

# NP

- quelles sont les preuves (solutions) des instances positives ?
- que fait le vérificateur ?
- justifier que les preuves sont de taille polynomial et que le vérificateur est polynomial

Ex Clique  $C$  de graphe  $G=(V,E)$

$C \subseteq V$  tq. pour tous  $u, v \in C$ ,  
 $u \neq v : (u, v) \in E$

## CLIQUE

Entrée :  $G$ , entier  $k$

Q : Est-ce que  $G$  possède une clique de taille  $k$  ?

① Algs naïf pour CLIQUE :

- générer tous les  $C \subseteq V, |C|=k$
- vérifier si un des ensembles est clique

Complexité : ( $|V|=n$ )

$$\binom{n}{k} \leq n^k$$

pas poly!

$$k=3$$

$$k=n/2$$

$$n^{n/2} = 2^{O(n \log n)}$$

② CLIQUE  $\in$  NP

$x = G, k$  (graphe + entier)

$y$  sous-ensemble de sommets  
de taille  $k$

$V$  prend  $\langle x, y \rangle$  et vérifie que  $y$   
est une clique de  $G$

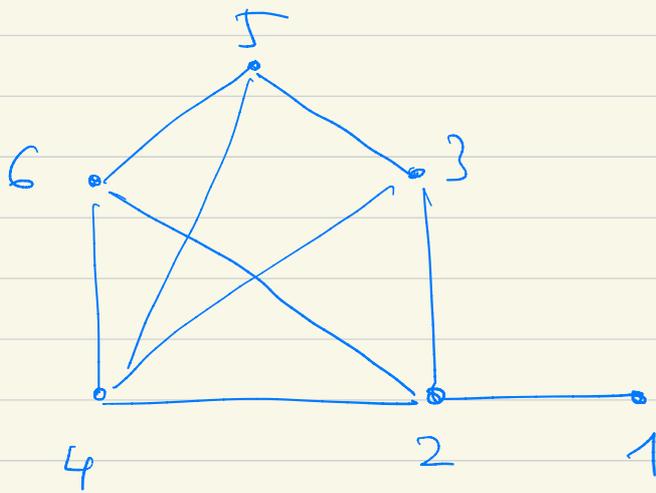
- $y$  est de taille polynomiale, en supposant que  $k \leq |V|$   $\rightarrow O(n)$   
(sinon, la réponse est NON)
  - $V$  est polynomial parce que vérifier que les sommets de  $y$  sont 2 à 2 adjacents se fait en temps poly  $O(n^2)$  avec matrice d'incidence
- 

### Chemin Hamiltonien

Entrée  $G$  non-orienté

Q: Est-ce que  $G$  possède un chemin hamiltonien (qui visite chaque sommet exactement une fois) ?

Ex



Algo naïf

$$V = \{1, 2, \dots, n\}$$

1 énumérer toutes les permutations de  $V$

2 vérifier s'il y en a une qui définit un chemin

Complexité

$$n! \cdot n \in 2^{O(n \log n)}$$

# perm. ↓  
étape 2

$$n! \leq n^n$$

CH  $\in$  NP

exp:  $2^{\sqrt{n}}$   
 $n = 2^{\log n}$

- entrée  $x$  : graphe  $G = (V, E)$   
preuve  $y$  : permutation de  $V$
- vérificateur  $V$  prend  $(G, y)$  et vérifie que  $y$  est bien un chemin
- $|y| \leq \underline{n}$  taille( $x$ )  
polynôme  $p$  : linéaire  $O(n+m)$   
temps de  $V$  : linéaire  $O(n^2)$  (avec matrice)  
 $p(n) = n$

---

$P \subseteq NP$

$A$  est pl. de la classe  $P$   $A \in P$   
donc il ex. algo polynomial  $\Pi$  qui résout  $A$  en temps polynomial

$$y = \emptyset$$

$$V := \Pi$$

On sait trouver des solutions pour  
A sans aide (= certificat (preuve))

---



les pb. de NP possèdent des  
vérificateurs polynomiaux

les pb de P possèdent des  
algorithmes polynomiaux

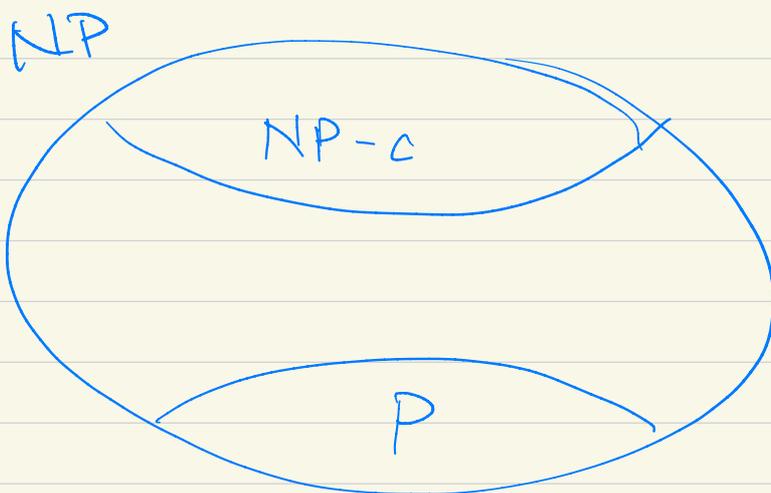
Def

$A$  est NP-complet si:

1)  $A \in \text{NP}$

2)  $\forall A' \in \text{NP} : A' \leq_p A$

( $A$  est NP-difficile)



NP-c :  
NP-complet

Si  $A$  est NP-complet et  $A \in P$   
alors  $P = \text{NP}$

$$\left[ \begin{array}{l} A' \leq_p A \text{ et } A \in P \\ \Rightarrow A' \in P \end{array} \right.$$

+ (2)

On verra que SAT est NP-complet.

Donc, si SAT  $\in$  P alors NP = P

Mais aussi: 3-COL  $\in$  P

Chemin hamiltonien  $\in$  P

:

3-COL  $\leq_p$  SAT

Chemin ham.  $\leq_p$  SAT

Pour SAT on a des algorithmes spécifiques ("SAT-solveurs") qui sont plus performants que les approches naïves.

On peut les utiliser, en les combinant avec les réductions.