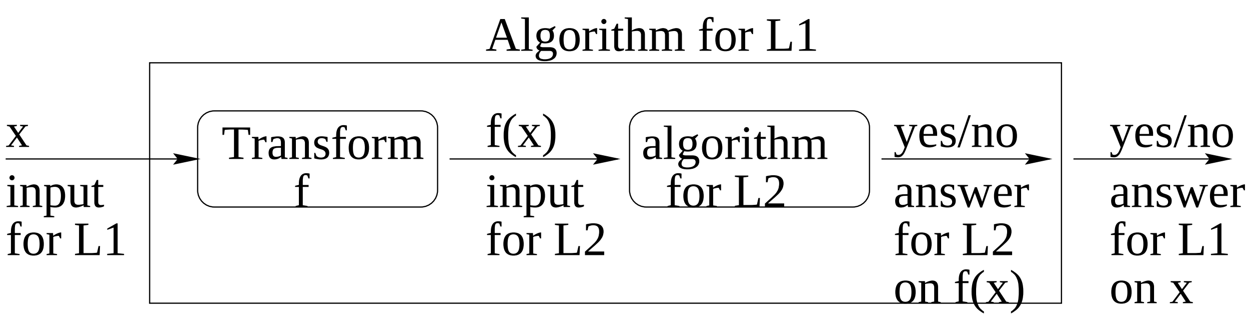
Reductions between Decision Problems

What is Reduction?

Let L_1 and L_2 be two decision problems.

Suppose algorithm A_2 solves L_2. That is, if y is an input for L_2 then algorithm A_2 will answer Yes or No depending upon whether $y \in L_2$ or not.

The idea is to find a transformation f from L_1 to L_2 so that the algorithm A_2 can be part of an algorithm A_1 to solve L_1.

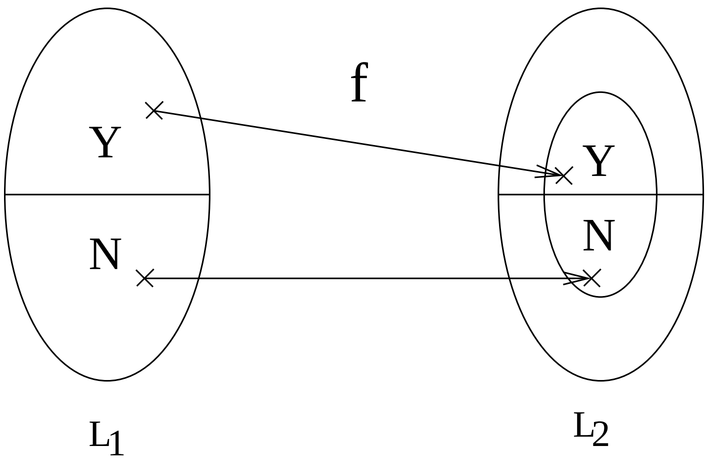


***Polynomial*-Time Reductions**

Definition: A Polynomial-Time Reduction from L_1 to L_2 is a transformation f with the following properties:

- f transforms
  an input x for L_1 into an input $f(x)$ for L_2 s.t.

  $f(x)$ is a yes-input for L_2 if and only if x is a yes-input for L_1.



We require a yes-input of L_1 maps to a yes-input of L_2, and a no-input of L_1 maps to a no-input of L_2.

Polynomial-Time Reductions

- $f(x)$ is computable in polynomial time (in $size(x)$).

