Part VII. Selected Topics

Chapter 34 NP-Completeness

1. Intractable problems
   • decision versions of optimization problems

2. Nondeterministic computational models
   • nondeterministic computation = certificate + verification

3. NP-completeness framework
   • reduction, polynomial-time reduction

4. NP-completeness proof
   • NP-complete problems, reduction techniques.
Chapter 34 NP-Completeness
Chapter 34 NP-Completeness

1. Intractable problems
Chapter 34 NP-Completeness

1. Intractable problems
   • decision versions of optimization problems
Chapter 34 NP-Completeness

1. Intractable problems
   - decision versions of optimization problems

2. Nondeterministic computational models
Chapter 34 NP-Completeness

1. Intractable problems
   - decision versions of optimization problems

2. Nondeterministic computational models
   - nondeterministic computation = certificate + verification
Chapter 34 NP-Completeness

1. Intractable problems
   • decision versions of optimization problems

2. Nondeterministic computational models
   • nondeterministic computation = certificate + verification

3. NP-completeness framework
Part VII. Selected Topics

Chapter 34 NP-Completeness

1. Intractable problems
   - decision versions of optimization problems

2. Nondeterministic computational models
   - nondeterministic computation = certificate + verification

3. NP-completeness framework
   - reduction, polynomial-time reduction
Chapter 34 NP-Completeness

1. Intractable problems
   • decision versions of optimization problems

2. Nondeterministic computational models
   • nondeterministic computation = certificate + verification

3. NP-completeness framework
   • reduction, polynomial-time reduction

4. NP-completeness proof
Part VII. Selected Topics

Chapter 34 NP-Completeness

1. Intractable problems
   • decision versions of optimization problems

2. Nondeterministic computational models
   • nondeterministic computation = certificate + verification

3. NP-completeness framework
   • reduction, polynomial-time reduction

4. NP-completeness proof
   • NP-complete problems, reduction techniques.
Chapter 34. NP-Completeness

1. Intractable problems
   - We have seen many problems solvable in polynomial time, e.g., sorting, SCC, MST.
   - There are problems that do not seem to have polynomial time algorithms, i.e., not solvable in time $O(n \log n)$, $O(n^3)$, or $O(n^{100})$.
   - Why would a time $O(n^{100})$-time algorithm be attractive? Only theoretical? Practical significance as well.
Chapter 34. NP-Completeness

1. Intractable problems
   - We have seen many problems solvable in polynomial time, e.g., sorting, SCC, MST.
   - There are problems that do not seem to have polynomial time algorithms, i.e., not solvable in time \(O(n \log n),\) \(O(n^3),\) or \(O(n^{100})\).
   - Why would a time \(O(n^{100})\)-time algorithm be attractive? Only theoretical? Practical significance as well.
Chapter 34. NP-Completeness

1. Intractable problems
Chapter 34. NP-Completeness

1. Intractable problems

- we have seen many problems solvable in polynomial time
1. Intractable problems

- we have seen many problems solvable in polynomial time
  e.g., sorting, SCC, MST
Chapter 34. NP-Completeness

1. Intractable problems

- we have seen many problems solvable in polynomial time
  e.g., sorting, SCC, MST

- there are problems that do not seem to have polynomial time algorithms
Chapter 34. NP-Completeness

1. Intractable problems

- we have seen many problems solvable in polynomial time
e.g., sorting, SCC, MST

- there are problems that do not seem to have polynomial time algorithms
  i.e., not solvable in time $O(n \log n)$,
Chapter 34. NP-Completeness

1. Intractable problems

- we have seen many problems solvable in polynomial time
  e.g., sorting, SCC, MST

- there are problems that do not seem to have polynomial time algorithms
  i.e., not solvable in time $O(n \log n)$, $O(n^3)$, or
Chapter 34. NP-Completeness

1. Intractable problems

• we have seen many problems solvable in polynomial time
e.g., sorting, SCC, MST

• there are problems that do not seem to have polynomial time algorithms
  i.e., not solvable in time $O(n \log n)$, $O(n^3)$, or $O(n^{100})$. 
Chapter 34. NP-Completeness

1. Intractable problems

- we have seen many problems solvable in polynomial time
  e.g., sorting, SCC, MST

- there are problems that do not seem to have polynomial time algorithms
  i.e., not solvable in time $O(n \log n)$, $O(n^3)$, or $O(n^{100})$.

- why would a time $O(n^{100})$-time algorithm be attractive?
Chapter 34. NP-Completeness

1. Intractable problems

- we have seen many problems solvable in polynomial time
  e.g., sorting, SCC, MST

- there are problems that do not seem to have polynomial time algorithms
  i.e., not solvable in time $O(n \log n)$, $O(n^3)$, or $O(n^{100})$.

- why would a time $O(n^{100})$-time algorithm be attractive?
  only theoretical?
Chapter 34. NP-Completeness

1. Intractable problems

• we have seen many problems solvable in polynomial time
  e.g., sorting, SCC, MST

• there are problems that do not seem to have polynomial time algorithms
  i.e., not solvable in time $O(n \log n)$, $O(n^3)$, or $O(n^{100})$.

• why would a time $O(n^{100})$-time algorithm be attractive?
  only theoretical? practical significance as well
Chapter 34. NP-Completeness

Define: a Hamiltonian cycle in a graph is a circular path going through every vertex exactly once. Different from an Eulerian cycle that goes through every edge exactly once.
Chapter 34. NP-Completeness

Define: a Hamiltonian cycle in a graph is a circular path going through every vertex exactly once.
Chapter 34. NP-Completeness

Define: a Hamiltonian cycle in a graph is a circular path going through every vertex exactly once.
Define: a Hamiltonian cycle in a graph is a circular path going through every vertex exactly once.

Different from Eulerian cycle that goes through every edge exactly once.
Define: a Hamiltonian cycle in a graph is a circular path going through every vertex exactly once.

Different from Eulerian cycle that goes through every edge exactly once.
Chapter 34. NP-Completeness

Travel Salesman Problem (TSP)

Input: an edge-weighted graph \( G = (V, E) \);
Output: a Hamiltonian cycle of the minimum weight sum.

- Intuitively, a circular path is a permutation of \( (v_1, v_2, \ldots, v_n) \) or simply a permutation of \( (1, 2, \ldots, n) \), where \(|V| = n\).

So the problem has time upper bound \( O(n! \cdot |E|) \), exponential time.

\[ n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 \geq n \times (n-1) \times \cdots \times n^2 \geq (n^2)^n \]

All known algorithms (solving TSP) are of exponential-time.
Chapter 34. NP-Completeness

Travel Salesman Problem (TSP)

Input: an edge-weighted graph $G = (V, E)$;

Intuitively, a circular path is a permutation of $(v_1, v_2, ..., v_n)$ or simply a permutation of $(1, 2, ..., n)$, where $|V| = n$.

So the problem has time upper bound $O(n! |E|)$, exponential time.

$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 \geq n \times (n-1) \cdots \times n^2 \geq (n^2)^n$.

All known algorithms (solving TSP) are of exponential-time.
Chapter 34. NP-Completeness

**Travel Salesman Problem (TSP)**

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.

Intuitively, a circular path is a permutation of $(v_1, v_2, ..., v_n)$ or simply a permutation of $(1, 2, ..., n)$, where $|V| = n$.

The problem has time upper bound $O(n! |E|)$, exponential time.

$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 \geq n \times (n-1) \times \cdots \times n^2 \geq (n^2)^n$.

All known algorithms (solving TSP) are of exponential-time.
Chapter 34. NP-Completeness

**Travel Salesman Problem (TSP)**

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.

- intuitively, a circular path is a permutation of $(v_1, v_2, \ldots, v_n)$ or simply a permutation of $(1, 2, \ldots, n)$, where $|V| = n$. 

$\prod_{i=1}^{n} 1 \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 \geq (n^2)^{n/2}$

\[ n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 \geq n \times (n-1) \times \cdots \times n^2 \geq (n^2)^{n/2} \]

\[ O(n!) \times |E| \]

\[ O(n^n) \text{ exponential time.} \]

\[ \text{all known algorithms (solving TSP)} \text{ are of exponential-time.} \]
Travel Salesman Problem (TSP)

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.

- intuitively, a circular path is a permutation of $(v_1, v_2, \ldots, v_n)$ or simply a permutation of $(1, 2, \ldots, n)$, where $|V| = n$. so the problem has time upper bound $O(n!|E|)$, exponential time.
Chapter 34. NP-Completeness

**Travel Salesman Problem (TSP)**

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.

- intuitively, a circular path is a permutation of $(v_1, v_2, \ldots, v_n)$ or simply a permutation of $(1, 2, \ldots, n)$, where $|V| = n$. so the problem has time upper bound $O(n!|E|)$, exponential time.

$$n! = n \times (n - 1) \times (n - 2) \times \cdots \times 2 \times 1 \geq n \times (n - 1) \cdots \times \frac{n}{2} \geq \left(\frac{n}{2}\right)^{\frac{n}{2}}$$

- all known algorithms (solving TSP) are of exponential-time.
Chapter 34. NP-Completeness

Instead of considering the Travel Salesman Problem (TSP),

Input: an edge-weighted graph \( G = (V, E) \);

Output: a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:

H-Cycle Weight Decision (HCW)

Input: an edge-weighted graph \( G = (V, E) \), a weight value \( K \);

Output: "YES" if and only if there is a Hamiltonian cycle of weight \( \leq K \) in \( G \).

- HCW appears to "easier" than TSP as an H-cycle is not produced in the answer.
- However, HCW may not be "easier".

Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.
Chapter 34. NP-Completeness

Instead of considering

Travel Salesman Problem (TSP)

Input: an edge-weighted graph $G = (V,E)$
Output: a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem: H-Cycle Weight Decision (HCW)

Input: an edge-weighted graph $G = (V,E)$, a weight value $K$
Output: "YES" if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

• HCW appears to "easier" than TSP as an H-cycle is not produced in the answer.
• However, HCW may not be "easier"

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.
Instead of considering

**Travel Salesman Problem (TSP)**

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.
Instead of considering

**Travel Salesman Problem (TSP)**

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:
Chapter 34. NP-Completeness

Instead of considering

Travel Salesman Problem (TSP)

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:

H-Cycle Weight Decision (HCW)

**Input:** an edge-weighted graph $G = (V, E)$, a weight value $K$;

- HCW appears to “easier” than TSP as an H-cycle is not produced in the answer.
- However, HCW may not be “easier”

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.
Instead of considering

**Travel Salesman Problem (TSP)**
- **Input:** an edge-weighted graph $G = (V, E)$;
- **Output:** a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:

**H-Cycle Weight Decision (HCW)**
- **Input:** an edge-weighted graph $G = (V, E)$, a weight value $K$;
- **Output:** “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$. 

Instead of considering

**Travel Salesman Problem (TSP)**
- **Input**: an edge-weighted graph $G = (V, E)$;
- **Output**: a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:

**H-Cycle Weight Decision (HCW)**
- **Input**: an edge-weighted graph $G = (V, E)$, a weight value $K$;
- **Output**: “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

- **HCW appears to “easier”** than TSP as an H-cycle is not produced in the answer.
Instead of considering

**Travel Salesman Problem (TSP)**
- **Input**: an edge-weighted graph $G = (V, E)$;
- **Output**: a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:

**H-Cycle Weight Decision (HCW)**
- **Input**: an edge-weighted graph $G = (V, E)$, a weight value $K$;
- **Output**: “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

- **HCW appears to “easier”** than TSP as an H-cycle is not produced in the answer.

- **However, HCW may not be “easier”**
Instead of considering

**Travel Salesman Problem (TSP)**
- **Input:** an edge-weighted graph $G = (V, E)$;
- **Output:** a Hamiltonian cycle of the minimum weight sum.

We may consider a related problem:

**H-Cycle Weight Decision (HCW)**
- **Input:** an edge-weighted graph $G = (V, E)$, a weight value $K$;
- **Output:** “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

- HCW appears to “easier” than TSP as an H-cycle is not produced in the answer.
- However, HCW may not be “easier”

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially,
Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially, P-time algorithms for TSP
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially, P-time algorithms for TSP $\implies$ P-time algorithms for HCW,
Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially, P-time algorithms for TSP $\implies$ P-time algorithms for HCW, why?
Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially, P-time algorithms for TSP $\implies$ P-time algorithms for HCW, why?

How to prove:
Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially, P-time algorithms for TSP $\implies$ P-time algorithms for HCW, why?

How to prove: P-time algorithms for TSP
Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Trivially, P-time algorithms for TSP $\implies$ P-time algorithms for HCW, why?

How to prove: P-time algorithms for TSP $\iff$ P-time algorithms for HCW?
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)
- assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/“NO”
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP \(\iff\) P-time algorithms for HCW)

- assume P-time algorithm \(A\) for HCW such that \(A(G, K) = \text{"YES/"NO}\)
- construct a P-time algorithm \(B(G)\) for TSP to behave as follows:
Chapter 34. NP-Completeness

Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Proof: (P-time algorithms for TSP ⇐ P-time algorithms for HCW)

1. assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/“NO"
2. construct a P-time algorithm $B(G)$ for TSP to behave as follows:

   1. on input $G$, for every possible values of $K$, call $A(G, K)$;
Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Proof: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/“NO”
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

  1. on input $G$, for every possible values of $K$, call $A(G, K)$;
     remember the smallest $k_{min}$ such that $A(G, k_{min}) =$ “YES”.

How to make Step 1 P-time?
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time **if and only if** TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) = \text{"YES"/"NO"}$
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

  1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) = \text{"YES"}$.
Chapter 34. NP-Completeness

Theorem 1: HCW is solvable in P-time if and only if TSP is solvable in P-time.

Proof: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

• assume P-time algorithm $A$ for HCW such that $A(G, K) = \text{"YES/"NO}^$

• construct a P-time algorithm $B(G)$ for TSP to behave as follows:

1. on input $G$, for every possible values of $K$, call $A(G, K)$;
   remember the smallest $k_{\text{min}}$ such that $A(G, k_{\text{min}}) = \text{"YES"}^$.

2. mark all edges in $G$ as “unvisited”;

   How to make Step 1 P-time?
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/NO”
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

  1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) =$ “YES”.

  2. mark all edges in $G$ as “unvisited”; while there are “unvisited” edges in $G$
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- Assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/ “NO”
- Construct a P-time algorithm $B(G)$ for TSP to behave as follows:
  1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) =$ “YES”.
  2. mark all edges in $G$ as “unvisited”; while there are “unvisited” edges in $G$ pick an “unvisited” edge $(u, v)$, mark it “visited”;
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP \(\iff\) P-time algorithms for HCW)

- assume P-time algorithm \(A\) for HCW such that \(A(G,K) = \text{"YES/"NO"}\)
- construct a P-time algorithm \(B(G)\) for TSP to behave as follows:

1. on input \(G\), for every possible values of \(K\), call \(A(G,K)\);
   remember the smallest \(k_{\text{min}}\) such that \(A(G,k_{\text{min}}) = \text{"YES"}\).

