Théorème de Ladner

Weikun He

ENS

Janvier 2011

Le théorème de Ladner

Théorème (R. E. Ladner, 1975)

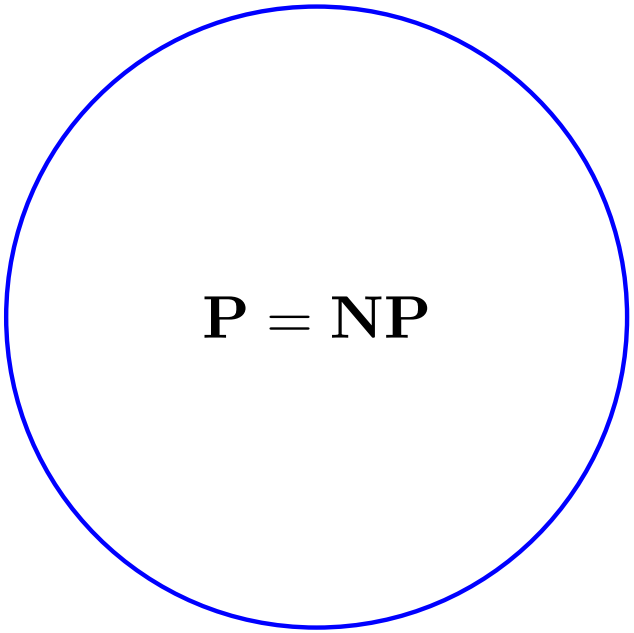
Si $\mathbf{P} \neq \mathbf{NP}$, *alors il existe des langages qui ne sont ni* $\mathbf{P}$ *ni* $\mathbf{NP}$*-complets.*

P vs NP

Un langage de **NP** est dit **NP**-intermédiaire s'il n'est ni dans **P** ni **NP**-complet.
Deux situations sont possibles.

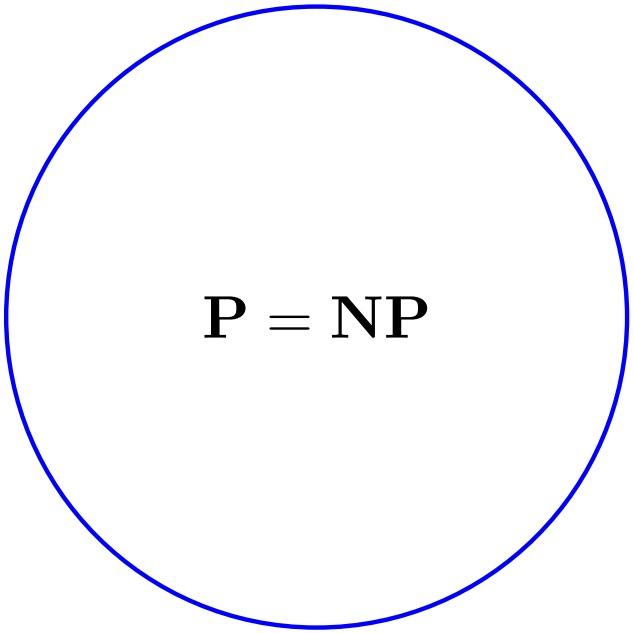
P vs NP

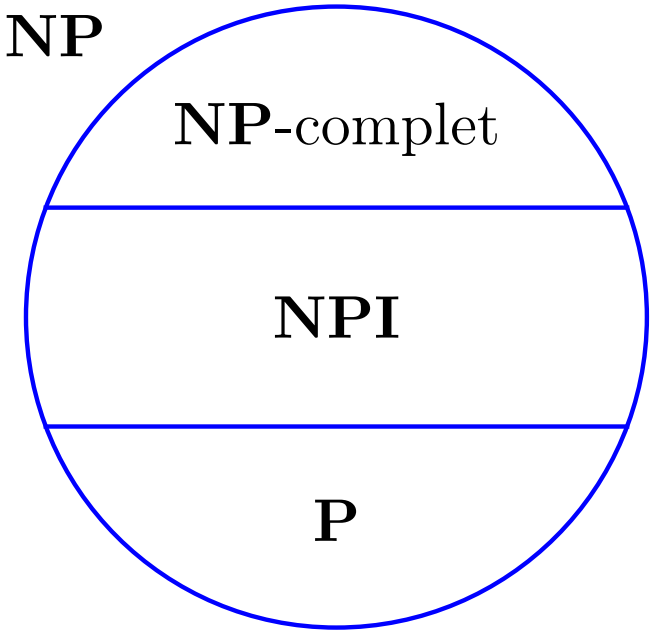
Un langage de **NP** est dit **NP**-intermédiaire s'il n'est ni dans **P** ni **NP**-complet.
Deux situations sont possibles.