If such an f exists, we say that

L_1 is polynomial-time reducible to L_2,

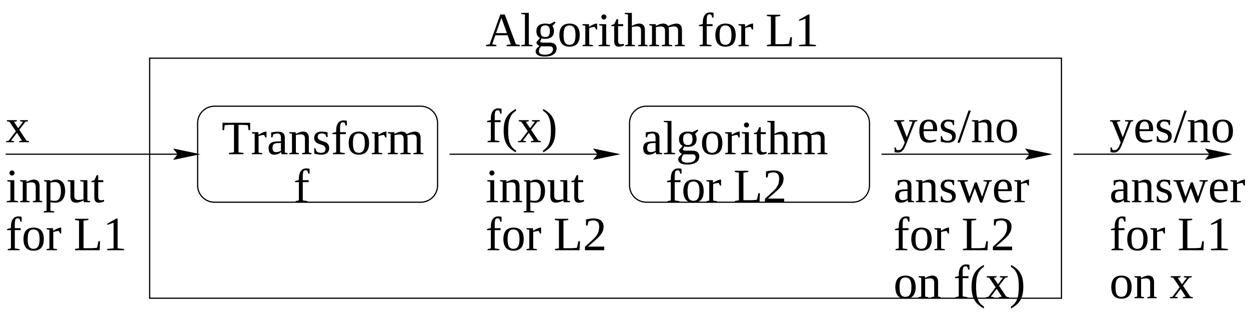
and write $L_1 \leq_P L_2$.

Polynomial-Time Reductions

Question: What can we do with a polynomial time reduction $f : L_1 \to L_2$?

Answer: Given an algorithm A_2 for the decision problem L_2, we can develop an algorithm A_1 to solve L_1.

In particular (proof on next slide)
if A_2 is a polynomial time algorithm for L_2 and $L_1 \leq_P L_2$
then we can construct a polynomial time algorithm for L_1.



Polynomial-Time Reduction $f : L_1 \to L_2$

Theorem:
If $L_1 \leq_P L_2$ and $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

Proof: $L_2 \in \mathcal{P}$ means that we have a polynomial-time algorithm A_2 for L_2. Since $L_1 \leq_P L_2$, we have a polynomial-time transformation f mapping input x for L_1 to an input for L_2. Combining these, we get the following polynomial-time algorithm for solving L_1:

(1) take input x for L_1 and compute $f(x)$;

(2) run A_2 on input $f(x)$, and return the answer found (for L_2 on $f(x)$) as the answer for L_1 on x.

Each of Steps (1) and (2) takes polynomial time. So the combined algorithm takes polynomial time. Hence $L_1 \in \mathcal{P}$.

Warning

We have just seen

Theorem:
If $L_1 \leq_P L_2$ and $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

Note that this **does not imply** that
If $L_1 \leq_P L_2$ and $L_1 \in \mathcal{P}$, then $L_2 \in \mathcal{P}$.
This statement is not true.

Reduction between Decision Problems

Lemma (Transitivity of the relation $\leq_P$):
If $L_1 \leq_P L_2$ and $L_2 \leq_P L_3$, then $L_1 \leq_P L_3$.

Proof: Since $L_1 \leq_P L_2$, there is a polynomial-time reduction f_1 from L_1 to L_2.
Similarly, since $L_2 \leq_P L_3$ there is a polynomial-time reduction f_2 from L_2 to L_3.

Note that $f_1(x)$ can be calculated in time polynomial in $size(x)$.
In particular this implies that $size(f_1(x))$ is polynomial in $size(x)$.
$f(x) = f_2(f_1(x))$ can therefore be calculated in time polynomial in $size(x)$.

Furthermore x is a yes-input for L_1 if and only if $f(x)$ is a yes-input for L_3(why). Thus the combined transformation defined by

$$f(x) = f_2(f_1(x))$$

is a polynomial-time reduction from L_1 to L_3.
Hence $L_1 \leq_P L_3$.

Finally: The Class $\mathcal{NP}$-Complete ($\mathcal{NPC}$)

We have finally reached our goal of introducing class $\mathcal{NPC}$.

Definition: The class $\mathcal{NPC}$ of $\mathcal{NP}$-complete problems consists of all decision problems L such that

(a) $L \in \mathcal{NP}$;

(b) for every $L' \in \mathcal{NP}$, $L' \leq_P L$.

Intuitively, $\mathcal{NPC}$ consists of all the **hardest** problems in $\mathcal{NP}$.