2. mark all edges in \(G\) as “unvisited”;
   while there are “unvisited” edges in \(G\)
     pick an “unvisited” edge \((u,v)\), mark it “visited”;
   let \(G' = G - \{(u,v)\}\);
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/NO”
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

1. on input $G$, for every possible values of $K$, call $A(G, K)$;
   remember the smallest $k_{min}$ such that $A(G, k_{min}) =$ “YES”.

2. mark all edges in $G$ as “unvisited”;
   while there are “unvisited” edges in $G$
      pick an “unvisited” edge $(u, v)$, mark it “visited”;
      let $G' = G - \{(u, v)\}$;
   if $A(G', k_{min}) =$ “YES”
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) =$“YES/“NO"
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

  1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) =$“YES”.

  2. mark all edges in $G$ as “unvisited”;
     while there are “unvisited” edges in $G$
     pick an “unvisited” edge $(u, v)$, mark it “visited”;
     let $G' = G - \{(u, v)\}$;
     if $A(G', k_{min}) =$ “YES”
     then $G = G'$;
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) = \text{"YES/"NO}$
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

1. on input $G$, for every possible values of $K$, call $A(G, K)$;
   remember the smallest $k_{min}$ such that $A(G, k_{min}) = \text{"YES"}$.

2. mark all edges in $G$ as “unvisited”;
   while there are “unvisited” edges in $G$
   pick an “unvisited” edge $(u, v)$, mark it “visited”;
   let $G' = G - \{(u, v)\}$;
   if $A(G', k_{min}) = \text{"YES"}$
   then $G = G'$;
   else mark $(u, v)$ “critical”;

How to make Step 1 P-time?

Theorem 1 says problems HCW and TSP are “polynomially equivalent.”
Chapter 34. NP-Completeness

**Theorem 1:** HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof:** (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) = “YES/NO”$
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) = “YES”$.

2. mark all edges in $G$ as “unvisited”; while there are “unvisited” edges in $G$
   pick an “unvisited” edge $(u, v)$, mark it “visited”;
   let $G' = G - \{(u, v)\}$;
   if $A(G', k_{min}) = “YES”$
   then $G = G'$;
   else mark $(u, v)$ “critical”;

return (all “critical” edges)
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP ⇐ P-time algorithms for HCW)

- assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/“NO"
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{\text{min}}$ such that $A(G, k_{\text{min}}) =$ “YES”.
2. mark all edges in $G$ as “unvisited”; while there are “unvisited” edges in $G$
   - pick an “unvisited” edge $(u, v)$, mark it “visited”; let $G' = G - \{(u, v)\}$;
   - if $A(G', k_{\text{min}}) = $ “YES”
     - then $G = G'$;
   - else mark $(u, v)$ “critical”;
   return (all “critical” edges)

- show algorithm $B$ runs in P-time.
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)
- assume P-time algorithm $A$ for HCW such that $A(G, K) =$ “YES/“NO”
- construct a P-time algorithm $B(G)$ for TSP to behave as follows:

1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) =$ “YES”.

2. mark all edges in $G$ as “unvisited”;
   - while there are “unvisited” edges in $G$
     - pick an “unvisited” edge $(u, v)$, mark it “visited”;
     - let $G' = G - \{(u, v)\}$;
     - if $A(G', k_{min}) =$ “YES”
       - then $G = G'$;
     - else mark $(u, v)$ “critical”;
   - return (all “critical” edges)

- show algorithm $B$ runs in P-time. How to make Step 1 P-time?
Chapter 34. NP-Completeness

**Theorem 1**: HCW is solvable in P-time if and only if TSP is solvable in P-time.

**Proof**: (P-time algorithms for TSP $\iff$ P-time algorithms for HCW)

- Assume P-time algorithm $A$ for HCW such that $A(G, K) = \text{"YES/NO"}$
- Construct a P-time algorithm $B(G)$ for TSP to behave as follows:

  1. on input $G$, for every possible values of $K$, call $A(G, K)$; remember the smallest $k_{min}$ such that $A(G, k_{min}) = \text{"YES"}$.

  2. mark all edges in $G$ as “unvisited”; while there are “unvisited” edges in $G$
     - pick an “unvisited” edge $(u, v)$, mark it “visited”;
     - let $G' = G - \{(u, v)\};$
     - if $A(G', k_{min}) = \text{"YES"}$
       - then $G = G'$;
     - else mark $(u, v)$ “critical”;
     - return (all “critical” edges)

- Show algorithm $B$ runs in P-time. How to make Step 1 P-time?

Theorem 1 says problems HCW and TSP are “polynomially equivalent”.

[Translation note: The first paragraph is translated as is, the second paragraph is translated with minor adjustments for clarity. The third paragraph is translated with a focus on improving the flow of the text.]
Consider another related problem:

**H-Cycle Decision (HC)**

**Input:** an edge-weighted graph $G = (V,E)$

**Output:** "YES" if and only there is a Hamiltonian cycle in $G$.

Compared with **H-Cycle Weight Decision (HCW)**

**Input:** an edge-weighted graph $G = (V,E)$, a weight value $K$

**Output:** "YES" if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

• Which problem is seemingly "easier"?

**Theorem 2:** HCW is P-time solvable if and only if HC is P-time solvable.

Can you prove it?

**Theorem 2** says problems HCW and HC are "polynomially equivalent".
Consider another related problem:

**H-Cycle Decision (HC)**

**Input:** an edge-weighted graph $G = (V, E)$;

Compared with **H-Cycle Weight Decision (HCW)**

**Input:** an edge-weighted graph $G = (V, E)$, a weight value $K$;

**Output:** “YES” if and only if there is a Hamiltonian cycle of weight $\leq K$ in $G$.

• Which problem is seemingly “easier”?

Theorem 2: **HCW** is P-time solvable if and only if **HC** is P-time solvable.

Can you prove it?

Theorem 2 says problems **HCW** and **HC** are "polynomially equivalent".
Consider another related problem:

**H-Cycle Decision (HC)**

**Input**: an edge-weighted graph $G = (V, E)$;

**Output**: “YES” if and only there is a Hamiltonian cycle in $G$.
Chapter 34. NP-Completeness

Consider another related problem:

**H-Cycle Decision (HC)**

**Input:** an edge-weighted graph \( G = (V, E) \);

**Output:** “YES” if and only there is a Hamiltonian cycle in \( G \).

Compared with
Chapter 34. NP-Completeness

Consider another related problem:

**H-Cycle Decision (HC)**
- **Input**: an edge-weighted graph $G = (V, E)$;
- **Output**: “YES” if and only there is a Hamiltonian cycle in $G$.

Compared with

**H-Cycle Weight Decision (HCW)**
- **Input**: an edge-weighted graph $G = (V, E)$, a weight value $K$;
- **Output**: “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

\[\text{Theorem 2: HCW is P-time solvable if and only if HC is P-time solvable.}\]
Consider another related problem:

**H-Cycle Decision (HC)**
- **Input:** an edge-weighted graph \( G = (V, E) \);
- **Output:** “YES” if and only there is a Hamiltonian cycle in \( G \).

Compared with

**H-Cycle Weight Decision (HCW)**
- **Input:** an edge-weighted graph \( G = (V, E) \), a weight value \( K \);
- **Output:** “YES” if and only there is a Hamiltonian cycle of weight \( \leq K \) in \( G \).

- Which problem is seemingly “easier”? 

---

**Theorem 2**: \( HCW \) is P-time solvable if and only if \( HC \) is P-time solvable. Can you prove it? 

Theorem 2 says problems \( HCW \) and \( HC \) are “polynomially equivalent.”
Consider another related problem:

**H-Cycle Decision (HC)**
- **Input**: an edge-weighted graph $G = (V, E)$;
- **Output**: “YES” if and only there is a Hamiltonian cycle in $G$.

Compared with

**H-Cycle Weight Decision (HCW)**
- **Input**: an edge-weighted graph $G = (V, E)$, a weight value $K$;
- **Output**: “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

- Which problem is seemingly “easier”?

**Theorem 2**: HCW is P-time solvable if and only if HC is P-time solvable.
Consider another related problem:

**H-Cycle Decision (HC)**
- **Input**: an edge-weighted graph \( G = (V, E) \);
- **Output**: “YES” if and only there is a Hamiltonian cycle in \( G \).

Compared with

**H-Cycle Weight Decision (HCW)**
- **Input**: an edge-weighted graph \( G = (V, E) \), a weight value \( K \);
- **Output**: “YES” if and only there is a Hamiltonian cycle of weight \( \leq K \) in \( G \).

- Which problem is seemingly “easier”?

**Theorem 2**: HCW is P-time solvable if and only if HC is P-time solvable.

*Can you prove it?*
Consider another related problem:

**H-Cycle Decision (HC)**

**Input:** an edge-weighted graph $G = (V, E)$;

**Output:** “YES” if and only there is a Hamiltonian cycle in $G$.

Compared with

**H-Cycle Weight Decision (HCW)**

**Input:** an edge-weighted graph $G = (V, E)$, a weight value $K$;

**Output:** “YES” if and only there is a Hamiltonian cycle of weight $\leq K$ in $G$.

• Which problem is seemingly “easier”?

**Theorem 2:** HCW is P-time solvable if and only if HC is P-time solvable.

Can you prove it?

Theorem 2 says problems HCW and HC are “polynomially equivalent”.
Chapter 34. NP-Completeness

**Corollary 3:** Problems TSP, HCW, and HC are all “polynomially equivalent”.

**Theorem 4:** \(\text{MaxIS} \) is P-time solvable if and only if \(\text{IS} \) is P-time solvable.

Can you prove the theorem?
Corollary 3: Problems TSP, HCW, and HC are all “polynomially equivalent”.

There are other problems that have the similar situation.
Corollary 3: Problems TSP, HCW, and HC are all “polynomially equivalent”.

There are other problems that have the similar situation.

Max Independent Set (MaxIS)
Input: graph $G = (V, E)$;
Chapter 34. NP-Completeness

Corollary 3: Problems TSP, HCW, and HC are all “polynomially equivalent”.

There are other problems that have the similar situation.

Max Independent Set (MaxIS)
Input: graph $G = (V, E)$;
Output: an independent set of vertices of the maximum size;
Chapter 34. NP-Completeness

**Corollary 3:** Problems TSP, HCW, and HC are all “polynomially equivalent”.

There are other problems that have the similar situation.

**Max Independent Set (MaxIS)**

**Input:** graph $G = (V, E)$;

**Output:** an independent set of vertices of the maximum size;

**Independent Set (IS)**

**Input:** graph $G = (V, E)$, integer $k$;
Corollary 3: Problems TSP, HCW, and HC are all “polynomially equivalent”.

There are other problems that have the similar situation.

**Max Independent Set (MaxIS)**
- **Input:** graph $G = (V, E)$;
- **Output:** an independent set of vertices of the maximum size;

**Independent Set (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$. 
Chapter 34. NP-Completeness

**Corollary 3:** Problems TSP, HCW, and HC are all “polynomially equivalent”.

There are other problems that have the similar situation.

**Max Independent Set (MaxIS)**
- **Input:** graph $G = (V, E)$;
- **Output:** an independent set of vertices of the maximum size;

**Independent Set (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$.

**Theorem 4:** MaxIS is P-time solvable if and only if IS is P-time solvable.
Chapter 34. NP-Completeness

**Corollary 3:** Problems TSP, HCW, and HC are all "polynomially equivalent".

There are other problems that have the similar situation.

**Max Independent Set (MaxIS)**
- **Input:** graph $G = (V, E)$;
- **Output:** an independent set of vertices of the maximum size;

**Independent Set (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$.

**Theorem 4:** MaxIS is P-time solvable if and only if IS is P-time solvable.

Can you prove the theorem?
Chapter 34. NP-Completeness

Similarly,
Similarly,

**Min Vertex Cover (MinVC)**

**Input:** graph $G = (V, E)$;

**Theorem 5:** MinVC is P-time solvable if and only if VC is P-time solvable.

Can you prove the theorem?
Similarly,

**Min Vertex Cover (MinVC)**

**Input:** graph $G = (V, E)$;

**Output:** a vertex cover set of vertices of the minimum size;
Similarly,

**Min Vertex Cover (MinVC)**
- **Input**: graph $G = (V, E)$;
- **Output**: a vertex cover set of vertices of the minimum size;

**Vertex Cover (VC)**
- **Input**: graph $G = (V, E)$, integer $k$;
Chapter 34. NP-Completeness

Similarly,

**Min Vertex Cover (MinVC)**
- **Input:** graph $G = (V, E)$;
- **Output:** a vertex cover set of vertices of the minimum size;

**Vertex Cover (VC)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has a vertex cover of size $\leq k$. 

Theorem 5: MinVC is P-time solvable if and only if VC is P-time solvable.

Can you prove the theorem?
Similarly,

\textbf{Min Vertex Cover (MinVC)}
\begin{itemize}
  \item \textbf{Input:} graph \( G = (V, E) \);
  \item \textbf{Output:} a vertex cover set of vertices of the minimum size;
\end{itemize}

\textbf{Vertex Cover (VC)}
\begin{itemize}
  \item \textbf{Input:} graph \( G = (V, E) \), integer \( k \);
  \item \textbf{Output:} \textit{"YES" if and only if} \( G \) has a vertex cover of size \( \leq k \).
\end{itemize}

\textbf{Theorem 5:} \textbf{MinVC} is P-time solvable \textbf{if and only if} \textbf{VC} is P-time solvable.
Similarly,

**Min Vertex Cover (MinVC)**
- **Input:** graph $G = (V, E)$;
- **Output:** a vertex cover set of vertices of the minimum size;

**Vertex Cover (VC)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has a vertex cover of size $\leq k$.

**Theorem 5:** MinVC is P-time solvable if and only if VC is P-time solvable.

Can you prove the theorem?
Conclusions:

1. "Polynomial equivalency" can be established between optimization problems and decision problems. To study tractability of optimization problems, often it suffices to investigate decision problems. (Decision problems are also called languages.)

2. "Polynomial equivalency" can also be established between different decision problems, e.g., Corollary 6: \( VC \) is P-time solvable if and only if \( IS \) is P-time solvable.

3. However, "Polynomial equivalency" does not tell us the tractability of the problems.

4. We need a rigorous framework to study tractability via the notion "Polynomial equivalency".
Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.
Chapter 34. NP-Completeness

Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.

   To study tractability of optimization problems, often it suffices to investigate decision problems.
Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.

   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)
Chapter 34. NP-Completeness

Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.

   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)

2. “Polynomial equivalency” can also be established
Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.
   
