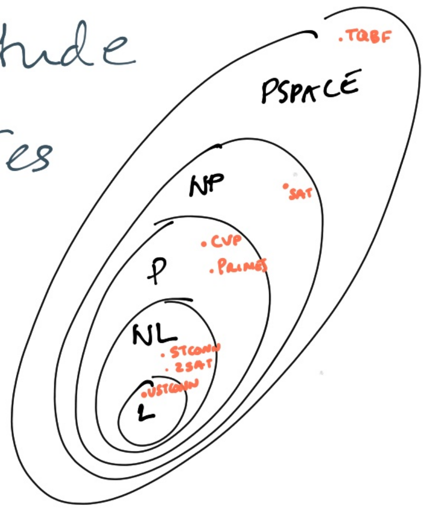
INTRODUCTION à la COMPLEXITÉ

Sophie Laplante

IRIF, Université Paris-Diderot

Plan :

- Qu'est-ce qu'une classe de complexité ?
- P, NP, PSPACE, L, NL
- Réductions, complétude
- Classes probabilistes



Classes de complexité

__Def__ Un __langage__ est un sous-ensemble de chaînes sur un alphabet fini Σ. $(L \subseteq \Sigma^*)$

__Ex.__ $\Sigma = \{0,1\}$

$L_{01} = \{w \in \Sigma^* \mid w$ contient autant de 0 que de 1 $\}$

__Def__ Une __classe de complexité__ est un ensemble de langages $(\mathcal{C} \subseteq 2^{\Sigma^*})$

__Ex__ $REG = \{L \subseteq \Sigma^* \mid L$ est un langage regulier $\}$

$= \{L \subseteq \Sigma^* \mid \exists$ un automate fini A déterministe t.q. $L = \mathcal{L}(A)\}$

__Prop__ $L_{01} \notin REG$

Quelques langages

STCONN = $\{\langle G, s, t\rangle$: il existe un chemin de s à t dans G (orienté) $\}$

USTCONN = $\{\langle G, s, t\rangle$: il existe un chemin de s à t dans G (non-orienté) $\}$

PRIMES = $\{x$: x est premier $\}$

CVP = $\{\langle C, x\rangle$: Le circuit C sur entrée x s'évalue à VRAI $\}$

SAT = $\{\varphi$: il existe une valuation x qui rend la formule $\varphi(x)$ VRAIE $\}$

TQBF = $\{\Phi$: la formule quantifiée Φ est VRAIE $\}$

...

Modèle + ressource + borne

Typiquement on définit une classe de complexité en termes de ressource de calcul

→ Modèle de calcul (Automate, circuit, machine de Turing, ...)

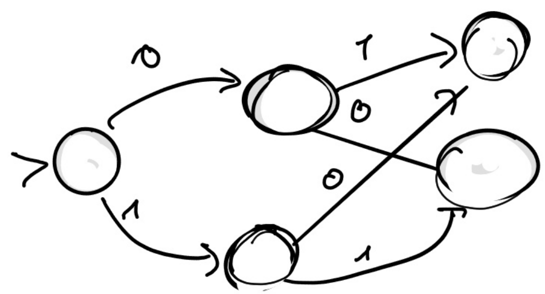
→ Notion de coût (temps, espace, communication...)

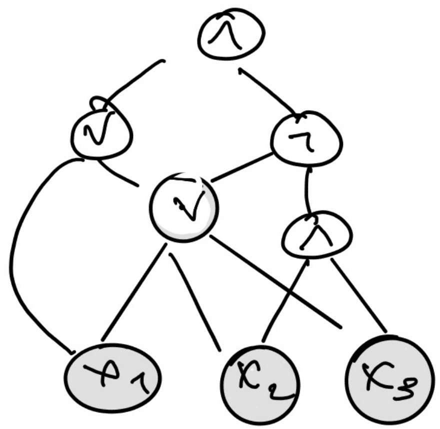
→ Borne asymptotique (logarithmique, polynomial...)

Modèle de calcul

Spécifie

- Les opérations élémentaires
- Comment elles s'enchaînent
- L'état initial (où se trouve la donnée du problème ?)
- L'état final (comment on s'arrête ? où se trouve le résultat ?)