$\mathcal{NP}$-Completeness and Its Properties

The major reason we are interested in NP-Completeness is the following theorem which states that either *all* $\mathcal{NP}$-Complete problems are polynomial time solvable or *all* $\mathcal{NP}$-Complete problemsare not polynomial time solvable.

Theorem: Suppose that L is $\mathcal{NPC}$.

- If there is a polynomial-time algorithm for L, then there is a polynomial-time algorithm for every $L' \in \mathcal{NP}$.

  Proof: By the theorem on Page 5.

- If there is no polynomial-time algorithm for L, then there is no polynomial-time algorithm for any $L' \in \mathcal{NPC}$.

  Proof: By the previous conclusion.

The Classes $\mathcal{P}$, $\mathcal{NP}$, co-$\mathcal{NP}$, and $\mathcal{NPC}$

Proposition: $\mathcal{P} \subseteq \mathcal{NP}$.
Simple proof omitted

Question 1: Is $\mathcal{NPC} \subseteq \mathcal{NP}$?
Yes, by definition!

Question 2: Is $\mathcal{P} = \mathcal{NP}$?
Open problem! Probably very hard
It is generally believed that $\mathcal{P} \neq \mathcal{NP}$.
Proving this (or the opposite) would win you the US$1,000,000 Clay Prize.

Question 3: Is $\mathcal{NP} = \text{co}-\mathcal{NP}$?
Open problem! Probably also very hard
Note: if $\mathcal{NP} \neq \text{co}-\mathcal{NP}$, then $\mathcal{P} \neq \mathcal{NP}$ (why?).

The Class $\mathcal{NP}$-Complete ($\mathcal{NPC}$)

Given the transitivity property of the relation $\leq_p$, we have an alternative way to show that a decision $L \in \mathcal{NPC}$:

(a) $L \in \mathcal{NP}$;

(b) for some $L' \in \mathcal{NPC}$, $L' \leq_P L$.

Cook's Theorem (SAT $\in \mathcal{NPC}$)

Unfortunately, it appears impossible to find *one* problem $L \in \mathcal{NPC}$. By definition, it requires us to show *every* $L^{'} \in \mathcal{NP}$, $L' \leq_P L$. But there are infinitely many problem in NP, so how can we argue there exists a reduction for every $L^{'}$ to L?

Cook's Theorem (1971): $\mathsf{SAT} \in \mathcal{NPC}$. (For a proof, see pp. 997-998 of the textbook.)

Remark: Since Cook showed that $\mathsf{SAT} \in \mathcal{NPC}$, thousands of problems have been shown to be in $\mathcal{NPC}$ using the reduction approach described earlier.

Remark: With a little more work we can also show that $3 - \mathsf{CNF} - \mathsf{SAT} \in \mathcal{NPC}$ as well. pp. 998-1002.

Note: For the purposes of this course you only need to know the validity of Cook's Theorem, and 3-CNF-SAT $\in \mathcal{NPC}$ but do not need to know how to prove they are correct.

Proving that problems are $\mathcal{NPC}$

In the rest of this lecture we will discuss some specific $\mathcal{NP}$-Complete problems.

1. $\mathsf{SAT}$and $\mathsf{3\text{-}CNF-SAT}$.
   We will assume that they are $\mathcal{NP}$-Complete. (From textbook)

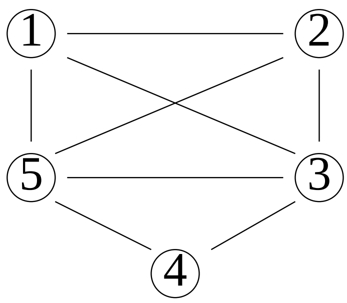
2. DCLIQUE:
   by showing $\mathsf{3-CNF-SAT} \le_{\mathsf{P}} \mathsf{DCLIQUE}$
   The reduction used is very unexpected!

3. Decision Vertex Cover DVC:
   by showing $\mathsf{DCLIQUE} \le_{\mathsf{P}} \mathsf{DVC}$
   The reduction used is very natural.

4. Decision Independent Set (DIS):
   by showing $\mathsf{DVC} \le_{\mathsf{P}} \mathsf{IS}$
   The reduction used is very natural.