   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)

2. “Polynomial equivalency” can also be established between different decision problems,
Chapter 34. NP-Completeness

Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.
   
   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)

2. “Polynomial equivalency” can also be established between different decision problems, e.g.,
Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.

   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)

2. “Polynomial equivalency” can also be established between different decision problems, e.g.,

   **Corollary 6:** VC is P-time solvable if and only if IS is P-time solvable.
Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.

   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)

2. “Polynomial equivalency” can also be established between different decision problems, e.g.,

   **Corollary 6:** VC is P-time solvable if and only if IS is P-time solvable.

3. However, “Polynomial equivalency” does not tell us the tractability of the problems.
Conclusions:

1. “Polynomial equivalency” can be established between optimization problems and decision problems.
   
   To study tractability of optimization problems, often it suffices to investigate decision problems.
   (Decision problems are also called languages.)

2. “Polynomial equivalency” can also be established between different decision problems, e.g.,

   **Corollary 6**: VC is P-time solvable if and only if IS is P-time solvable.

3. However, “Polynomial equivalency” does not tell us the tractability of the problems.

4. We need a rigorous framework to study tractability via the notion “Polynomial equivalency”.
2. Nondeterministic algorithms

Deterministic algorithms

- Given input data, a deterministic algorithm has its every step completely determined by the algorithm and data.
- All algorithms we have seen so far are deterministic.
- Every deterministic algorithm can be unfolded into a linear sequence of steps (when the input is given).
Chapter 34. NP-Completeness

2. Nondeterministic algorithms

Deterministic algorithms
Chapter 34. NP-Completeness

2. Nondeterministic algorithms

Deterministic algorithms

• Given input data, a deterministic algorithm has its every step completely determined by the algorithm and data.
Chapter 34. NP-Completeness

2. Nondeterministic algorithms

Deterministic algorithms

- Given input data, a deterministic algorithm has its every step completely determined by the algorithm and data.
- All algorithms we have seen so far are deterministic.
Chapter 34. NP-Completeness

2. Nondeterministic algorithms

Deterministic algorithms

- Given input data, a deterministic algorithm has its every step completely determined by the algorithm and data.

- All algorithms we have seen so far are deterministic.

- Every deterministic algorithm can be unfolded into a linear sequence of steps (when the input is given).

```plaintext
M = -\infty
n = 3
i = 1
check 1 \leq 3
check -\infty < 10
M = 10
i = 2
check 2 \leq 3
check 10 < 30
M = 30
i = 3
check 3 \leq 3
check 30 < 20
i = 4
check 4 \leq 3
return (30)
```

Unfolded when input $L = (10, 30, 20)$
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps;
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.
A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.

Let us call this tree model of nondeterministic algorithms.
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.
- each step has more than one nondeterministic choice.
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.
- each step has more than one nondeterministic choice.
- a path from root to a leaf is a sequence of nondeterministic choices;
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.
- each step has more than one nondeterministic choice.
- a path from root to a leaf is a sequence of nondeterministic choices; thus a nondeterministic execution of the algorithm.
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.
- each step has more than one nondeterministic choice.
- a path from root to a leaf is a sequence of nondeterministic choices; thus a nondeterministic execution of the algorithm.
- algorithm answers “YES” if one execution path leads to “YES”.

Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.
- each step has more than one nondeterministic choice.
- a path from root to a leaf is a sequence of nondeterministic choices; thus a nondeterministic execution of the algorithm.
- algorithm answers “YES” if one execution path leads to “YES”.
- the running time is the number of steps on a longest path.
Chapter 34. NP-Completeness

A deterministic algorithm can be thought of a linear path of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a nondeterministic algorithm, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a tree of steps.
- each step has more than one nondeterministic choice.
- a path from root to a leaf is a sequence of nondeterministic choices; thus a nondeterministic execution of the algorithm.

- algorithm answers “YES” if one execution path leads to “YES”.
- the running time is the number of steps on a longest path.
- if running time is $n$, there may be $\geq 2^n$ paths.
Chapter 34. NP-Completeness

A **deterministic algorithm** can be thought of a **linear path** of steps; each vertex uniquely determines its successor step.

- the running time is the number of steps on the path.

In a **nondeterministic algorithm**, when unfolded, there may be more than one possible successor.

- a nondeterministic algorithm can be thought of a **tree** of steps.
- each step has more than one **nondeterministic** choice.
- a path from root to a leaf is a sequence of nondeterministic choices; thus a nondeterministic execution of the algorithm.
- algorithm answers “YES” if one execution path leads to “YES”.
- the running time is the number of steps on a **longest path**.
- if running time is $n$, there may be $\geq 2^n$ paths.

Let us call this **tree model** of nondeterministic algorithms.
Chapter 34. NP-Completeness

Deterministic

\[ f(n) \]

Non Deterministic

\[ f(n) \]

yes

no
Use nondeterministic algorithms to solve problem Hamiltonian Cycle.
Use **nondeterministic algorithms** to solve problem **Hamiltonian Cycle** in polynomial time.
Use nondeterministic algorithms to solve problem Hamiltonian Cycle in polynomial time.

1. starting from any vertex \( v \) in the graph;
Chapter 34. NP-Completeness

Use **nondeterministic algorithms** to solve problem **Hamiltonian Cycle** in polynomial time.

(1) starting from any vertex $v$ in the graph;
(2) nondeterministically choose one of its (at most $n - 1$) neighbors which has not been chosen;
Chapter 34. NP-Completeness

Use nondeterministic algorithms to solve problem Hamiltonian Cycle in polynomial time.

(1) starting from any vertex \( v \) in the graph;
(2) nondeterministically choose one of its (at most \( n - 1 \)) neighbors which has not been chosen;
   let the newly picked vertex be \( v \), go to step (2)
Chapter 34. NP-Completeness

Use nondeterministic algorithms to solve problem Hamiltonian Cycle in polynomial time.

(1) starting from any vertex \( v \) in the graph;
(2) nondeterministically choose one of its (at most \( n - 1 \)) neighbors which has not been chosen;
   let the newly picked vertex be \( v \), go to step (2)
(3) if all vertices have been chosen,
   return “YES” if their edges form an H-cycle;
   return “NO” if their edges do NOT form an H-cycle;
Use **nondeterministic algorithms** to solve problem **Hamiltonian Cycle** in polynomial time.

(1) starting from any vertex \( v \) in the graph;
(2) nondeterministically choose one of its (at most \( n - 1 \)) neighbors which has not been chosen;
   let the newly picked vertex be \( v \), go to step (2)
(3) if all vertices have been chosen,
   return “YES” if their edges form an H-cycle;
   return “NO” if their edges do NOT form an H-cycle;

• The algorithm will answer “YES” iff there is a H-cycle in \( G \).
Chapter 34. NP-Completeness

Use **nondeterministic algorithms** to solve problem **Hamiltonian Cycle** in polynomial time.

1. starting from any vertex \( v \) in the graph;
2. nondeterministically choose one of its (at most \( n - 1 \)) neighbors which has not been chosen;
   let the newly picked vertex be \( v \), go to step (2)
3. if all vertices have been chosen,
   return “YES” if their edges form an H-cycle;
   return “NO” if their edges do NOT form an H-cycle;

- The algorithm will answer “YES” iff there is a H-cycle in \( G \).
  Because each path try one permutation of vertices.
Use nondeterministic algorithms to solve problem Hamiltonian Cycle in polynomial time.

(1) starting from any vertex \( v \) in the graph;
(2) nondeterministically choose one of its (at most \( n - 1 \)) neighbors which has not been chosen;
    let the newly picked vertex be \( v \), \textbf{go to} step (2)
(3) if all vertices have been chosen,
    \textbf{return} “YES” if their edges form an H-cycle;
    \textbf{return} “NO” if their edges do NOT form an H-cycle;

• The algorithm will answer “YES” iff there is a H-cycle in \( G \).
  Because each path try one permutation of vertices.
• The algorithm runs in polynomial time as each path takes \( O(n) \) steps.
Problems like Independent Set, Vertex Cover, HCW can all be solved with nondeterministic algorithms in polynomial time.
Chapter 34. NP-Completeness

Problems like **Independent Set**, **Vertex Cover**, **HCW** can all be solved with **nondeterministic algorithms** in **polynomial time**.

**Can you prove the claim?**
Chapter 34. NP-Completeness

**Definition:** \( \mathcal{P} \) is the class of languages (i.e., decision problems) that can be solved by deterministic polynomial-time algorithms.
Chapter 34. NP-Completeness

**Definition:** $\mathcal{P}$ is the class of languages (i.e., decision problems) that can be solved by *deterministic polynomial-time algorithms*.

- class $\mathcal{P}$ contains problems like \textsc{Reachability}
Chapter 34. NP-Completeness

**Definition**: $\mathcal{P}$ is the class of languages (i.e., decision problems) that can be solved by deterministic polynomial-time algorithms.

- class $\mathcal{P}$ contains problems like **Reachability** and many others.
Chapter 34. NP-Completeness

**Definition:** \( \mathcal{P} \) is the class of languages (i.e., decision problems) that can be solved by **deterministic polynomial-time algorithms**.

- class \( \mathcal{P} \) contains problems like \textsc{Reachability} and many others.

**Definition:** \( \mathcal{NP} \) is the class of languages (i.e., decision problems) that can be solved by **nondeterministic polynomial-time algorithms**.
Chapter 34. NP-Completeness

**Definition**: $\mathcal{P}$ is the class of languages (i.e., decision problems) that can be solved by deterministic polynomial-time algorithms.

- class $\mathcal{P}$ contains problems like Reachability and many others.

**Definition**: $\mathcal{NP}$ is the class of languages (i.e., decision problems) that can be solved by nondeterministic polynomial-time algorithms.

- class $\mathcal{NP}$ contains problems like VC, HC, IS and many others.

Because every deterministic algorithm is a special case of a nondeterministic algorithm, $\mathcal{P} \subseteq \mathcal{NP}$.
Chapter 34. NP-Completeness

**Definition:** \( \mathcal{P} \) is the class of languages (i.e., decision problems) that can be solved by **deterministic polynomial-time algorithms**.

- class \( \mathcal{P} \) contains problems like \textsc{Reachability} and many others.

**Definition:** \( \mathcal{NP} \) is the class of languages (i.e., decision problems) that can be solved by **nondeterministic polynomial-time algorithms**.

- class \( \mathcal{NP} \) contains problems like \textsc{VC}, \textsc{HC}, \textsc{IS} and many others.

Because every deterministic algorithm is a special case of a nondeterministic algorithm,

\[
\mathcal{P} \subseteq \mathcal{NP}
\]
Chapter 34. NP-Completeness

Definition: $\mathcal{P}$ is the class of languages (i.e., decision problems) that can be solved by deterministic polynomial-time algorithms.

- class $\mathcal{P}$ contains problems like Reachability and many others.

Definition: $\mathcal{NP}$ is the class of languages (i.e., decision problems) that can be solved by nondeterministic polynomial-time algorithms.

- class $\mathcal{NP}$ contains problems like VC, HC, IS and many others.

Because every deterministic algorithm is a special case of a nondeterministic algorithm,

$$\mathcal{P} \subseteq \mathcal{NP}$$
Chapter 34. NP-Completeness

**Definition:** \( P \) is the class of languages (i.e., decision problems) that can be solved by **deterministic polynomial-time algorithms**.

- class \( P \) contains problems like **Reachability** and many others.

**Definition:** \( NP \) is the class of languages (i.e., decision problems) that can be solved by **nondeterministic polynomial-time algorithms**.

- class \( NP \) contains problems like **VC**, **HC**, **IS** and many others.

Because every deterministic algorithm is a special case of a nondeterministic algorithm,

\[ P \subseteq NP \]
Chapter 34. NP-Completeness

**Definition**: $\mathcal{P}$ is the class of languages (i.e., decision problems) that can be solved by **deterministic polynomial-time algorithms**.

- class $\mathcal{P}$ contains problems like Reachability and many others.

**Definition**: $\mathcal{NP}$ is the class of languages (i.e., decision problems) that can be solved by **nondeterministic polynomial-time algorithms**.

- class $\mathcal{NP}$ contains problems like VC, HC, IS and many others.

Because every deterministic algorithm is a special case of a nondeterministic algorithm,

$$\mathcal{P} \subseteq \mathcal{NP}$$
Chapter 34. NP-Completeness

**Definition:** $\mathcal{P}$ is the class of languages (i.e., decision problems) that can be solved by deterministic polynomial-time algorithms.

- class $\mathcal{P}$ contains problems like **Reachability** and many others.

**Definition:** $\mathcal{NP}$ is the class of languages (i.e., decision problems) that can be solved by nondeterministic polynomial-time algorithms.

- class $\mathcal{NP}$ contains problems like **VC**, **HC**, **IS** and many others.

Because every deterministic algorithm is a special case of a nondeterministic algorithm,

$$\mathcal{P} \subseteq \mathcal{NP}$$
We consider the tree model of nondeterministic algorithms.

We may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps). Each nondeterministic path can be represented with a binary string: 0 for branching left, 1 for right. We can assume the algorithm does all nondeterministic choices before other operations. So we can model the computation as

1. First choose a binary string nondeterministically,
2. Follow the specified path deterministically

The binary string is called the certificate or witness; the deterministic computation part is called verification. Deterministic algorithms are when the certificate is empty.
Chapter 34. NP-Completeness

We consider the tree model of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices
Chapter 34. NP-Completeness

We consider the **tree model** of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices
  (5 choices can be simulated with 4 nondeterministic steps)
We consider the tree model of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps)
- each nondeterministic path can be represented with a binary string:
Chapter 34. NP-Completeness

We consider the tree model of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices
  (5 choices can be simulated with 4 nondeterministic steps)
- each nondeterministic path can be represented with a binary string:
  0 for branching left, 1 for right.
We consider the **tree model** of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps)

- each nondeterministic path can be represented with a binary string: 0 for branching left, 1 for right.

- we can assume the algorithm does **all** nondeterministic choices **before** other operations.

So we can model the computation as:

1. first choose a binary string nondeterministically, and
2. follow the specified path deterministically

The binary string is called **certificate** or **witness**; the deterministic computation part is called **verification**.
We consider the tree model of nondeterministic algorithms.

• we may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps)

• each nondeterministic path can be represented with a binary string: 0 for branching left, 1 for right.

• we can assume the algorithm does all nondeterministic choices before other operations. So we can model the computation as
We consider the **tree model** of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices
  (5 choices can be simulated with 4 nondeterministic steps)

- each nondeterministic path can be represented with a binary string:
  0 for branching left, 1 for right.

