Université de Paris
LIPADE

Algorithmic Complexity

Examples of Problems and their Proof of Complexity

Jean-Guy Mailly (jean-guy.mailly@u-paris.fr)

2022

Outline

3-SAT

Definition

- k-CNF: a CNF formula such that each clause contains at most k literals
- 3-SAT$= \{\phi \mid \phi$ is a 3-CNF formula and ϕ is satisfiable$\}$

Theorem

3-SAT is NP-complete.

Independent Set

Definition

Given a non directed graph $G = \langle N, E \rangle$, an independent set is a set of nodes $I \subseteq N$ such that $\forall x, y \in I$, $\{x, y\} \notin E$

The Decision Problem

$IS = \{(G, k) \mid G \text{ has at least one independent set of size } \geq k\}$

We will prove that *IS* is NP-complete

IS $\in$ NP?

- To prove that IS $\in$ NP, we need to prove that verifying a positive certificate for IS is $\in$ P
- What is a positive certificate for IS?

IS $\in$ NP?

- To prove that IS $\in$ NP, we need to prove that verifying a positive certificate for IS is $\in$ P
- What is a positive certificate for IS?
- A positive certificate is an independent set of size $\geq k$

IS $\in$ NP?

- To prove that IS $\in$ NP, we need to prove that verifying a positive certificate for IS is $\in$ P
- What is a positive certificate for IS?
- A positive certificate is an independent set of size $\geq k$
- Exercise: find a polynomial algorithm for it

IS $\in$ NP: Proof

Algorithm 1 Verifiy IS Certificate

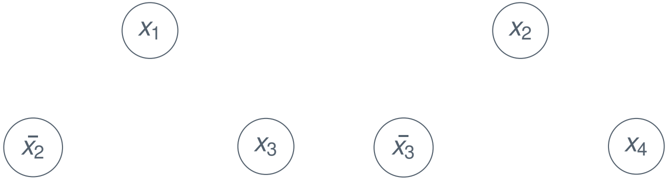
```
Input: G = ⟨N, E⟩, k, I ⊆ N
  if |I| < k then
      return NO
  else
      for x ∈ I do
          for y ∈ I do
              if {x, y} ∈ E then
                  return NO
              end if
          end for
      end for
      return YES
  end if
```

IS is NP-hard?

- We need to prove that $\mathcal{P} \leq^{\mathsf{P}}_{f}$ *IS*, with $\mathcal{P}$ a NP-hard problem
- We use $\mathcal{P} =$ 3-SAT
- We have to find f : 3-SAT$\rightarrow$ *IS* such that ϕ is a satisfiable 3-SAT formula iff $f(\phi) = (G, k)$ with
  - G is a non-directed graph
  - G has at least one independent set of size $\geq k$

The Poly-time Reduction for IS (1/4)

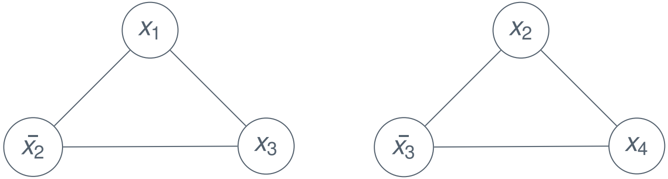
- We consider a 3-CNF formula ϕ on variables $X = \{x_1, \ldots, x_n\}$
- ϕ is a set of clauses $\{cl_1, \ldots, cl_m\}$, with each clauses made of (at most) 3 literals
- For every clause cl_i we make a "triangle" of nodes: *e.g.* $\phi = (x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_3 \vee x_4)$



- if the same literal appears in several clauses, we duplicate the node (not the case on this example)

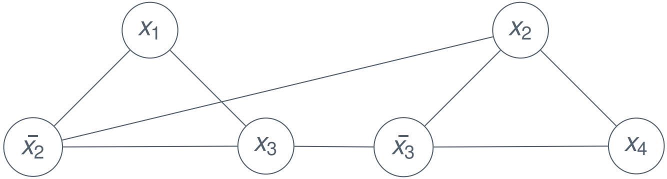
The Poly-time Reduction for IS (2/4)

- $\phi = (x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_3 \vee x_4)$
- We add an edge between nodes into a same clause