Problem: CLIQUE

Clique: A *clique* in an undirected graph $G = (V, E)$ is a subset $V' \subseteq V$ of vertices such that each pair $u, v \in V'$ is connected by an edge $(u, v) \in E$. In other words, a clique is a complete subgraph of G (a vertex is a clique of size 1, an edge a clique of size 2).

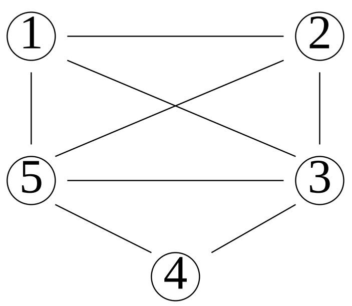


Find a clique with 4 vertices

CLIQUE: Find a clique of maximum size in a graph.

$\mathcal{NPC}$ Problem: DCLIQUE

The Decision Clique Problem (DCLIQUE): Given an undirected graph G and an integer k, determine whether G has a clique with k vertices.



Find a clique with 4 vertices

Theorem: DCLIQUE $\in \mathcal{NPC}$.

Proof: We need to show two things.
(a) That DCLIQUE $\in \mathcal{NP}$ and
(b) That there is some $L \in \mathcal{NPC}$ such that

$$L \leq_P \text{DCLIQUE}.$$

Proof that DCLIQUE $\in \mathcal{NPC}$

Theorem: DCLIQUE $\in \mathcal{NPC}$.

Proof: We need to show two things.
(a) That DCLIQUE $\in \mathcal{NP}$ and
(b) That there is some $L \in \mathcal{NPC}$ such that

$$L \leq_P \text{DCLIQUE}.$$

Proving (a) is easy. A certificate will be a set of vertices $V' \subseteq V$, $|V'| = k$ that is a possible clique. To check that V' is a clique all that is needed is to check that all edges (u, v) with $u \neq v$, $u, v \in V'$, are in E. This can be done in time $O(|V|^2)$ if the edges are kept in an adjacency matrix (and even if they are kept in an adjacency list – how?).

To prove (b) we will show that

$$3-\text{CNF}-\text{SAT} \leq_P \text{DCLIQUE}.$$

This will be the hard part.
We will do this by building a 'gadget' that allows a reduction from the 3 – CNF – SAT problem (on logical formulas) to the DCLIQUE problem (on graphs, and integers).

Proof that $\mathsf{DCLIQUE} \in \mathcal{NPC}$ (cont)

Recall (from Lecture 18) that the input to $3-\mathsf{CNF}-\mathsf{SAT}$ is a logical formula ϕ of the form

$$\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

where each C_i is of the form

$$C_i = y_{i,1} \vee y_{i,2} \vee y_{i,3}$$

where each $y_{i,j}$ is a variable or the negation of a variable.

As an example

$$C_1 = (x_1 \vee \neg x_2 \vee \neg x_3)\,,\; C_2 = (\neg x_1 \vee x_2 \vee x_3)\,,\; C_3 = (x_1 \vee x_2 \vee x_3)$$

We will define a polynomial transformation f from $3-\mathsf{CNF}-\mathsf{SAT}$ to $\mathsf{DCLIQUE}$

$$f : \phi \mapsto (G, k)$$

that builds a graph G and integer k such that ϕ is a Yes-input to $3-\mathsf{CNF}-\mathsf{SAT}$ if and only if (G, k) is a Yes-input to $\mathsf{DCLIQUE}$.

Proof that DCLIQUE $\in \mathcal{NPC}$ (cont)

Suppose that ϕ is a $3-\mathrm{CNF}-\mathrm{SAT}$ formula with n clauses, i.e., $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_n$. We start by setting $k = n$.
We now construct graph $G = (V, E)$.