- we can assume the algorithm does **all** nondeterministic choices **before**
  other operations. So we can model the computation as
Chapter 34. NP-Completeness

We consider the tree model of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps)
- each nondeterministic path can be represented with a binary string: 0 for branching left, 1 for right.
- we can assume the algorithm does all nondeterministic choices before other operations. So we can model the computation as
  
  (1) first choose a binary string nondeterministically, and
We consider the **tree model** of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices
  (5 choices can be simulated with 4 nondeterministic steps)
- each nondeterministic path can be represented with a binary string:
  0 for branching left, 1 for right.
- we can assume the algorithm does all nondeterministic choices **before**
  other operations. So we can model the computation as
  
  (1) first choose a binary string nondeterministically, and
  (2) follow the specified path deterministically
We consider the **tree model** of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps)
- each nondeterministic path can be represented with a binary string: 0 for branching left, 1 for right.
- we can assume the algorithm does **all** nondeterministic choices **before** other operations. So we can model the computation as
  
  (1) first choose a binary string nondeterministically, and
  (2) follow the specified path deterministically

The binary string is called **certificate** or **witness**; The deterministic computation part is called **verification**.
Chapter 34. NP-Completeness

We consider the **tree model** of nondeterministic algorithms.

- we may assume each step has exactly 2 nondeterministic choices (5 choices can be simulated with 4 nondeterministic steps)
- each nondeterministic path can be represented with a binary string: 0 for branching left, 1 for right.
- we can assume the algorithm does **all** nondeterministic choices **before** other operations. So we can model the computation as

  (1) first choose a binary string nondeterministically, and 
  (2) follow the specified path deterministically

The binary string is called **certificate** or **witness**;
The deterministic computation part is called **verification**.

**Deterministic algorithms are when the certificate is empty.**
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

\[
\text{\#P} \text{ is defined with certificate } y = \epsilon, \text{ i.e., empty string.}
\]
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

• to nondeterministically choose a binary string of a polynomial length,
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is
- to nondeterministically choose a binary string of a polynomial length,
- then to compute deterministically in polynomial time.

Let $\Pi \in \text{NP}$. Then there is a deterministic algorithm $A_{\Pi}$, and a constant $c > 0$, such that
(1) if $x$ is a positive instance of $\Pi$, there is a binary string $y$ of length $n^c$, $A_{\Pi}(x,y) = \text{"YES"}$;
(2) if $x$ is a negative instance of $\Pi$, for all binary string $y$ of length $n^c$, $A_{\Pi}(x,y) = \text{"NO"}$;
and $A_{\Pi}$ runs in time $O(n^c)$.

We call $y$ a certificate/witness and $A_{\Pi}$ the verification algorithm.

$P$ is defined with certificate $y = \epsilon$, i.e., empty string.
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

- to nondeterministically choose a binary string of a polynomial length,
- then to compute deterministically in polynomial time.

Let $\Pi \in \mathcal{NP}$. Then there is a deterministic algorithm $A_{\Pi}$, and a constant $c > 0$, such that
Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

- to nondeterministically choose a binary string of a polynomial length,
- then to compute deterministically in polynomial time.

Let $\Pi \in \mathcal{NP}$. Then there is a deterministic algorithm $A_\Pi$, and a constant $c > 0$, such that

1. if $x$ is a positive instance of $\Pi$, there is a binary string $y$ of length $n^c$, $A_\Pi(x, y) = \text{“YES”};$

$P$ is defined with certificate $y = \epsilon$, i.e., empty string.
Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

- to nondeterministically choose a binary string of a polynomial length,
- then to compute deterministically in polynomial time.

Let \( \Pi \in \mathcal{NP} \). Then there is a deterministic algorithm \( A_\Pi \), and a constant \( c > 0 \), such that

1. if \( x \) is a positive instance of \( \Pi \), there is a binary string \( y \) of length \( n^c \),
   \( A_\Pi(x, y) = \text{"YES"} \);
2. if \( x \) is a negative instance of \( \Pi \), for all binary string \( y \) of length \( n^c \),
   \( A_\Pi(x, y) = \text{"NO"} \);
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

- to nondeterministically choose a binary string of a polynomial length,
- then to compute deterministically in polynomial time.

Let \( \Pi \in \mathcal{NP} \). Then there is a deterministic algorithm \( A_\Pi \), and a constant \( c > 0 \), such that

1. if \( x \) is a positive instance of \( \Pi \), there is a binary string \( y \) of length \( n^c \),
   \( A_\Pi(x, y) = \text{“YES”} \);
2. if \( x \) is a negative instance of \( \Pi \), for all binary string \( y \) of length \( n^c \),
   \( A_\Pi(x, y) = \text{“NO”} \);

and \( A_\Pi \) runs in time \( O(n^c) \).
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

• to nondeterministically choose a binary string of a polynomial length,
• then to compute deterministically in polynomial time.

Let $\Pi \in \mathcal{NP}$. Then there is a deterministic algorithm $A_\Pi$, and a constant $c > 0$, such that

(1) if $x$ is a positive instance of $\Pi$, there is a binary string $y$ of length $n^c$, $A_\Pi(x, y) = “YES”;$
(2) if $x$ is a negative instance of $\Pi$, for all binary string $y$ of length $n^c$, $A_\Pi(x, y) = “NO”;
and $A_\Pi$ runs in time $O(n^c)$.

We call $y$ a certificate/witness and $A_\Pi$ the verification algorithm.
Chapter 34. NP-Completeness

Alternative view of nondeterministic polynomial-time computation

Every nondeterministic polynomial time computation is

- to nondeterministically choose a binary string of a polynomial length,
- then to compute deterministically in polynomial time.

Let $\Pi \in \mathcal{NP}$. Then there is a deterministic algorithm $A_{\Pi}$, and a constant $c > 0$, such that

1. if $x$ is a positive instance of $\Pi$, there is a binary string $y$ of length $n^c$, $A_{\Pi}(x, y) = \text{"YES"}$;
2. if $x$ is a negative instance of $\Pi$, for all binary string $y$ of length $n^c$, $A_{\Pi}(x, y) = \text{"NO"}$;

and $A_{\Pi}$ runs in time $O(n^c)$.

We call $y$ a certificate/witness and $A_{\Pi}$ the verification algorithm.

$\mathcal{P}$ is defined with certificate $y = \epsilon$, i.e., empty string.
Definition of $NP$ in terms of languages:

Let $L \subseteq \{0,1\}^*$ be a language in the class $NP$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0,1\}^*$, $x \in L \iff \exists y, |y| \leq |x|^c$, $A_L(x,y) = 1$ and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what?
in $m = |x,y| = |x| + |y| \leq n + n^c$.

So if $A_L$ runs in polynomial time $m^d \leq (n + n^c)^d \leq (2n^c)^d = O(n^{dc})$, also polynomial time of $n = |x|$.
Chapter 34. NP-Completeness

Definition of $NP$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $NP$. 

A language $L$ is in the class $NP$ if there exists a deterministic algorithm $A_L$ and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$, $x \in L \iff \exists y, |y| \leq |x|^c$, $A_L(x,y) = 1$ and $A_L$ runs in polynomial time.
Chapter 34. NP-Completeness

Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$,
Chapter 34. NP-Completeness

Definition of \( \mathcal{NP} \) in terms of languages:

Let \( L \subseteq \{0, 1\}^* \) be a language in the class \( \mathcal{NP} \). Then there is a deterministic algorithm \( A_L \), and a constant \( c > 0 \), such that, for every \( x \in \{0, 1\}^* \),
Definition of $NP$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $NP$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L$$
Chapter 34. NP-Completeness

Definition of \( \mathcal{NP} \) in terms of languages:

Let \( L \subseteq \{0, 1\}^* \) be a language in the class \( \mathcal{NP} \). Then there is a deterministic algorithm \( A_L \), and a constant \( c > 0 \), such that, for every \( x \in \{0, 1\}^* \),

\[
x \in L \iff \exists y,
\]

where \( A_L \) runs in polynomial time.
Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c,$$

$A_L$ runs in polynomial time of $m = |x,y| = |x| + |y| \leq n + n^c$. So if $A_L$ runs in polynomial time

$$m \leq (n + n^c) \leq (2n^c) = O(n^{cd}),$$

also polynomial time of $n = |x|$. 

Class $\mathcal{P}$ is defined with certificate $y = \epsilon$, i.e., empty string.
Chapter 34. NP-Completeness

Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a **deterministic** algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$
Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.
Definition of $\mathbf{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathbf{NP}$. Then there is a \textbf{deterministic} algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1
\]

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time
Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what?
Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a \textbf{deterministic} algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y|$
Chapter 34. NP-Completeness

Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y| = |x| + |y|$
Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y| = |x| + |y| \leq n + n^c$. 
Chapter 34. NP-Completeness

Definition of \( \mathcal{NP} \) in terms of languages:

Let \( L \subseteq \{0, 1\}^* \) be a language in the class \( \mathcal{NP} \). Then there is a deterministic algorithm \( A_L \), and a constant \( c > 0 \), such that, for every \( x \in \{0, 1\}^* \),

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1
\]

and \( A_L \) runs in polynomial time.

\( A_L \) runs in polynomial time of what? in \( m = |x, y| = |x| + |y| \leq n + n^c \).

So if \( A_L \) runs in polynomial time \( m^d \)
Chapter 34. NP-Completeness

Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y| = |x| + |y| \leq n + n^c$.

So if $A_L$ runs in polynomial time $m^d \leq (n + n^c)$
Definition of \( \mathcal{NP} \) in terms of languages:

Let \( L \subseteq \{0, 1\}^* \) be a language in the class \( \mathcal{NP} \). Then there is a
\textbf{deterministic} algorithm \( A_L \), and a constant \( c > 0 \), such that, for every
\( x \in \{0, 1\}^* \),

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1
\]
and \( A_L \) runs in polynomial time.

\( A_L \) runs in polynomial time of what? in \( m = |x, y| = |x| + |y| \leq n + n^c \).

So if \( A_L \) runs in polynomial time \( m^d \leq (n + n^c)^d \)
Chapter 34. NP-Completeness

Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y| = |x| + |y| \leq n + nc$. So if $A_L$ runs in polynomial time $m^d \leq (n + nc)^d \leq (2nc)^d$. 
Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y| = |x| + |y| \leq n + n^c$.

So if $A_L$ runs in polynomial time $m^d \leq (n + n^c)^d \leq (2n^c)^d = O(n^{dc})$,
Chapter 34. NP-Completeness

Definition of $\mathcal{NP}$ in terms of languages:

Let $L \subseteq \{0, 1\}^*$ be a language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

$A_L$ runs in polynomial time of what? in $m = |x, y| = |x| + |y| \leq n + n^c$.

So if $A_L$ runs in polynomial time $m^d \leq (n + n^c)^d \leq (2n^c)^d = O(n^{dc})$,
also polynomial time of $n = |x|$. 

Definition of \( \mathcal{NP} \) in terms of languages:

Let \( L \subseteq \{0, 1\}^\ast \) be a language in the class \( \mathcal{NP} \). Then there is a deterministic algorithm \( A_L \), and a constant \( c > 0 \), such that, for every \( x \in \{0, 1\}^\ast \),

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1
\]

and \( A_L \) runs in polynomial time.

\( A_L \) runs in polynomial time of what? in \( m = |x, y| = |x| + |y| \leq n + n^c \).

So if \( A_L \) runs in polynomial time \( m^d \leq (n + n^c)^d \leq (2n^c)^d = O(n^{dc}) \),
also polynomial time of \( n = |x| \).

Class \( \mathcal{P} \) is defined with certificate \( y = \epsilon \), i.e., empty string.
Chapter 34. NP-Completeness
Chapter 34. NP-Completeness

Proof that $HC \in \mathcal{NP}$.
Proof that $HC \in \mathcal{NP}$.

We need to show there is a deterministic algorithm $A$ and a constant $c > 0$, such that for any $G$,

$$G \in HC \iff \exists y, |y| \leq |G|^c, A(G, y) = \text{“YES”}$$

We can design that

- certificate $y$ represents a sequence of ordered vertices;
Proof that $\text{HC} \in \mathcal{NP}$.

We need to show there is a deterministic algorithm $A$ and a constant $c > 0$, such that for any $G$,

$$G \in \text{HC} \iff \exists y, |y| \leq |G|^c, A(G, y) = \text{“YES”}$$

We can design that

- certificate $y$ represents a sequence of ordered vertices;

- algorithm $A$ is to verify that $y$ does form a $H$-cycle.
Proof that $HC \in \mathcal{NP}$.

We need to show there is a deterministic algorithm $A$ and a constant $c > 0$, such that for any $G$,

$$G \in HC \iff \exists y, |y| \leq |G|^c, A(G, y) = \text{"YES"}$$

We can design that

- certificate $y$ represents a sequence of ordered vertices;
- algorithm $A$ is to verify that $y$ does form a H-cycle.

Details:

- $y = B_1 B_2 \ldots B_n$, where $B_i$ is a binary representation of some vertex in $G$;
Proof that \( HC \in \mathcal{NP} \).

We need to show there is a deterministic algorithm \( A \) and a constant \( c > 0 \), such that for any \( G \),

\[
G \in HC \iff \exists y, |y| \leq |G|^c, A(G, y) = \text{"YES"}
\]

We can design that

- certificate \( y \) represents a sequence of ordered vertices;
- algorithm \( A \) is to verify that \( y \) does form a \( H \)-cycle.

Details:

- \( y = B_1 B_2 \ldots B_n \), where \( B_i \) is a binary representation of some vertex in \( G \); How many bits does \( B_i \) need?
Proof that $HC \in NP$.

We need to show there is a deterministic algorithm $A$ and a constant $c > 0$, such that for any $G$,

$$G \in HC \iff \exists y, |y| \leq |G|^c, A(G, y) = "YES"$$

We can design that

- certificate $y$ represents a sequence of ordered vertices;
- algorithm $A$ is to verify that $y$ does form a H-cycle.

Details:

- $y = B_1B_2 \ldots B_n$, where $B_i$ is a binary representation of some vertex in $G$; How many bits does $B_i$ need? $\lceil \log_2 n \rceil$
Chapter 34. NP-Completeness

Proof that $HC \in \mathcal{NP}$.

We need to show there is a deterministic algorithm $A$ and a constant $c > 0$, such that for any $G$,

$$G \in HC \iff \exists y, |y| \leq |G|^c, A(G, y) = \text{"YES"}$$

We can design that

- certificate $y$ represents a sequence of ordered vertices;
- algorithm $A$ is to verify that $y$ does form a H-cycle.

Details:

- $y = B_1 B_2 \ldots B_n$, where $B_i$ is a binary representation of some vertex in $G$; How many bits does $B_i$ need? $\lceil \log_2 n \rceil$
- whether $y$ forms a H-cycle can be verified in time
Proof that $HC \in \mathcal{NP}$.

We need to show there is a deterministic algorithm $A$ and a constant $c > 0$, such that for any $G$,

$$G \in HC \iff \exists y, |y| \leq |G|^c, A(G, y) = "YES"$$

We can design that

- certificate $y$ represents a sequence of ordered vertices;
- algorithm $A$ is to verify that $y$ does form a H-cycle.