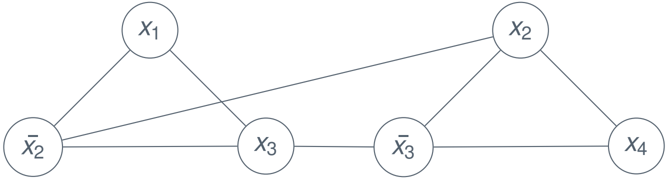
The Poly-time Reduction for IS (2/4)

- $\phi = (x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_3 \vee x_4)$
- We add an edge between nodes into a same clause
- We add an edge between pairs of contradictory nodes



The Poly-time Reduction for IS (2/4)

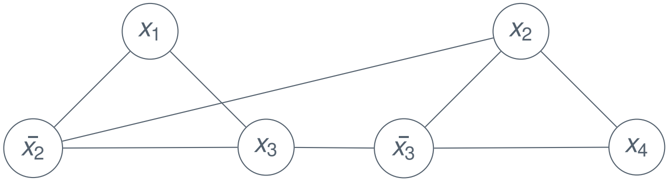
- $\phi = (x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_3 \vee x_4)$
- We add an edge between nodes into a same clause
- We add an edge between pairs of contradictory nodes



- These steps define G_ϕ; we choose $k = m$ (number of clauses/triangles)

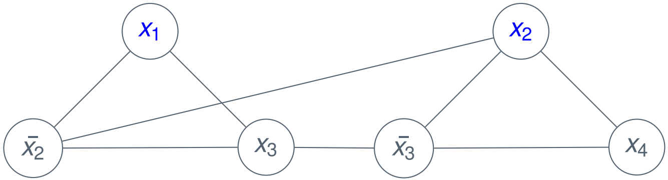
The Poly-time Reduction for IS (3/4)

- Computing is polynomial: at most $3 \times m$ nodes in the graph ($m =$ number of clauses)
- If ϕ is satisfiable, let ω be a model of ϕ. For each clause $cl_i \in \phi$, we choose a literal l_i in cl_i that is satisfied. The set of all l_i is an IS of G_ϕ, with size k. *E.g.* $\omega = \{x_1, x_2, x_3, x_4\} \models \phi$. Pour $cl_1 : x_1$, pour $cl_2 : x_2$



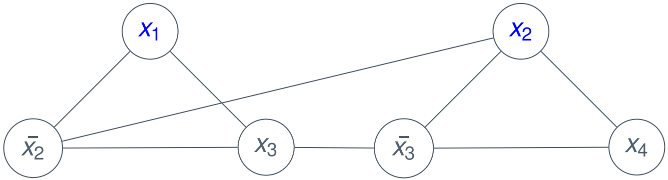
The Poly-time Reduction for IS (3/4)

- Computing is polynomial: at most $3 \times m$ nodes in the graph ($m =$ number of clauses)
- If ϕ is satisfiable, let ω be a model of ϕ. For each clause $cl_i \in \phi$, we choose a literal l_i in cl_i that is satisfied. The set of all l_i is an IS of G_ϕ, with size k. *E.g.* $\omega = \{x_1, x_2, x_3, x_4\} \models \phi$. Pour cl_1 : x_1, pour cl_2 : x_2



The Poly-time Reduction for IS (3/4)

- Computing is polynomial: at most $3 \times m$ nodes in the graph ($m =$ number of clauses)
- If ϕ is satisfiable, let ω be a model of ϕ. For each clause $cl_i \in \phi$, we choose a literal l_i in cl_i that is satisfied. The set of all l_i is an IS of G_ϕ, with size k. *E.g.* $\omega = \{x_1, x_2, x_3, x_4\} \models \phi$. Pour cl_1 : x_1, pour cl_2 : x_2



- $\phi \in$ 3-SAT$\Rightarrow (G_\phi, k) \in IS$

The Poly-time Reduction for IS (4/4)

- Suppose that $(G_\phi, k) \in IS$, let I be an IS of size $\geq k$
- For each triangle, there is exactly one node in I
- Nodes x_i and $\bar{x}_i$ are not together in I (since there is an edge between them)
- The nodes in I make a satisfying interpretation of ϕ

