



Classe NP vs. P

Un problème A est ...

- dans P s'il existe un algorithme

polynomial qui le résout

(cad., l'algorithme accepte une

instance x de A si et seulement si

x est positive)

- dans NP s'il existe un vérificateur

polynomial V qui accepte une

paire (x, y) si et seulement si

y montre que x est instance

positive de A (y : preuve / solution)

ET ...

...

1) x est instance positive de $A \Rightarrow$
il existe un y de taille polyn.
tq. V accepte (x, y)

2) x est instance négative de $A \Rightarrow$
il n'existe aucun y tq.
 V accepte (x, y)

Ex ① $A = \text{SAT}$

x : formule φ en CNF

y : valuation val : $\{1, \dots, n\} \rightarrow \{0, 1\}$

des variables de φ (x_1, \dots, x_n)

$n + 3 \cdot m$
↓ clauses

② $A = 3\text{-COL}$

x : graphe G

y : coloration des sommets avec $\{1, 2, 3\}$

$n + m$
arcs

Parfois ce n'est pas très facile de vérifier l'appartenance à NP.

Ex. Programmation linéaire en entiers
(ILP, integer linear programming)

L'entrée est un système d'équations linéaires, avec coefficients entiers :

$$A \vec{x} = \vec{b}$$

Entrée $\left\{ \begin{array}{l} A : \text{matrice } m \times n \text{ avec } A(i,j) \in \mathbb{Z} \\ \vec{b} : \text{vecteur de } \mathbb{Z}^m \end{array} \right.$

On cherche $\vec{x} \in \mathbb{Z}^n$ tq. $A\vec{x} = \vec{b}$

par exemple : $A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ -2 & 1 & & \\ & -2 & 1 & \\ & & & \dots \end{pmatrix} \vec{b} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$$x_2 = 2x_1, \quad x_3 = 2x_2, \quad \dots \quad x_n = 2x_{n-1}$$

$x_1 = 1$ \rightarrow sol. de valeurs exponent.

$$x_n = 2^{n-1}$$

Mais la représentation binaire de 2^n
est de taille polynomiale!

La difficulté ici est de démontrer
que s'il existe une solution, alors
il ex. une de taille polynomiale.

Ex Voyageur de commerce

Entrée : graphe complet $V = \{1, \dots, n\}$

avec arcs pondérés :

$$p(i, j) = \text{pois de l'arc } i \rightarrow j \\ \in \mathbb{N} \cup \{\infty\}$$

et entier $P \in \mathbb{N}$

Question est-ce qu'il ex. un chemin
qui passe exactement une fois par
chaque sommet et dont le poids est P ?

Autrement dit : est-ce qu'il ex. une suite d'indices i_1, \dots, i_n tq.

$i_j \neq i_k$ pour tous $j \neq k$ (donc une permutation de $\{1, \dots, n\}$)

$$\text{tq. } \sum_{j=1}^{n-1} P(i_j, i_{j+1}) = P ?$$

les poids ici sont représentés en binaire (\rightarrow valeurs exponentielles)

X : graphe avec arcs pondérés
+ P

γ : permutation de $\{1, \dots, n\}$

V doit calculer la somme

$$\sum_{j=1}^{n-1} P(i_j, i_{j+1})$$

\rightarrow possible en temps polynomial