Details:

- $y = B_1B_2\ldots B_n$, where $B_i$ is a binary representation of some vertex in $G$; How many bits does $B_i$ need? $[\log_2 n]$.
- whether $y$ forms a H-cycle can be verified in time $O(|E|)$
Chapter 34. NP-Completeness

exercises:

Proof that $\text{Independent Set} \in \text{NP}$.

Proof that $\text{Vertex Cover} \in \text{NP}$.

Notes
1. To prove a language is in the class $\text{NP}$ by no mean to prove that the language can be solved in polynomial time. Instead, it only shows the language is in the class $\text{NP}$.

2. There is a difference between deciding $x \in L$ and checking $A_L(x,y) = 1$.

3. As between convicting a suspect vs checking an evidence against the suspect.
Chapter 34. NP-Completeness

exercises:

Proof that $\text{Independent Set} \in \mathcal{NP}$.

Proof that $\text{Vertex Cover} \in \mathcal{NP}$.

Notes
Chapter 34. NP-Completeness

exercises:

Proof that \textsc{Independent Set} \in \mathcal{NP} .

Proof that \textsc{Vertex Cover} \in \mathcal{NP} .

Notes

1. to prove a language is in the class \mathcal{NP} by no mean to prove that the language can be solved in polynomial time. Instead, it only shows the language is in the class \mathcal{NP} .
exercises:

Proof that Independent Set $\in \mathcal{NP}$.

Proof that Vertex Cover $\in \mathcal{NP}$.

Notes

1. to prove a language is in the class $\mathcal{NP}$ by no mean to prove that the language can be solved in polynomial time. Instead, it only shows the language is in the class $\mathcal{NP}$.

2. there is a difference between deciding $x \in L$ and checking $A_L(x, y) = 1$. 
exercises:

Proof that \textbf{Independent Set} \in \mathcal{NP}.

Proof that \textbf{Vertex Cover} \in \mathcal{NP}.

Notes

1. to prove a language is in the class \mathcal{NP} by no mean to prove that the language can be solved in polynomial time. Instead, it only shows the language is in the class \mathcal{NP}.

2. there is a difference between deciding \textit{x ⇔ L} and checking \textit{A_L(x, y) = 1}.

3. as between \underline{convicting a suspect} vs \underline{checking an evidence against the suspect}.
3. NP-Completeness Framework
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
- A language contains positive instances of the corresponding decision problem.
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
- A language contains **positive instances** of the corresponding decision problem.
- Define

\[
\overline{L} = \{x : x \notin L\}
\]
Chapter 34. NP-Completeness

3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
- A language contains positive instances of the corresponding decision problem.
- Define

\[ \overline{L} = \{ x : x \notin L \} \]

called complement of \( L \)
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
- A language contains positive instances of the corresponding decision problem.
- Define $L = \{x : x \notin L\}$ called complement of $L$

$$L \cup \overline{L} = \{0, 1\}^*$$
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
- A language contains positive instances of the corresponding decision problem.
- Define

\[ \overline{L} = \{ x : x \notin L \} \] called complement of \( L \)

\[ L \cup \overline{L} = \{0, 1\}^* = \mathcal{U}, \]
3. NP-Completeness Framework

The notion of reduction (i.e., transformation) between languages

- We use languages for decision problems.
- A language contains positive instances of the corresponding decision problem.

- Define

  \[ \overline{L} = \{ x : x \not\in L \} \] called complement of \( L \)

  \[ L \cup \overline{L} = \{0, 1\}^* = \mathcal{U}, \text{ called universe} \]
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$. 
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$,
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that
Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$

That is,

$$x \in L_1 \implies f(x) \in L_2;$$
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet $\{0, 1\}$.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$

That is,

$$x \in L_1 \implies f(x) \in L_2; \quad x \in \overline{L_1} \implies f(x) \in \overline{L_2};$$
Chapter 34. NP-Completeness

Let $L_1$ and $L_2$ are two languages over the alphabet \{0, 1\}.

A reduction from $L_1$ to $L_2$, denoted as $L_1 \leq L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$

That is,

$$x \in L_1 \implies f(x) \in L_2; \quad x \in \overline{L_1} \implies f(x) \in \overline{L_2};$$
Chapter 34. NP-Completeness

Two example problems:
Two example problems:

**Independent Set (IS)**

**Input**: graph $G = (V, E)$, integer $k$;

**Output**: "YES" if and only if $G$ has an independent set of size $\geq k$.
Chapter 34. NP-Completeness

Two example problems:

**INDEPENDENT SET (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$. 
Chapter 34. NP-Completeness

Two example problems:

**INDEPENDENT SET (IS)**

**INPUT**: graph $G = (V, E)$, integer $k$;

**OUTPUT**: “YES” if and only if $G$ has an independent set of size $\geq k$.

and
Two example problems:

**INDEPENDENT SET (IS)**
- **INPUT:** graph $G = (V, E)$, integer $k$;
- **OUTPUT:** “YES” if and only if $G$ has an independent set of size $\geq k$.

and

**VERTEX COVER (VC)**
- **INPUT:** graph $G = (V, E)$, integer $k$;
Two example problems:

**Independent Set (IS)**
- **Input**: graph $G = (V, E)$, integer $k$;
- **Output**: “YES” if and only if $G$ has an independent set of size $\geq k$.

and

**Vertex Cover (VC)**
- **Input**: graph $G = (V, E)$, integer $k$;
- **Output**: “YES” if and only if $G$ has a vertex cover of size $\leq k$. 

Consider their corresponding languages:

$L_{IS} = \{\langle G, k \rangle : G \text{ has an independent set of size } \geq k \}$

$L_{VC} = \{\langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \}$
Two example problems:

**INDEPENDENT SET (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$.

and

**VERTEX COVER (VC)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has a vertex cover of size $\leq k$.

Consider their corresponding languages:
Chapter 34. NP-Completeness

Two example problems:

**Independent Set (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$.

and

**Vertex Cover (VC)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has a vertex cover of size $\leq k$.

Consider their corresponding languages:

$$L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \}$$
Chapter 34. NP-Completeness

Two example problems:

**INDEPENDENT SET (IS)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has an independent set of size $\geq k$.

and

**VERTEX COVER (VC)**
- **Input:** graph $G = (V, E)$, integer $k$;
- **Output:** “YES” if and only if $G$ has a vertex cover of size $\leq k$.

Consider their corresponding languages:

$$L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \}$$

$$L_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \}$$
Two example problems:

**INDEPENDENT SET (IS)**
- **Input:** graph \( G = (V, E) \), integer \( k \);
- **Output:** “YES” if and only if \( G \) has an independent set of size \( \geq k \).

and

**VERTEX COVER (VC)**
- **Input:** graph \( G = (V, E) \), integer \( k \);
- **Output:** “YES” if and only if \( G \) has a vertex cover of size \( \leq k \).

Consider their corresponding languages:

\[ L_{IS} = \{ <G, k> : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{ <G, k> : G \text{ has a vertex cover of size } \leq k \} \]
Chapter 34. NP-Completeness

\[ L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]
Chapter 34. NP-Completeness

$L_{IS} = \{\langle G, k \rangle : G \text{ has an independent set of size } \geq k \}$

$L_{VC} = \{\langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \}$
Chapter 34. NP-Completeness

\[ L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

Theorem:

\[ L_{IS} \leq L_{VC} \]

Proof:

We use the fact that complement set of an independent set is a vertex cover in the same graph.

We construct a mapping \( f \) that maps instance \( \langle G, k \rangle \) to instance \( \langle G, |G| - k \rangle \), i.e.,

\[ f(\langle G, k \rangle) = \langle G, |G| - k \rangle \]

This is a reduction from \( L_{IS} \) to \( L_{VC} \) because \( G \) has an i.s. of size \( \geq k \) if and only if \( G \) has an v.c. of size \( \leq |G| - k \).
Chapter 34. NP-Completeness

\[ L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

**Theorem:** \( L_{IS} \leq L_{VC} \)
Chapter 34. NP-Completeness

\[ \mathcal{L}_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ \mathcal{L}_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

**Theorem:** \( L_{IS} \leq L_{VC} \)

**Proof:**
Chapter 34. NP-Completeness

\[ L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

**Theorem**: \( L_{IS} \leq L_{VC} \)

**Proof**: we use the fact that complement set of an independent set is a vertex cover in the same graph
Chapter 34. NP-Completeness

\[ L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

**Theorem:** \( L_{IS} \leq L_{VC} \)

**Proof:** we use the fact that complement set of an independent set is a vertex cover in the same graph

We construct a mapping \( f \) that maps instance \( \langle G, k \rangle \) to instance \( \langle G, |G| - k \rangle \),
Chapter 34. NP-Completeness

\[ L_{IS} = \{ \langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{ \langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

**Theorem:** \( L_{IS} \leq L_{VC} \)

**Proof:** we use the fact that complement set of an independent set is a vertex cover in the same graph

We construct a mapping \( f \) that maps instance \( \langle G, k \rangle \) to instance \( \langle G, |G| - k \rangle \), i.e.,

\[ f(\langle G, k \rangle) \]
Chapter 34. NP-Completeness

$L_{IS} = \{\langle G, k \rangle : G \text{ has an independent set of size } \geq k \}$

$L_{VC} = \{\langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \}$

Because the two problems are very relevant to each other, we have:

**Theorem:** $L_{IS} \leq L_{VC}$

**Proof:** we use the fact that complement set of an independent set is a vertex cover in the same graph

We construct a mapping $f$ that maps instance $\langle G, k \rangle$ to instance $\langle G, |G| - k \rangle$, i.e.,

$$f(\langle G, k \rangle) = \langle G, |G| - k \rangle$$

This is a reduction from $L_{IS}$ to $L_{VC}$ because

$G$ has an i.s. of size $\geq k \iff G$ has an v.c. of size $\leq |G|-k$
Chapter 34. NP-Completeness

\[ L_{IS} = \{\langle G, k \rangle : G \text{ has an independent set of size } \geq k \} \]

\[ L_{VC} = \{\langle G, k \rangle : G \text{ has a vertex cover of size } \leq k \} \]

Because the two problems are very relevant to each other, we have:

**Theorem:** \( L_{IS} \leq L_{VC} \)

**Proof:** we use the fact that complement set of an independent set is a vertex cover in the same graph

We construct a mapping \( f \) that maps instance \( \langle G, k \rangle \) to instance \( \langle G, |G| - k \rangle \), i.e.,

\[ f(\langle G, k \rangle) = \langle G, |G| - k \rangle \]

This is a reduction from \( L_{IS} \) to \( L_{VC} \) because

\[ G \text{ has an i.s. of size } \geq k \iff G \text{ has an v.c. of size } \leq |G| - k \]

So \( L_{IS} \leq L_{VC} \).
Chapter 34. NP-Completeness

An important motivation for reduction:
Chapter 34. NP-Completeness

An important motivation for reduction:

- a reduction transforms instances of the first problem to the instances of the second problem;
Chapter 34. NP-Completeness

An important motivation for reduction:

• a reduction transforms instances of the first problem to the instances of the second problem;

• algorithms solving the second problem can be used to solve the first;

where algorithm $F$ computes the reduction $f$, 

An important motivation for reduction:

- a reduction transforms instances of the first problem to the instances of the second problem;
- algorithms solving the second problem can be used to solve the first;

where algorithm $F$ computes the reduction $f$, and algorithm $A_2$ solves for $L_2$. 

![Diagram showing the reduction process](image)
Chapter 34. NP-Completeness

An important motivation for reduction:

- a reduction transforms instances of the first problem to the instances of the second problem;
- algorithms solving the second problem can be used to solve the first;

where algorithm $F$ computes the reduction $f$, and algorithm $A_2$ solves for $L_2$

So the combined algorithm (gray-color box) solves for $L_1$. 
Formally,
Chapter 34. NP-Completeness

Formally,

A polynomial-time reduction from $L_1$ to $L_2$, denoted as $L_1 \leq_p L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$,
Chapter 34. NP-Completeness

Formally,

A polynomial-time reduction from $L_1$ to $L_2$, denoted as $L_1 \leq_p L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that
Chapter 34. NP-Completeness

Formally,

A polynomial-time reduction from $L_1$ to $L_2$, denoted as $L_1 \leq_p L_2$, is some mapping function $f : \{0, 1\}^* \to \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,
Formally,

A polynomial-time reduction from $L_1$ to $L_2$, denoted as $L_1 \leq_p L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$
Chapter 34. NP-Completeness

Formally,

A polynomial-time reduction from \( L_1 \) to \( L_2 \), denoted as \( L_1 \leq_p L_2 \), is some mapping function \( f : \{0, 1\}^* \rightarrow \{0, 1\}^* \), such that for any \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2
\]

where \( f \) can be computed in time \( O(|x|^c) \) for some fixed \( c > 0 \).
Chapter 34. NP-Completeness

Formally,

A polynomial-time reduction from $L_1$ to $L_2$, denoted as $L_1 \leq_p L_2$, is some mapping function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, such that for any $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2$$

where $f$ can be computed in time $O(|x|^c)$ for some fixed $c > 0$.

For example, $L_{IS} \leq_p L_V$. 
Chapter 34. NP-Completeness

Theorem: Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$. 
Chapter 34. NP-Completeness

**Theorem:** Let \( L_1 \leq_p L_2 \). If \( L_2 \in \mathcal{P} \), then \( L_1 \in \mathcal{P} \).

**Proof:** Assume algorithm \( F \) computes \( f \), and algorithm \( A_2 \) solves for \( L_2 \).
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$

We need to show that the gray box runs in polynomial time
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$. We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

Total time is the sum of time for $F$ and time for $A_2$. 
**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

![Diagram showing the boxes for algorithms $F$, $A_2$, and $A_1$.](image)

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

![Diagram](image)

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$

**now, what is the length of $f(x)$?**
Theorem: Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

Proof: Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$ now, what is the length of $f(x)$?

Because $F$ runs in time $O(|x|^c)$,
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$

now, what is the length of $f(x)$?

Because $F$ runs in time $O(|x|^c)$, the number of bits outputted by $F$ is $O(|x|^c)$.
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$

Now, what is the length of $f(x)$?

Because $F$ runs in time $O(|x|^c)$, the number of bits outputted by $F$ is $O(|x|^c)$. So

$$O(|x|^c) + O(|f(x)|^d)$$
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$

**now, what is the length of $f(x)$?**

Because $F$ runs in time $O(|x|^c)$, the number of bits outputted by $F$ is $O(|x|^c)$.