The Poly-time Reduction for IS (4/4)

- Suppose that $(G_\phi, k) \in IS$, let I be an IS of size $\geq k$
- For each triangle, there is exactly one node in I
- Nodes x_i and $\bar{x}_i$ are not together in I (since there is an edge between them)
- The nodes in I make a satisfying interpretation of ϕ
- $(G_\phi, k) \in IS \Rightarrow \phi \in$ 3-SAT

The Poly-time Reduction for IS (4/4)

- Suppose that $(G_\phi, k) \in \mathit{IS}$, let I be an IS of size $\geq k$
- For each triangle, there is exactly one node in I
- Nodes x_i and $\bar{x}_i$ are not together in I (since there is an edge between them)
- The nodes in I make a satisfying interpretation of ϕ
- $(G_\phi, k) \in \mathit{IS} \Rightarrow \phi \in$ 3-SAT
- $3-\mathrm{SAT} \leq_f^{\mathrm{P}} \mathit{IS}$: IS is NP-hard

The Poly-time Reduction for IS (4/4)

- Suppose that $(G_\phi, k) \in IS$, let I be an IS of size $\geq k$
- For each triangle, there is exactly one node in I
- Nodes x_i and $\bar{x}_i$ are not together in I (since there is an edge between them)
- The nodes in I make a satisfying interpretation of ϕ
- $(G_\phi, k) \in IS \Rightarrow \phi \in$ 3-SAT
- $3\text{−SAT} \leq_f^{\mathrm{P}} IS$: IS is NP-hard
- We conclude that IS is NP-complete

Outline

Independent Set

Clique

Clique

Definition

Given a non directed graph $G = \langle N, E \rangle$, a clique is a set of nodes $C \subseteq N$ such that $\forall x, y \in C$, $\{x, y\} \in E$

The Decision Problem

$Clique = \{(G, k) \mid G \text{ has at least one clique of size } \geq k\}$

We will prove that *Clique* is NP-complete

Clique $\in$ NP?

- To prove that *Clique* $\in$ NP, we need to prove that verifying a positive certificate for *Clique* is $\in$ P
- What is a positive certificate for Clique?

Clique $\in$ NP?

- To prove that *Clique* $\in$ NP, we need to prove that verifying a positive certificate for *Clique* is $\in$ P
- What is a positive certificate for Clique?
- A positive certificate is a clique of size $\geq k$

Clique $\in$ NP?

- To prove that *Clique* $\in$ NP, we need to prove that verifying a positive certificate for *Clique* is $\in$ P
- What is a positive certificate for Clique?
- A positive certificate is a clique of size $\geq k$
- Exercise: find a polynomial algorithm for it

Clique $\in$ NP: Proof

Algorithm 2 Verifiy Clique Certificate

Input: $G = \langle N, E \rangle, k, C \subseteq N$

```
if |C| < k then
    return NO
else
    for x ∈ C do
        for y ∈ C do
            if {x, y} ∉ E then
                return NO
            end if
        end for
    end for
    return YES
end if
```

Clique is NP-hard?

- We will prove that *IS* $\leq_f^{\mathsf{P}}$ *Clique*
- Exercise: prove it

Clique is NP-hard: Intuition

- From $(G = \langle N, E \rangle, k)$ an instance of *IS*, make $(G' = \langle N', E' \rangle, k')$ an instance of *Clique*:

Clique is NP-hard: Intuition

- From $(G = \langle N, E \rangle, k)$ an instance of *IS*, make $(G' = \langle N', E' \rangle, k')$ an instance of *Clique*:
  - $k' = k$
  - $N' = N$
  - $E' = \mathit{Pairs}(N) \setminus E$, where $\mathit{Pairs}(N) = \{\{x, y\} \mid x, y \in N\}$

Clique is NP-hard: Intuition

- From $(G = \langle N, E \rangle, k)$ an instance of *IS*, make $(G' = \langle N', E' \rangle, k')$ an instance of *Clique*:
  - $k' = k$
  - $N' = N$
  - $E' = Pairs(N) \setminus E$, where $Pairs(N) = \{\{x, y\} \mid x, y \in N\}$
- $S \subseteq N$ is an IS of size k in G iff S is a clique of size k in G'