(I) For each clause $C_i = x_{i,1} \vee x_{i,2} \vee x_{i,3}$ we create 3 vertices, v_1^i, v_2^i, v_3^i, in V so G has $3n$ vertices. We will *label* these vertices with the corresponding variable or variable negation that they represent. (Note that many vertices might share the same label)

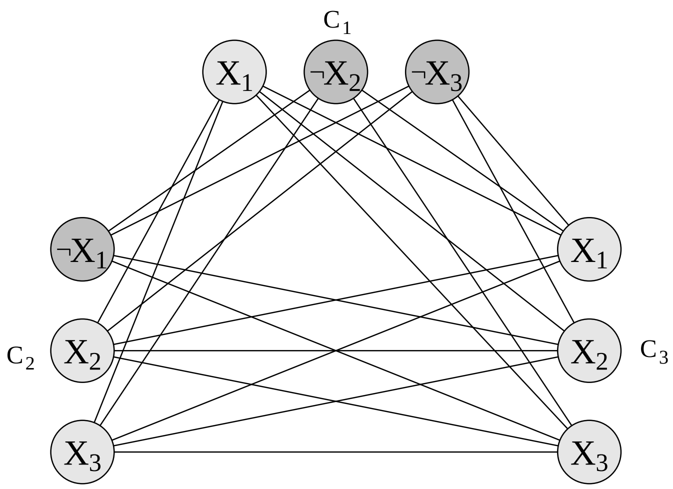
(II) We create an *edge* between vertices v_j^i and $v_{j'}^{i'}$ if and only if the following two conditions hold:
(a) v_j^i and $v_{j'}^{i'}$ are in different triples, i.e., $i \neq i'$, and
(b) v_j^i is not the *negation* of $v_{j'}^{i'}$.

Note that the transformation maps *all* 3-CNF-SAT inputs to *some* DCLIQUE inputs, i.e., it does not require *all* DCLIQUE inputs have pre-images from 3-CNF-SAT inputs.

Proof that DCLIQUE $\in \mathcal{NPC}$ (cont)

Here is a formula $\phi = C_1 \wedge C_2 \wedge C_3$ and its corresponding graph:

$C_1 = (x_1 \vee \neg x_2 \vee \neg x_3)$, $C_2 = (\neg x_1 \vee x_2 \vee x_3)$, $C_3 = (x_1 \vee x_2 \vee x_3)$



Note that the assignment $X_1 = T, X_2 = F, X_3 = T$ satisfies ϕ (a yes-input for 3-CNF-SAT). This corresponds to the clique of size 3 comprising the $\neg x_2$ node in C_1, the x_3 node in C_2, and the x_3 node in C_3 (a yes-input for DCLIQUE).

Proof that DCLIQUE $\in \mathcal{NPC}$ (cont)

We claim that a $3-$CNF formula ϕ with k clauses is satisfiable if and only if $f(\phi) = (G, k)$ has a clique of size k.

$Y \Rightarrow Y$: If ϕ is satisfiable, then in each k clause, there must be at least one true literal. Let the true literal in each clause be $\underbrace{(x_i, \neg x_j, ..., \neg x_w).}_{k \text{ literals}}$ Observe the true literals must be consistence to each others, i.e., for any i, $x_i, \neg x_i$ will not appear together in the true assignment. The corresponding k vertices $(x_i, \neg x_j, ..., \neg x_w)$ will form a complete subgraph (a clique) in G. Since in our construction of G, every vertex will be connected to other vertex if they are logically consistent. Since, for any i, x_i and $\neg x_i$ will not appear together in the vertex list, every vertex in the list must be connected by an edge forming a complete subgraph (clique) of size k.

Proof that $\text{DCLIQUE} \in \mathcal{NPC}$ (cont)

$Y \Leftarrow Y$: Suppose G has a clique of size k. Observe that there is *no* edge between vertices in the same clause. Hence, each one clause 'contributes' exactly one vertex to the clique. Moreover, since other logically consistent vertex will be connected by a edge, every vertex in the clique must be logically consistent. Hence, those vertices in the clqiue is a true assignment which makes ϕ satisfiable.