So

$$O(|x|^c) + O(|f(x)|^d) = O(|x|^c + O((|x|^c)^d))$$
Chapter 34. NP-Completeness

**Theorem:** Let $L_1 \leq_p L_2$. If $L_2 \in \mathcal{P}$, then $L_1 \in \mathcal{P}$.

**Proof:** Assume algorithm $F$ computes $f$, and algorithm $A_2$ solves for $L_2$.

We need to show that the gray box runs in polynomial time if both $F$ and $A_2$ runs in polynomial time:

![Diagram](image)

Total time is the sum of time for $F$ and time for $A_2$.

$$O(|x|^c) + O(|f(x)|^d)$$

now, what is the length of $f(x)$?

Because $F$ runs in time $O(|x|^c)$, the number of bits outputted by $F$ is $O(|x|^c)$.

So

$$O(|x|^c) + O(|f(x)|^d) = O(|x|^c + O((|x|^c)^d)) = O(|x|^{cd})$$
Theorem: Polynomial-time reductions compose (are transitive). That is, if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

Proof. Assume functions \( f \) for \( L_1 \leq_p L_2 \) and function \( h \) for \( L_2 \leq_p L_3 \). For every \( x \in \{0, 1\}^* \), \( x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3 \). That is, \( x \in L_1 \iff h(f(x)) \in L_3 \). So the composite function \( h \circ f \) realizes the reduction \( L_1 \leq_p L_3 \).

But we need to show the reduction is \( \leq_p \), i.e., a polynomial-time reduction. Assume that algorithm \( F \) computes \( f \): \( F(x) = f(x) \) in time \( O(|x|^c) \) and algorithm \( H \) computes \( h \): \( H(y) = h(y) \) in time \( O(|y|^d) \). Let \( y = f(x) \), the total time for computing \( h \circ f \) is the time of \( F \) and the time of \( H \): \( O(|x|^c) + O(|f(x)|^d) = O(|x|^c) + O(|x|^cd) \). So \( L_1 \leq_p L_3 \).
Chapter 34. NP-Completeness

**Theorem**: Polynomial-time reductions compose (are transitive). That is, if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

Proof. Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

For every \( x \in \{0, 1\}^* \),
\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3.
\]
That is, \( x \in L_1 \iff h(f(x)) \in L_3 \). So composite function \( (h \circ f) \) realizes reduction \( L_1 \leq_p L_3 \).

But we need to show the reduction is \( \leq_p \), i.e., a polynomial time reduction.

Assume that algorithm \( F \) computes \( f \) in time \( O(|x|^c) \) and algorithm \( H \) computes \( h \) in time \( O(|y|^d) \).

Let \( y = f(x) \), the total time for computing \( (h \circ f) \) is
\[
O(|x|^c) + O(|f(x)|^d) = O(|x|^c + |x|^cd) = O(|x|^c(1 + d)).
\]

So \( L_1 \leq_p L_3 \).
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is, if $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \);

Assume that algorithm \( F \) computes \( f \): \( F(x) = f(x) \) in time \( O(|x|^c) \) and algorithm \( H \) computes \( h \): \( H(y) = h(y) \) in time \( O(|y|^d) \). Let \( y = f(x) \), the total time for computing \((h \circ f)\) = time of \( F \) and time of \( H \) = \( O(|x|^c) + O(|f(x)|^d) \) = \( O(|x|^c) + O(|x|^{cd}) \) so \( L_1 \leq_p L_3 \).
Chapter 34. NP-Completeness

**Theorem**: Polynomial-time reductions compose (are transitive). That is
If \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof**. Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is if $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.

**Proof.** Assume functions $f$ for $L_1 \leq_p L_2$; function $h$ for $L_2 \leq_p L_3$.

for every $x \in \{0, 1\}^*$,

$$x \in L_1$$
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is, if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2
\]
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is

If \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is \( x \in L_1 \)
Chapter 34. NP-Completeness

**Theorem**: Polynomial-time reductions compose (are transitive). That is if $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.

**Proof.** Assume functions $f$ for $L_1 \leq_p L_2$; function $h$ for $L_2 \leq_p L_3$.

for every $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3$$

That is $x \in L_1 \iff h(f(x)) \in L_3$
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is
if $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.

**Proof.** Assume functions $f$ for $L_1 \leq_p L_2$; function $h$ for $L_2 \leq_p L_3$.

for every $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3$$

That is $x \in L_1 \iff h(f(x)) \in L_3$

So composite function $(h \circ f)$ realizes reduction $L_1 \leq L_3$. 
Theorem: Polynomial-time reductions compose (are transitive). That is

If \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

Proof. Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is \( x \in L_1 \iff h(f(x)) \in L_3 \)

So composite function \( (h \circ f) \) realizes reduction \( L_1 \leq L_3 \).

But we need to show the reduction is \( \leq_p \), i.e., a polynomial time reduction.
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is \( x \in L_1 \iff h(f(x)) \in L_3 \)

So composite function \( (h \circ f) \) realizes reduction \( L_1 \leq L_3 \).

But we need to show the reduction is \( \leq_p \), i.e., a polynomial time reduction.

Assume that algorithm \( F \) computes \( f \): \( F(x) = f(x) \) in time \( O(|x|^c) \)
Chapter 34. NP-Completeness

Theorem: Polynomial-time reductions compose (are transitive). That is

If $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.

Proof. Assume functions $f$ for $L_1 \leq_p L_2$; function $h$ for $L_2 \leq_p L_3$.

for every $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3$$

That is $x \in L_1 \iff h(f(x)) \in L_3$

So composite function $(h \circ f)$ realizes reduction $L_1 \leq L_3$.

But we need to show the reduction is $\leq_p$, i.e., a polynomial time reduction.

Assume that algorithm $F$ computes $f$: $F(x) = f(x)$ in time $O(|x|^c)$
and algorithm $H$ computes $h$: $H(y) = h(y)$ in time $O(|y|^d)$
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is

If \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
    x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is \( x \in L_1 \iff h(f(x)) \in L_3 \)

So composite function \((h \circ f)\) realizes reduction \( L_1 \leq L_3 \).

But we need to show the reduction is \( \leq_p \), i.e., a polynomial time reduction.

Assume that algorithm \( F \) computes \( f \): \( F(x) = f(x) \) in time \( O(|x|^c) \)
and algorithm \( H \) computes \( h \): \( H(y) = h(y) \) in time \( O(|y|^d) \)

Let \( y = f(x) \), the total time for computing \((h \circ f) = \) time of \( F \) and time of \( H \)

\[
    = O(|x|^c) + O(|f(x)|^d)
\]
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is
If \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).
for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is \( x \in L_1 \iff h(f(x)) \in L_3 \)

So composite function \((h \circ f)\) realizes reduction \( L_1 \leq L_3 \). 
But we need to show the reduction is \( \leq_p \), i.e., a polynomial time reduction.

Assume that algorithm \( F \) computes \( f: F(x) = f(x) \) in time \( O(|x|^c) \)
and algorithm \( H \) computes \( h: H(y) = h(y) \) in time \( O(|y|^d) \)

Let \( y = f(x), \) the total time for computing \((h \circ f) = \) time of \( F \) and time of \( H \)

\[
= O(|x|^c) + O(|f(x)|^d) = O(|x|^c) + O((|x|^c)^d)
\]
Chapter 34. NP-Completeness

**Theorem:** Polynomial-time reductions compose (are transitive). That is if \( L_1 \leq_p L_2 \) and \( L_2 \leq_p L_3 \), then \( L_1 \leq_p L_3 \).

**Proof.** Assume functions \( f \) for \( L_1 \leq_p L_2 \); function \( h \) for \( L_2 \leq_p L_3 \).

for every \( x \in \{0, 1\}^* \),

\[
x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3
\]

That is \( x \in L_1 \iff h(f(x)) \in L_3 \)

So composite function \( (h \circ f) \) realizes reduction \( L_1 \leq L_3 \).

But we need to show the reduction is \( \leq_p \), i.e., a polynomial time reduction.

Assume that algorithm \( F \) computes \( f: F(x) = f(x) \) in time \( O(|x|^c) \)
and algorithm \( H \) computes \( h: H(y) = h(y) \) in time \( O(|y|^d) \)

Let \( y = f(x) \), the total time for computing \( (h \circ f) = \) time of \( F \) and time of \( H \)

\[
= O(|x|^c) + O(|f(x)|^d) = O(|x|^c) + O((|x|^c)^d) = O(|x|^c) + O(|x|^{cd})
\]
Theorem: Polynomial-time reductions compose (are transitive). That is if $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.

Proof. Assume functions $f$ for $L_1 \leq_p L_2$; function $h$ for $L_2 \leq_p L_3$.

for every $x \in \{0, 1\}^*$,

$$x \in L_1 \iff f(x) \in L_2 \iff h(f(x)) \in L_3$$

That is $x \in L_1 \iff h(f(x)) \in L_3$

So composite function $(h \circ f)$ realizes reduction $L_1 \leq L_3$.
But we need to show the reduction is $\leq_p$, i.e., a polynomial time reduction.

Assume that algorithm $F$ computes $f$: $F(x) = f(x)$ in time $O(|x|^c)$
and algorithm $H$ computes $h$: $H(y) = h(y)$ in time $O(|y|^d)$

Let $y = f(x)$, the total time for computing $(h \circ f)$ = time of $F$ and time of $H$

$$= O(|x|^c) + O(|f(x)|^d) = O(|x|^c) + O((|x|^c)^d) = O(|x|^c) + O(|x|^{cd})$$

So $L_1 \leq_p L_3$. 
Some conclusions:

• Using $\leq_p$, languages in $\text{NP}$ can be ordered partially;

• If those languages at the end of a $\leq_p$ chain have polynomial-time algorithms, so does every language on the chain.

• Informally, those at the end of a $\leq_p$ chain are called $\text{NP}$-hard.
Chapter 34. NP-Completeness

Some conclusions:

- Using $\leq_p$, languages in $\mathcal{NP}$ can be ordered partially;
Chapter 34. NP-Completeness

Some conclusions:

- Using $\leq_p$, languages in $NP$ can be ordered partially;
- If those languages at the end of a $\leq_p$ chain have polynomial-time algorithms, so does every language on the chain.
Some conclusions:

- Using $\leq_p$, languages in $NP$ can be ordered partially;
- If those languages at the end of a $\leq_p$ chain have polynomial-time algorithms, so does every language on the chain.
- Informally, those at the end of a $\leq_p$ chain are called $NP$-hard.
Chapter 34. NP-Completeness

Definition 1: $L$ is NP-hard

Definition 1: $L$ is NP-complete if (1) $L$ is NP-hard and (2) $L \in \text{NP}$.

Properties of NP-hard problems

• If $L$ is NP-hard and $L \in \text{P}$, then $\text{P} = \text{NP}$.

Proof?

• If $L$ is NP-hard and $L \leq_p L'$, then $L'$ is NP-hard.

Proof?
Chapter 34. NP-Completeness

**Definition 1:** $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

**Properties of NP-hard problems**

• If $L$ is NP-hard and $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.

**Proof?**

• If $L$ is NP-hard and $L \leq_p L'$, then $L'$ is NP-hard.

**Proof?**

How to prove a language is NP-hard?
Chapter 34. NP-Completeness

**Definition 1:** $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

**Definition 1:** $L$ is **NP-complete**
Chapter 34. NP-Completeness

Defn 1: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

Defn 1: $L$ is **NP-complete** if (1) $L$ is NP-hard

Chapter 34. NP-Completeness

**Definition 1:** $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

**Definition 1:** $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.
Chapter 34. NP-Completeness

**Definition 1:** $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

**Definition 1:** $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

Properties of NP-hard problems
Chapter 34. NP-Completeness

**Definition 1:** \( L \) is **NP-hard** if for every language \( L' \in \mathcal{NP} \), \( L' \leq_p L \).

**Definition 1:** \( L \) is **NP-complete** if (1) \( L \) is NP-hard and (2) \( L \in \mathcal{NP} \).

**Properties of NP-hard problems**

- If \( L \) is NP-hard
Chapter 34. NP-Completeness

Definition 1: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

Definition 1: $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

**Properties of NP-hard problems**

- If $L$ is NP-hard and $L \in \mathcal{P}$,
Chapter 34. NP-Completeness

**Definition 1:** \( L \) is **NP-hard** if for every language \( L' \in \mathcal{NP} \), \( L' \leq_p L \).

**Definition 1:** \( L \) is **NP-complete** if (1) \( L \) is NP-hard and (2) \( L \in \mathcal{NP} \).

**Properties of NP-hard problems**

- If \( L \) is NP-hard and \( L \in \mathcal{P} \), then \( \mathcal{P} = \mathcal{NP} \).
Chapter 34. NP-Completeness

**Definition 1**: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

**Definition 1**: $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

**Properties of NP-hard problems**

- If $L$ is NP-hard and $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.
  
  Proof?
Chapter 34. NP-Completeness

**Definition 1**: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq^p L$.

**Definition 1**: $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

**Properties of NP-hard problems**

- If $L$ is NP-hard and $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.
  
  Proof?

- If $L$ is NP-hard
Chapter 34. NP-Completeness

Definition 1: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

Definition 1: $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

Properties of NP-hard problems

- If $L$ is NP-hard and $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$. 
  Proof?

- If $L$ is NP-hard and $L \leq_p L'$,
Chapter 34. NP-Completeness

**Definition 1:** \( L \) is **NP-hard** if for every language \( L' \in \mathcal{NP} \), \( L' \leq_p L \).

**Definition 1:** \( L \) is **NP-complete** if (1) \( L \) is NP-hard and (2) \( L \in \mathcal{NP} \).

**Properties of NP-hard problems**

- If \( L \) is NP-hard and \( L \in \mathcal{P} \), then \( \mathcal{P} = \mathcal{NP} \).
  
  *Proof?*

- If \( L \) is NP-hard and \( L \leq_p L' \), then \( L' \) is NP-hard.
Chapter 34. NP-Completeness

Definition 1: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

Definition 1: $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

**Properties of NP-hard problems**

- If $L$ is NP-hard and $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.  
  Proof?

- If $L$ is NP-hard and $L \leq_p L'$, then $L'$ is NP-hard.  
  Proof?
Chapter 34. NP-Completeness

Definition 1: $L$ is **NP-hard** if for every language $L' \in \mathcal{NP}$, $L' \leq_p L$.

Definition 1: $L$ is **NP-complete** if (1) $L$ is NP-hard and (2) $L \in \mathcal{NP}$.

Properties of NP-hard problems

- If $L$ is NP-hard and $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.
  
  Proof?

- If $L$ is NP-hard and $L \leq_p L'$, then $L'$ is NP-hard.
  
  Proof?