P vs NP

Un langage de **NP** est dit **NP**-intermédiaire s'il n'est ni dans **P** ni **NP**-complet.
Deux situations sont possibles.





Démonstration

On va montrer ceci :

Proposition

Si $L \in \mathbf{NP} \setminus \mathbf{P}$, alors il existe un langage $L' \in \mathbf{NP} \setminus \mathbf{P}$ tel que L' se réduit (en temps polynomial) à L mais L ne se réduit pas à L'.

Définition de L'

Soit L un langage dans $\mathbf{NP} \setminus \mathbf{P}$.

Définition de L'

Soit L un langage dans $\mathbf{NP} \setminus \mathbf{P}$. On définit un langage L' et une fonction $f : \mathbb{N} \to \mathbb{N}$.

Définition de L'

Soit L un langage dans $\mathbf{NP} \setminus \mathbf{P}$. On définit un langage L' et une fonction $f : \mathbb{N} \to \mathbb{N}$.
On pose $L' = \{w01^{n^{f(n)}} \mid w \in L \text{ et } n = |w|\}$.

Définition de L'

Soit L un langage dans $\mathbf{NP} \setminus \mathbf{P}$. On définit un langage L' et une fonction $f : \mathbb{N} \to \mathbb{N}$.
On pose $L' = \{w01^{n^{f(n)}} \mid w \in L \text{ et } n = |w|\}$.
Et pour $n \in \mathbb{N}$, $f(n)$ est, s'il existe, le plus petit $i < \log\log n$ tel que pour toute entrée $w \in \{0,1\}^{\leq \log\log n}$, M_i accepte w au bout de $|w|^i$ étapes de calcul si et seulement si $w \in L'$ Et si un tel i n'existe pas, on pose $f(n) = \log\log n$.

Propriétés de f

- Le calcul de $f(n)$, comme tel qu'on l'a décrit, s'arrête en un temps polynomial en n.

Propriétés de f

- Le calcul de $f(n)$, comme tel qu'on l'a décrit, s'arrête en un temps polynomial en n.
- f est croissante.

Propriétés de f

- Le calcul de $f(n)$, comme tel qu'on l'a décrit, s'arrête en un temps polynomial en n.
- f est croissante.
- f est stationnaire si $L' \in \mathbf{P}$.

Propriétés de f

- Le calcul de $f(n)$, comme tel qu'on l'a décrit, s'arrête en un temps polynomial en n.
- f est croissante.
- f est stationnaire si $L' \in \mathbf{P}$.
- f tend vers l'infini si $L' \notin \mathbf{P}$.

Et tout se passe bien . . .

- $L' \leqslant_p L$ et par conséquent, $L' \in \mathbf{NP}$

Et tout se passe bien . . .

- $L' \leqslant_p L$ et par conséquent, $L' \in \mathbf{NP}$
- Si $L' \in \mathbf{P}$ alors $L \leqslant_p L'$. Ce n'est pas possible.

Et tout se passe bien . . .

- $L' \leqslant_p L$ et par conséquent, $L' \in \mathbf{NP}$
- Si $L' \in \mathbf{P}$ alors $L \leqslant_p L'$. Ce n'est pas possible.
- $L \not\leqslant_p L'$

Quelques remarques

- Si $\mathbf{P} \neq \mathbf{NP}$, alors il y a une infinité de hiérarchies strictes dans l'intérieur de $\mathbf{NP}$.

Quelques remarques

- Si $\mathbf{P} \neq \mathbf{NP}$, alors il y a une infinité de hiérarchies strictes dans l'intérieur de $\mathbf{NP}$.
- L' n'est pas naturel.