Proof that $\mathrm{DCLIQUE} \in \mathcal{NPC}$ (cont)

Note that the graph G has $3k$ vertices and at most $3k(3k-1)/2$ edges and can be built in $O(k^2)$ time so f is a *Polynomial*-time reduction.

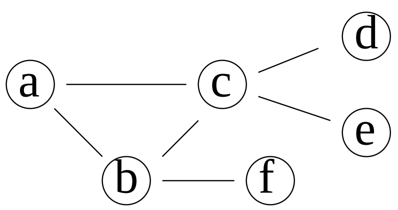
We have therefore just proven that

$$3-\mathrm{CNF} \le_{\mathrm{P}} \mathrm{DCLIQUE}.$$

Since we already know that $3-\mathrm{CNF} \in \mathcal{NPC}$ and have seen that $\mathrm{DCLIQUE} \in \mathcal{NP}$ we have just proven that $\mathrm{DCLIQUE} \in \mathcal{NPC}$.

Problem: VC

Vertex Cover: A *vertex cover* of G is a set of vertices such that every edge in G is incident to at least one of these vertices.

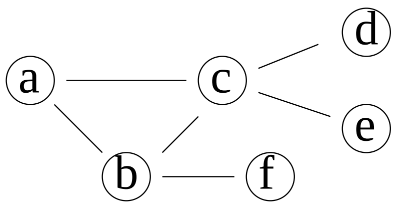


Find a vertex cover of G of size two

The Vertex Cover Problem (VC): Given a graph G, find a vertex cover of G of minimum size.

$\mathcal{NPC}$ Problem: DVC

The Decision Vertex Cover Problem (DVC): Given a graph G and integer k, determine whether G has a vertex cover with k vertices.



Find a vertex cover of G of size two

Theorem: DVC $\in \mathcal{NPC}$.

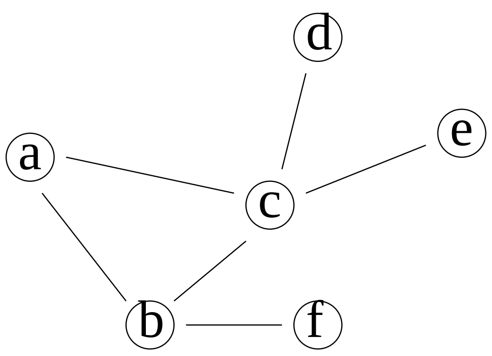
Proof: In Lecture 18, we showed that DVC $\in \mathcal{NP}$.

We show that DCLIQUE $\leq_P$ DVC. The conclusion then follows from the fact that DCLIQUE $\in \mathcal{NPC}$. A proof of DCLIQUE $\leq_P$ DVC will be given in the next few slides.

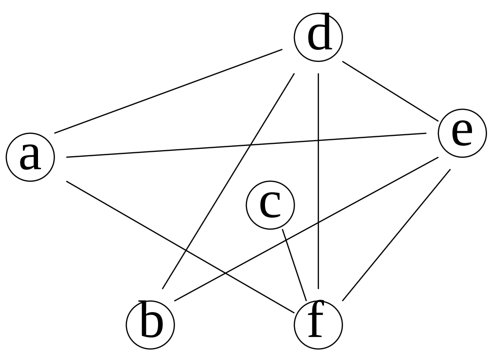
DVC $\in \mathcal{NPC}$: Complement of a Graph

The **complement of a graph** $G = (V, E)$ is defined by $\overline{G} = (V, \overline{E})$, where

$$\overline{E} = \{(u, v) \mid u, v \in V,\ u \neq v,\ (u, v) \notin E\}.$$



Graph G



Complement of G

Proof: DVC $\in \mathcal{NPC}$

Let $k^{'} = |V| - k$. We define a transformation f from DCLIQUE to DVC:

$$f : (G = (V, E), k) \mapsto (\overline{G} = (V, \bar{E}, k^{'})$$

- f can be computed (that is, $\overline{G}$ and $k^{'}$ can be determined) in time $O(|V|^2)$ time .