How to prove a language is NP-hard?
Chapter 34. NP-Completeness

4. NP-Completeness Proofs
4. NP-Completeness Proofs

To prove a language $L$ is NP-complete,
Chapter 34. NP-Completeness

4. NP-Completeness Proofs

To prove a language $L$ is NP-complete, we need to show it is NP-hard.
4. NP-Completeness Proofs

To prove a language $L$ is **NP-complete**, we need to show it is **NP-hard**. That is, we need to show
4. NP-Completeness Proofs

To prove a language $L$ is NP-complete, we need to show it is NP-hard. That is, we need to show

$$\text{for every language } L' \in \mathcal{NP}, \quad L' \leq_p L$$
4. NP-Completeness Proofs

To prove a language $L$ is NP-complete, we need to show it is NP-hard. That is, we need to show

$$\text{for every language } L' \in \mathcal{NP}, \ L' \leq_p L$$

- Apparently, it is not possible to enumerate all languages in NP and prove that everyone is polynomial-time reducible to $L$. 
4. NP-Completeness Proofs

To prove a language $L$ is NP-complete, we need to show it is NP-hard. That is, we need to show

$$\text{for every language } L' \in \mathcal{NP}, \; L' \leq_p L$$

- Apparently, it is not possible to enumerate all languages in NP and prove that everyone is polynomial-time reducible to $L$.

- Instead, formulate a generic language that represents all languages in NP.
4. NP-Completeness Proofs

To prove a language $L$ is **NP-complete**, we need to show it is **NP-hard**. That is, we need to show

$$\text{for every language } L' \in \mathcal{NP}, L' \leq_p L$$

- Apparently, it is not possible to enumerate all languages in NP and prove that everyone is polynomial-time reducible to $L$.

- Instead, formulate a **generic language** that represents all languages in NP and prove that every language in $\mathcal{NP}$ can be reduced to the generic language in polynomial time.
4. NP-Completeness Proofs

To prove a language $L$ is NP-complete, we need to show it is NP-hard. That is, we need to show

$$\text{for every language } L' \in \mathcal{NP}, \quad L' \leq_p L$$

- Apparently, it is not possible to enumerate all languages in NP and prove that everyone is polynomial-time reducible to $L$.

- Instead, formulate a generic language that represents all languages in NP and prove that every language in $\mathcal{NP}$ can be reduced to the generic language in polynomial time.

- To obtain such a generic language, we need to consider the definition of languages in NP.
Chapter 34. NP-Completeness

Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$, $x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$ and $A_L$ runs in polynomial time.

The "iff" relationship looks a little like the relationship in a reduction $x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \iff f(x) \in L_{tbd}$ where $L_{tbd}$ is a language to be defined.

Can we identify $L_{tbd}$ and $f$?
Chapter 34. NP-Completeness

Recall the definition of languages in \( \mathcal{NP} \):

Let \( L \subseteq \{0, 1\}^* \) be any language in the class \( \mathcal{NP} \). Then there is a deterministic algorithm \( A_L \),

Can we identify \( L_{tbd} \) and \( f \)?
Chapter 34. NP-Completeness

Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L$$
Chapter 34. NP-Completeness

Recall the definition of languages in \( \mathcal{NP} \):

Let \( L \subseteq \{0,1\}^* \) be any language in the class \( \mathcal{NP} \). Then there is a **deterministic** algorithm \( A_L \), and a constant \( c > 0 \), such that, for every \( x \in \{0,1\}^* \),

\[
x \in L \iff \exists y, A_L(x,y) = 1
\]

and \( A_L \) runs in polynomial time.

The "iff" relationship looks a little like the relationship in a reduction:

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x,y) = 1
\]

\( \iff \)

\[
x \in L \iff f(x) \in L_{\text{tbd}}
\]

where \( L_{\text{tbd}} \) is a language to be defined.

Can we identify \( L_{\text{tbd}} \) and \( f \)?
Chapter 34. NP-Completeness

Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c,$$

Can we identify $L_{tbd}$ and $f$?
Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.
Chapter 34. NP-Completeness

Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

The “iff” relationship looks a little like the relationship in a reduction
Chapter 34. NP-Completeness

Recall the definition of languages in \( NP \):

Let \( L \subseteq \{0, 1\}^* \) be any language in the class \( NP \). Then there is a deterministic algorithm \( A_L \), and a constant \( c > 0 \), such that, for every \( x \in \{0, 1\}^* \),

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1
\]

and \( A_L \) runs in polynomial time.

The “iff” relationship looks a little like the relationship in a reduction

\[
x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1
\]
Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

The “iff” relationship looks a little like the relationship in a reduction

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$
Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0, 1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0, 1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

The “iff” relationship looks a little like the relationship in a reduction

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

$\uparrow$

$$x \in L \iff f(x) \in L_{tbd}$$
Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0,1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a **deterministic** algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0,1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

and $A_L$ runs in polynomial time.

The “iff” relationship looks a little like the relationship in a reduction

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1$$

$
\uparrow$

$$x \in L \iff f(x) \in L_{tbd}$$

where $L_{tbd}$ is a language to be defined.
Chapter 34. NP-Completeness

Recall the definition of languages in $\mathcal{NP}$:

Let $L \subseteq \{0,1\}^*$ be any language in the class $\mathcal{NP}$. Then there is a deterministic algorithm $A_L$, and a constant $c > 0$, such that, for every $x \in \{0,1\}^*$,

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x,y) = 1$$

and $A_L$ runs in polynomial time.

The “iff” relationship looks a little like the relationship in a reduction

$$x \in L \iff \exists y, |y| \leq |x|^c, A_L(x,y) = 1$$

\[ \Downarrow \]

$$x \in L \iff f(x) \in L_{tbd}$$

where $L_{tbd}$ is a language to be defined.

Can we identify $L_{tbd}$ and $f$?
Again we examine

\[ x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \] (1)

\[ A_L \text{ is a deterministic algorithm can be implemented with a boolean circuit} \]
\[ B_L \]
\[ x_1 x_2 \ldots x_n \text{ and } y_1 y_2 \ldots y_m \] such that
\[ A_L(x, y) = 1 \text{ if and only if } B_L(x, y) = 1 \] (2)

Because \( x \) is given, circuit \( B_L \) can be made into circuit \( C_x L \) such that
\[ B_L(x, y) = 1 \text{ if and only if } C_x L(y) = 1 \] (3)

From (1), (2), and (3), we have
\[ x \in L \iff \exists y \text{ s.t. } C_x L(y) = 1 \] (4)
Chapter 34. NP-Completeness

Again we examine

\[ x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \]  

(1)

- \( A_L \) is a deterministic algorithm can be implemented with a boolean circuit \( B_L \) with two sets of input gates \( x = x_1 x_2 \ldots x_n \) and \( y = y_1 y_2 \ldots y_m \) such that

\[ A_L(x, y) = 1 \text{ if and only if } B_L(x, y) = 1 \]  

(2)
Chapter 34. NP-Completeness

Again we examine

\[ x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \]  \hspace{1cm} (1)

- \( A_L \) is a deterministic algorithm can be implemented with a boolean circuit \( B_L \) with two sets of input gates \( x = x_1x_2 \ldots x_n \) and \( y = y_1y_2 \ldots y_m \) such that

\[ A_L(x, y) = 1 \text{ if and only if } B_L(x, y) = 1 \]  \hspace{1cm} (2)
Chapter 34. NP-Completeness

Again we examine

\[ x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \]  

(1)

- \( A_L \) is a deterministic algorithm can be implemented with a boolean circuit \( B_L \) with two sets of input gates \( x = x_1 x_2 \ldots x_n \) and \( y = y_1 y_2 \ldots y_m \) such that

\[ A_L(x, y) = 1 \text{ if and only if } B_L(x, y) = 1 \]  

(2)

\[ B_L \]

\[ C^x_L \]
Chapter 34. NP-Completeness

Again we examine

\[ x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \]  

1. \( A_L \) is a deterministic algorithm can be implemented with a boolean circuit \( B_L \) with two sets of input gates \( x = x_1 x_2 \ldots x_n \) and \( y = y_1 y_2 \ldots y_m \) such that

\[ A_L(x, y) = 1 \iff B_L(x, y) = 1 \]  

2. Because \( x \) is given, circuit \( B_L \) can be made into circuit \( C^x_L \) such that

\[ B_L(x, y) = 1 \iff C^x_L(y) = 1 \]
Again we examine

\[ x \in L \iff \exists y, |y| \leq |x|^c, A_L(x, y) = 1 \]  \hspace{1cm} (1)

- \( A_L \) is a deterministic algorithm can be implemented with a boolean circuit \( B_L \) with two sets of input gates \( x = x_1 x_2 \ldots x_n \) and \( y = y_1 y_2 \ldots y_m \) such that

\[ A_L(x, y) = 1 \text{ if and only if } B_L(x, y) = 1 \]  \hspace{1cm} (2)

- Because \( x \) is given, circuit \( B_L \) can be made into circuit \( C_L^x \) such that

\[ B_L(x, y) = 1 \text{ if and only if } C_L^x(y) = 1 \]  \hspace{1cm} (3)

- From (1), (2), and (3), we have

\[ x \in L \iff \exists y C_L^x(y) = 1 \]  \hspace{1cm} (4)
Chapter 34. NP-Completeness

Now we have

\[ x \in L \iff \exists y C_L^x(y) = 1 \quad (5) \]
Now we have

\[ x \in L \iff \exists y C^x_L(y) = 1 \]  

(5)

- Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).
Now we have

\[ x \in L \iff \exists y \exists L (y) = 1 \tag{5} \]

- Define: a boolean circuit \( C \) is \textbf{satisfiable} if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).

  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
Chapter 34. NP-Completeness

Now we have

\[ x \in L \iff \exists y C^x_L(y) = 1 \]  

(5)

- Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).

  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
  but \( D(x_1, x_2) = (x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2) \) is not!
Chapter 34. NP-Completeness

Now we have

\[ x \in L \iff \exists y \; C^x_L(y) = 1 \]  

(5)

- Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).
  
  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
  
  but \( D(x_1, x_2) = (x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2) \) is not!

- Define the following language:

\[
CSAT = \{ C : \text{circuit } C \text{ is satisfiable} \}
\]
Now we have
\[ x \in L \iff \exists y \ C^x_L(y) = 1 \] \hspace{1cm} (5)

- Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).

  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
  but \( D(x_1, x_2) = (x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2) \) is not!

- Define the following language:

  \[ \text{CSAT} = \{ C : \text{circuit } C \text{ is satisfiable} \} \]

- From (4), we have

  \[ x \in L \iff C^x_L \in \text{CSAT} \] \hspace{1cm} (6)
Now we have
\[ x \in L \iff \exists y \, C_L^x(y) = 1 \] (5)

- Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).

  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
  but \( D(x_1, x_2) = (x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2) \) is not!

- Define the following language:

  \[ CSAT = \{ C : \text{circuit } C \text{ is satisfiable} \} \]

- From (4), we have

  \[ x \in L \iff C_L^x \in CSAT \] (6)

It remains to be shown
Chapter 34. NP-Completeness

Now we have

\[ x \in L \iff \exists y \ C^x_L(y) = 1 \quad (5) \]

• Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).

  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
  but \( D(x_1, x_2) = (x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2) \) is not!

• Define the following language:

  \[ CSAT = \{ C : \text{circuit } C \text{ is satisfiable} \} \]

• From (4), we have

  \[ x \in L \iff C^x_L \in CSAT \quad (6) \]

It remains to be shown

• that reducing **algorithm** \( A_L \) to **circuit** \( B_L \) is valid;
Now we have
\[ x \in L \iff \exists y \quad C_L^x(y) = 1 \]  
(5)

• Define: a boolean circuit \( C \) is **satisfiable** if there exists at least one set of values \( y \) to its input gates such that \( C(y) = 1 \).

  e.g., \( C(x_1, x_2) = (\neg x_1 \lor \neg x_2) \land (x_1 \lor x_2) \) is satisfiable;
  but \( D(x_1, x_2) = (x_1 \lor x_2) \land (x_1 \lor \neg x_2) \land (\neg x_1 \lor x_2) \land (\neg x_1 \lor \neg x_2) \) is not!

• Define the following language:

\[ CSAT = \{ C : \text{ circuit } C \text{ is satisfiable } \} \]

• From (4), we have
\[ x \in L \iff C_L^x \in CSAT \]  
(6)

It remains to be shown

• that reducing algorithm \( A_L \) to circuit \( B_L \) is valid; and

• that the reduction can be done in **polynomial time**.
Chapter 34. NP-Completeness

Unfold deterministic polynomial-time algorithm $A(x, y)$ with input $\langle x, y \rangle$.
Chapter 34. NP-Completeness

Unfold deterministic polynomial-time algorithm $A(x, y)$ with input $\langle x, y \rangle$
Chapter 34. NP-Completeness

The algorithm is physically implemented with a boolean circuit
Chapter 34. NP-Completeness

The algorithm is physically implemented with a boolean circuit.
Chapter 34. NP-Completeness

The algorithm is physically implemented with a boolean circuit.

\[ M \]

\[ x \]
\[ x_1 \ x_2 \ x_3 \ \ldots \ x_n \]

\[ y \]
\[ y_1 \ y_2 \ y_3 \ \ldots \ y_m \]
Chapter 34. NP-Completeness

The algorithm is physically implemented with a boolean circuit

And the circuit can be built from the algorithm in polynomial time.
Chapter 34. NP-Completeness

The above discussion shows that $L_{CSAT}$ is NP-hard.
The above discussion shows that $L_{CSAT}$ is NP-hard.

**Theorem**: Language $CSAT$ is NP-complete.
Chapter 34. NP-Completeness

The above discussion shows that $L_{CSAT}$ is NP-hard.

**Theorem:** Language $CSAT$ is NP-complete.

**Proof:** It suffices to show the $CSAT$ is in NP. *(Can you prove this?)*
Chapter 34. NP-Completeness

The above discussion shows that $L_{CSAT}$ is NP-hard.

**Theorem**: Language $CSAT$ is NP-complete.

**Proof**: It suffices to show the $CSAT$ is in NP. (Can you prove this?)

Actually, the following language SAT was first proved to be NP-complete [Cook'71]

$$SAT = \{\phi : \text{CNF boolean formula } \phi \text{ is satisfiable}\}$$
Chapter 34. NP-Completeness

The above discussion shows that $L_{CSAT}$ is NP-hard.

**Theorem:** Language $CSAT$ is NP-complete.

**Proof:** It suffices to show the $CSAT$ is in NP. *(Can you prove this?)*

Actually, the following language SAT was first proved to be NP-complete [Cook'71]

$$SAT = \{\phi : \text{CNF boolean formula } \phi \text{ is satisfiable} \}$$

**Cook’s Theorem:** SAT is NP-complete.
The above discussion shows that $L_{CSAT}$ is NP-hard.

**Theorem:** Language $CSAT$ is NP-complete.

**Proof:** It suffices to show the $CSAT$ is in NP. (Can you prove this?)

Actually, the following language SAT was first proved to be NP-complete [Cook’71] https://www.cs.toronto.edu/~sacook/homepage/1971.pdf

$$SAT = \{\phi : \text{CNF boolean formula } \phi \text{ is satisfiable}\}$$

**Cook’s Theorem:** SAT is NP-complete.

Cook’s reduction: characterizing a polynomial-time computation on nondeterministic Turing machine with a boolean formula,
Chapter 34. NP-Completeness

The above discussion shows that $L_{CSAT}$ is NP-hard.

**Theorem:** Language $CSAT$ is NP-complete.

**Proof:** It suffices to show the $CSAT$ is in NP. *(Can you prove this?)*

Actually, the following language SAT was first proved to be NP-complete [Cook’71]

\[
SAT = \{ \phi : \text{CNF boolean formula } \phi \text{ is satisfiable} \}
\]

**Cook’s Theorem:** SAT is NP-complete.

Cook’s reduction: characterizing a polynomial-time computation on nondeterministic Turing machine with a boolean formula, such that a *nondeterministic path* leading to the accept state *corresponds* to an *assignment to the variables* making the formula TRUE.
Chapter 34. NP-Completeness

It is very easy to convert a boolean formula to a boolean circuit. So...
It is very easy to convert a boolean formula to a boolean circuit. So

**Theorem:** $SAT \leq_p CSAT$. 
Chapter 34. NP-Completeness

It is very easy to convert a boolean formula to a boolean circuit. So

**Theorem:** $SAT \leq_p CSAT$.

On the other hand,
Chapter 34. NP-Completeness

It is very easy to convert a boolean formula to a boolean circuit. So

**Theorem**: $SAT \leq_p CSAT$.

On the other hand,

**Theorem**: $CSAT \leq_p SAT$. 
It is very easy to convert a boolean formula to a boolean circuit. So

**Theorem:** $SAT \leq_p CSAT$.

On the other hand,

**Theorem:** $CSAT \leq_p SAT$.

**how to convert a circuit to a boolean formula** (from network to tree)?
Chapter 34. NP-Completeness

It is very easy to convert a boolean formula to a boolean circuit. So

**Theorem:** $SAT \leq_p CSAT$.

On the other hand,

**Theorem:** $CSAT \leq_p SAT$.

**how to convert a circuit to a boolean formula** (from network to tree)? simply replicating gates may blow-up the size of formula to exponential!
Chapter 34. NP-Completeness

**Theorem:** \( C\text{SAT} \leq_p \text{SAT} \).
Chapter 34. NP-Completeness

**Theorem:** $CSAT \leq_p SAT$.

is satisfiable if and only if formula $\phi$ is satisfiable:
Chapter 34. NP-Completeness

**Theorem:** $CSAT \leq_p SAT$.

is satisfiable if and only if formula $\phi$ is satisfiable:

\[
\phi = x_{10} \land (x_4 \leftrightarrow \neg x_3) \\
\land (x_5 \leftrightarrow (x_1 \lor x_2)) \\
\land (x_6 \leftrightarrow \neg x_4) \\
\land (x_7 \leftrightarrow (x_1 \land x_2 \land x_4)) \\
\land (x_8 \leftrightarrow (x_5 \lor x_6)) \\
\land (x_9 \leftrightarrow (x_6 \lor x_7)) \\
\land (x_{10} \leftrightarrow (x_7 \land x_8 \land x_9)).
\]
Chapter 34. NP-Completeness

**Theorem:** $CSAT \leq_p SAT$.

$x_1$

$x_2$

$x_3$

$x_4$

$x_5$

$x_6$

$x_7$

$x_8$

$x_9$

$x_{10}$

is satisfiable if and only if formula $\phi$ is satisfiable:

$$\phi = x_{10} \land (x_4 \leftrightarrow \neg x_3)$$

$$\land (x_5 \leftrightarrow (x_1 \lor x_2))$$

$$\land (x_6 \leftrightarrow \neg x_4)$$

$$\land (x_7 \leftrightarrow (x_1 \land x_2 \land x_4))$$

$$\land (x_8 \leftrightarrow (x_5 \lor x_6))$$

$$\land (x_9 \leftrightarrow (x_6 \lor x_7))$$

$$\land (x_{10} \leftrightarrow (x_7 \land x_8 \land x_9)).$$

$\phi$ can be transformed to an equivalent CNF formula.
Chapter 34. NP-Completeness

Landscape of NP problems and beyond
Chapter 34. NP-Completeness

Landscape of NP problems and beyond
Many problems/languages have been proved NP-complete (Karp70s)
Example 1:

$\text{SAT} \leq_{p} 3\text{SAT} (z) = \Rightarrow (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2)$

$(y, z) = \Rightarrow (y, z, x_1) \land (y, z, \neg x_1) \land (x, y, z) \Rightarrow (x, y, z, u, v) \Rightarrow (y, z, x_1) \land \neg x_1, u, v)$
Chapter 34. NP-Completeness

Examples of reduction techniques

Example 1: $\text{SAT} \leq_p \text{3SAT}$
Examples of reduction techniques

Example 1: $\text{SAT} \leq_p 3\text{SAT}$

($z$)
Examples of reduction techniques

Example 1: SAT $\leq_p$ 3SAT

$(z) \mapsto (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2)$
Examples of reduction techniques

Example 1: \( \text{SAT} \leq_p \text{3SAT} \)

\[
(z) \implies (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2)
\]

\[
(y, z)
\]
Examples of reduction techniques

Example 1: SAT $\leq_p$ 3SAT

$$(z) \iff (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2)$$

$$(y, z) \iff (y, z, x_1) \land (y, z, \neg x_1)$$
Chapter 34. NP-Completeness

Examples of reduction techniques

Example 1: SAT ≤ₚ 3SAT

\( z \mapsto (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2) \)

\( (y, z) \mapsto (y, z, x_1) \land (y, z, \neg x_1) \)

\( (x, y, z) \)
Examples of reduction techniques

Example 1: $\text{SAT} \leq_p \text{3SAT}$

\[
\begin{align*}
(z) &\implies (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2) \\
(y, z) &\implies (y, z, x_1) \land (y, z, \neg x_1) \\
(x, y, z) &\implies (x, y, z)
\end{align*}
\]
Examples of reduction techniques

Example 1: SAT \leq_p 3SAT

(z) \mapsto (z, x_1, x_2) \wedge (z, x_1, \neg x_2) \wedge (z, \neg x_1, x_2) \wedge (z, \neg x_1, \neg x_2)

(y, z) \mapsto (y, z, x_1) \wedge (y, z, \neg x_1)

(x, y, z) \mapsto (x, y, z)

(y, z, u, v)
Examples of reduction techniques

Example 1: SAT $\leq_p$ 3SAT

(z) $\mapsto$ $(z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2)$

(y, z) $\mapsto$ $(y, z, x_1) \land (y, z, \neg x_1)$

(x, y, z) $\mapsto$ (x, y, z)

(y, z, u, v) $\mapsto$ $(y, z, x_1) \land (\neg x_1, u, v)$
Chapter 34. NP-Completeness

Examples of reduction techniques

Example 1: \( \text{SAT} \leq_p \text{3SAT} \)

\[
(z) \quad \Rightarrow \quad (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2)
\]

\[
(y, z) \quad \Rightarrow \quad (y, z, x_1) \land (y, z, \neg x_1)
\]

\[
(x, y, z) \quad \Rightarrow \quad (x, y, z)
\]

\[
(y, z, u, v) \quad \Rightarrow \quad (y, z, x_1) \land (\neg x_1, u, v)
\]

\[
(y, z, u, v, w)
\]
Chapter 34. NP-Completeness

Examples of reduction techniques

Example 1: SAT $\leq_p$ 3SAT

\[
\begin{align*}
(z) & \implies (z, x_1, x_2) \land (z, x_1, \neg x_2) \land (z, \neg x_1, x_2) \land (z, \neg x_1, \neg x_2) \\
(y, z) & \implies (y, z, x_1) \land (y, z, \neg x_1) \\
(x, y, z) & \implies (x, y, z) \\
(y, z, u, v) & \implies (y, z, x_1) \land (\neg x_1, u, v) \\
(y, z, u, v, w) & \implies (y, z, x_1) \land (\neg x_1, u, x_2) \land (\neg x_2, v, w)
\end{align*}
\]
Chapter 34. NP-Completeness

Example 2: 3SAT \leq_p IS
An assignment TRUE to one literal in each clause corresponds to an independent set in the transformed graph.
Example 2: $3\text{SAT} \leq_p \text{IS}$
Example 2: 3SAT $\leq_p$ IS

$$(x_1 \lor x_2 \lor \overline{x_3}) \land (x_2 \lor x_3 \lor \overline{x_4}) \land (x_1 \lor \overline{x_2} \lor x_4)$$
Example 2: 3SAT $\leq_p$ IS

\[(x_1 \lor x_2 \lor \overline{x_3}) \land (x_2 \lor x_3 \lor \overline{x_4}) \land (x_1 \lor \overline{x_2} \lor x_4)\]

An assignment TRUE to one literal in each clause
Example 2: $3\text{SAT} \leq_p \text{IS}$

An assignment TRUE to one literal in each clause corresponds to an independent set in the transformed graph.
Summary

Scope of the Final Exam

▶ Minimum spanning tree concept/properties of MST, greedy algorithms, generic, Kruskal's and Prim's

▶ Shortest path (single source and all pairs) concept/properties of shortest path, greedy algorithms, relaxation technique
  - single source: Bellman-Ford, Shortest-path-DAG, Dijkstra's
  - all pairs: DP, Floyd-Warshall
Summary

Scope of the Final Exam

Minimum spanning tree concept/properties of MST, greedy algorithms, generic, Kruskal's and Prim's

Shortest path (single source and all pairs) concept/properties of shortest path, greedy algorithms, relaxation technique
  single source: Bellman-Ford, Shortest-path-DAG, Dijkstra's
  all pairs: DP, Floyd-Warshall
Scope of the Final Exam

- Minimum spanning tree
Summary

Scope of the Final Exam

▶ Minimum spanning tree

concept/properties of MST, greedy algorithms,
Summary

Scope of the Final Exam

- Minimum spanning tree
  concept/properties of MST, greedy algorithms,
generic, Kruskal’s and Prim’s
- Shortest path (single source and all pairs)
  concept/properties of shortest path, greedy algorithms,
  relaxation technique
  single source: Bellman-Ford, Shortest-path-DAG, Dijkstra’s
  all pairs: DP, Floyd-Warshall
Summary

Scope of the Final Exam

▶ Minimum spanning tree
  concept/properties of MST, greedy algorithms, generic, Kruskal’s and Prim’s
▶ Shortest path (single source and all pairs)
Scope of the Final Exam

- Minimum spanning tree
  concept/properties of MST, greedy algorithms, generic, Kruskal’s and Prim’s

- Shortest path (single source and all pairs)
  concept/properties of shortest path, greedy algorithms, relaxation technique
Summary

Scope of the Final Exam

- Minimum spanning tree
  concept/properties of MST, greedy algorithms, generic, Kruskal’s and Prim’s

- Shortest path (single source and all pairs)
  concept/properties of shortest path, greedy algorithms, relaxation technique
  single source: Bellman-Ford, Shortest-path-DAG, Dijkstra’s
Summary

Scope of the Final Exam

▶ Minimum spanning tree

concept/properties of MST, greedy algorithms, generic, Kruskal’s and Prim’s

▶ Shortest path (single source and all pairs)

concept/properties of shortest path, greedy algorithms, relaxation technique

single source: Bellman-Ford, Shortest-path-DAG, Dijkstra’s

all pairs: DP, Floyd-Warshall
Summary
Summary

Scope of the Final Exam (cont’)

NP-completeness theory, non-deterministic computation, certificate, checker, definitions of NP class, proof that a language is in NP. Reduction, polynomial-time reduction, properties. Definition of NP-hard, NP-complete languages, properties. NP-completeness proofs (simple, assembly of previous known reductions).
Summary

Scope of the Final Exam (cont’)

- NP-completeness theory
Scope of the Final Exam (cont’)

- NP-completeness theory
  - non-deterministic computation, certificate, checker,
Summary

Scope of the Final Exam (cont’)

- NP-completeness theory
  
  non-deterministic computation, certificate, checker,
  
  definitions of NP class, proof that a language is in NP
Scope of the Final Exam (cont’)

- NP-completeness theory
  - non-deterministic computation, certificate, checker,
  - definitions of NP class, proof that a language is in NP
  - reduction, polynomial-time reduction, properties
Summary

Scope of the Final Exam (cont’)

- NP-completeness theory
  - non-deterministic computation, certificate, checker,
  - definitions of NP class, proof that a language is in NP
  - reduction, polynomial-time reduction, properties
  - definition of NP-hard, NP-complete languages, properties
Scope of the Final Exam (cont’)

- NP-completeness theory
  
  non-deterministic computation, certificate, checker,

  definitions of NP class, proof that a language is in NP

  reduction, polynomial-time reduction, properties

  definition of NP-hard, NP-complete languages, properties

  NP-completeness proofs (simple, assembly of previous known reductions)
More about algorithms and complexity theory

1. More landscapes of intractability problems
   - polynomial-time reductions
   - complexity classes beyond \( P \) and \( NP \).

2. Coping with the intractability
   - Exact algorithms via parameterization (parameterized computation)
   - Randomized algorithms (Monte Carlo algorithms)
   - Approximation algorithms (an introduction)
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   • polynomial-time reductions
   • complexity classes beyond \( P \) and \( NP \).
2. Coping with the intractability
   • Exact algorithms via parameterization (parameterized computation)
   • Randomized algorithms (Monte Carlo algorithms)
   • Approximation algorithms (an introduction)
What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   - polynomial-time reductions
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   - polynomial-time reductions
   - complexity classes beyond $\mathcal{P}$ and $\mathcal{NP}$. 
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   - polynomial-time reductions
   - complexity classes beyond $\mathcal{P}$ and $\mathcal{NP}$.

2. Coping with the intractability
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   • polynomial-time reductions
   • complexity classes beyond $\mathcal{P}$ and $\mathcal{NP}$.

2. Coping with the intractability
   • Exact algorithms via parameterization (parameterized computation)
What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   - polynomial-time reductions
   - complexity classes beyond $\mathcal{P}$ and $\mathcal{NP}$.

2. Coping with the intractability
   - Exact algorithms via parameterization (parameterized computation)
   - Randomized algorithms (Monte Carlo algorithms)
More about algorithms and complexity theory

What will be in CSCI 8470 Advanced Algorithms

1. More landscapes of intractability problems
   - polynomial-time reductions
   - complexity classes beyond $\mathcal{P}$ and $\mathcal{NP}$.

2. Coping with the intractability
   - Exact algorithms via parameterization (parameterized computation)
   - Randomized algorithms (Monte Carlo algorithms)
   - Approximation algorithms (an introduction)