- We claim that A graph G has a clique of size k (yes-input of DCLIQUE) if and only if the complement graph $\overline{G}$ has a vertex cover of size $|V| - k$ (a yes-input of DVC).

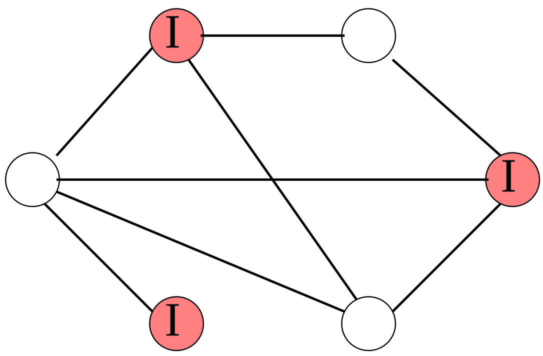
DVC $\in \mathcal{NPC}$: **Transformation**

$Y \Rightarrow Y$: Let $V^{'}$ be a clique of size k in G, then in $\bar{G}$, there is no edge between any two vertices $\in V^{'}$. Hence $V'' = V \setminus V'$ (size = $|V| - k$) is a VC in $\bar{G}$.

$Y \Leftarrow Y$: Let V' be a VC (size = $|V| - k$) of $\bar{G}$, and let $V'' = V \setminus V'$, where $|V''| = k$. By the definition of VC, if any $u, v \in V^{'}$, $(u, v) \notin \bar{E}$. Hence, for any $u, v \in V^{''}$, $(u, v) \in E$. Therefore $V^{''}$ is a clique of size k in G.

Problem: Independent Set

Definition: An *independent set* is a subset I of vertices in an undirected graph G such that no pair of vertices in I is joined by an edge of G.



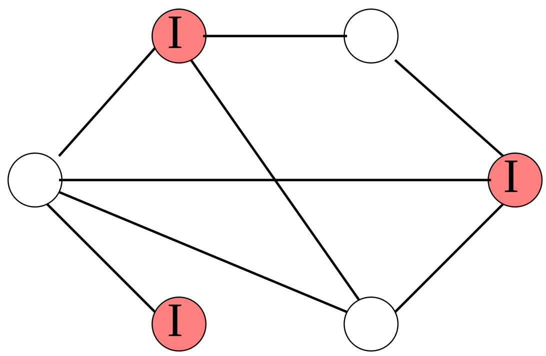
$\mathcal{NPC}$ Problem: Decision Independent Set (DIS)

Optimization Problem: Given an undirected graph G, find an independent set of maximum size.

Decision Problem (DIS): Given an undirected graph G and an integer k, does G contain an independent set consisting of k vertices?

Theorem: DVC $\in \mathcal{NPC}$.

Proof: It is very easy to see that DIS $\in \mathcal{NP}$. A certificate is a set of vertices $S \subseteq V$ and, in $O(|S|^2) = O(|V|^2)$ time we can check whether or not S is an independent set. In the next slide we will see that DCLIQUE $\leq_{\text{P}}$ DIS, completing the proof.



$\boxed{\text{DIS} \in \mathcal{NPC}}$

We can define a transformation from DCLIQUE to DIS:

$$f : (G = (V, E), k) \mapsto (\overline{G} = (V, \bar{E}), k)$$

We claim (G, k) is a Yes-input to DCLIQUE if and only if $(\bar{G}, k)$ is a Yes-input to DIS.

$Y \Rightarrow Y$: Let $V^{'}$ be a clique of size k of G. Hence in $\bar{G}$, there is no edge between any vertex in $V^{'}$ which means $V^{'}$ (size=k) is a IS of $\bar{G}$.

$Y \Leftarrow Y$: Let $V^{'}$ be a IS of size k in $\bar{G}$. Hence in G, every vertex in $V^{'}$ be be connected by an edge. Hence $V^{'}$ (size=k) is a clique of G.

Moreover, f can be calculated in polynomial time we have just shown that DCLIQUE $\leq_{\text{P}}$ DIS and completed the proof that DIS $\in \mathcal{NPC}$.

Decision versus Optimization Problems

The theory of $\mathcal{NP}$-Completeness revolves around decision problems. It was set up this way because it's easier to compare the difficulty of decision problems than that of optimization problems.

At first glance, this might seem unhelpful since we usually don't care at all about decision problems. We're interested in finding an optimal solution to our problem (the optimization version) not whether such a solution exists (decision version).

In reality, though, being able to solve a decision problem in polynomial time will often permit us to solve the corresponding optimization problem in polynomial time (using a polynomial number of calls to the decision problem). So, discussing the difficulty of decision problems is often really equivalent to discussing the difficulty of optimization problems.

In the next two slides we see an example of this phenomenon for VERTEX COVER by showing that having a polynomial algorithm for Decision Vertex Cover (DVC) would yield a polynomial algorithm for finding a minimal Vertex Cover.

Decision versus Optimization Problems (cont)

Here are the two problems and third related one

VC: Given undirected graph G find a minimal size vertex cover.
DVC: Given undirected graph G and k, is there a vertex cover of size k?
MVC: Given an undirected graph G, find the size of a minimal vertex cover.

Suppose that $DVC(G, k)$ returns Yes if G has a vertex cover of size k and No, otherwise.

Consider the following algorithm for solving MVC:

$k = 0$;
while (not DVC(G, k)) $k = k + 1$;
return(k);

Note that MVC calls DVC at most $|V|$ times so, if there is a polynomial time algorithm for DVC, then our algorithm for MVC is also polynomial.

Decision versus Optimization Problems (cont)

Here is an algorithm for calculating $VC(G)$ that uses the algorithm for MVC on the previous page. First set $k = MVC(G)$ and then run $VC(G, k)$ which is defined by:

```
// find a VC of size t
VC(G, t)
{
 // Let G_u be a graph such that the
 // vertex u, and its corresponding edges
 // are removed from G.
 // We then find the a vertex u such that
 if (MVC(G_u)==1) output u;
 // such u must exist, why?

 if (t > 1) VC(G_u, t-1);
}
```

(Show why the output vertices is a VC of G.)

Decision versus Optimization Problems (cont)

Note that this algorithm calls MVC at most $|V|^2$ times so, if MVC is polynomial in $size(G)$, then so is VC. We already saw that if DVC is polynomial in $size(G)$ so is MVC, so we've just shown that if we can solve DVC in polynomial time, we can solve VC in polynomial time.

NP-Hard Problems

A problem L is $\mathcal{NP}$-hard if some problem in $\mathcal{NPC}$ can be polynomially reduced to it (but L does not need to be in $\mathcal{NP}$).

In general, the Optimization versions of $\mathcal{NP}$-Complete problems are $\mathcal{NP}$-Hard.

For example, recall
VC: Given undirected graph G find a minimal size vertex cover.
DVC: Given undirected graph G and k, is there a vertex cover of size k?

If we can solve the optimization problem VC we can easily solve the decision problem DVC. Simply run VC on graph G and find a minimal vertex cover S. Now, given (G, k), solve $DVC(G, k)$ by checking whether $k \geq |S|$. If $k \geq |S|$ answer Yes, if not, answer No.

A List of $\mathcal{NPC}$ Problems Covered

Satisfiability of Boolean formulas (SAT)
Decision clique (DCLIQUE)
Decision vertex cover (DVC)
Decision independent set (DIS)

Remark: Several thousand decision problems have been shown to be in $\mathcal{NPC}$.

A Review on $\mathcal{NP}$-Completeness

Input size of problems.

Polynomial-time and nonpolynomial-time algorithms.

Polynomial-time solvable problems.

Decision problems.

Optimization problems and their decision problems.

The classes $\mathcal{P}$, $\mathcal{NP}$, co-$\mathcal{NP}$, and $\mathcal{NPC}$.

Polynomial-time reduction.

How to prove $L \in \mathcal{P}$, or $\mathcal{NP}$, or $\mathcal{NPC}$?

Examples of problems in the classes.