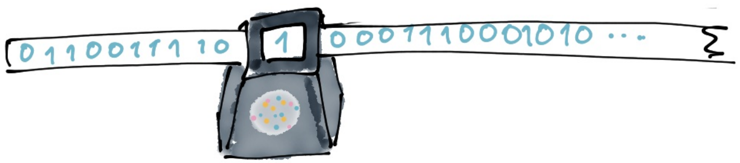
Machines de Turing

[Turing 1936] On Computable Numbers, with an application to the Entscheidungsproblem.

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]



A chaque instant :

- lit un symbole
- écrit un symbole
- met à jour l'état
- déplace la tête de lecture

Fonction de transition.

$$\boxed{\delta(a, q) = (a', q', G/D)}$$

symbole

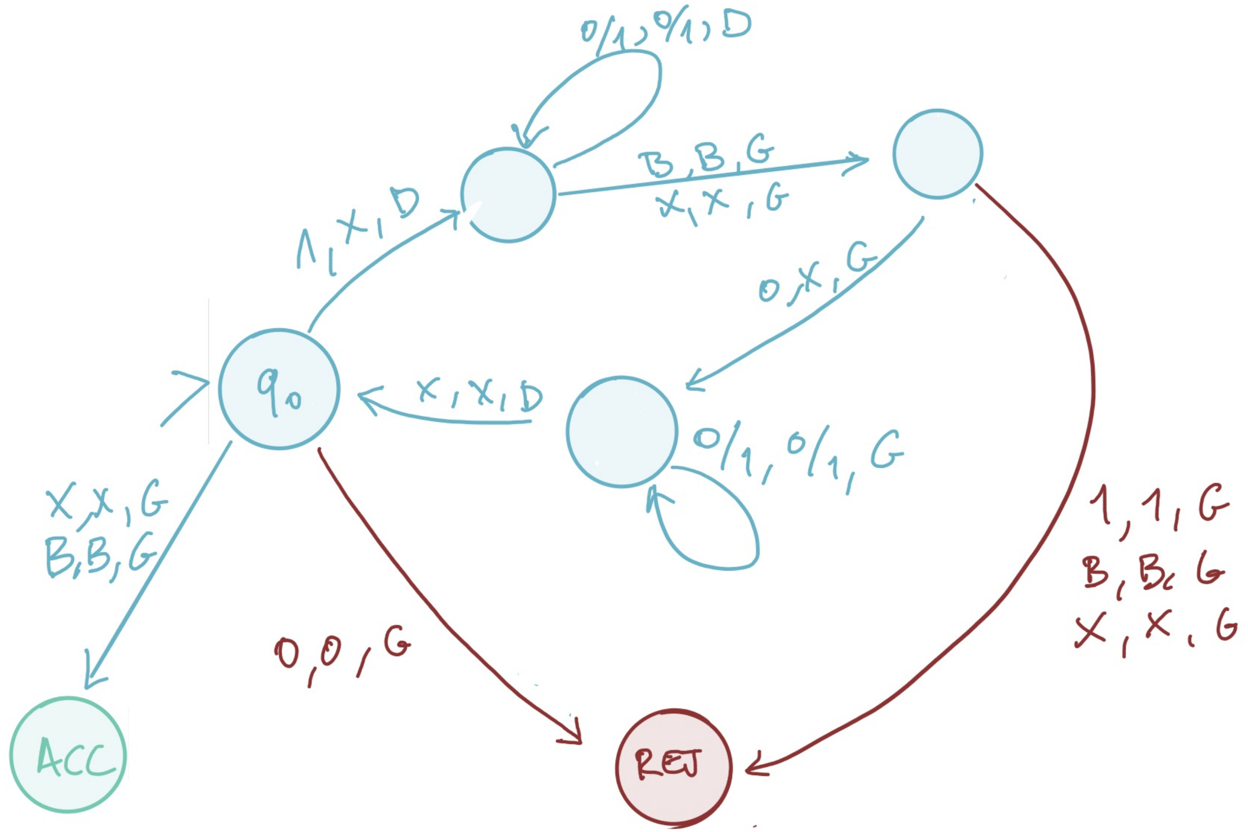
état

direction

La machine ACCEPTE si elle arrive dans l'état q_{ACC}

elle REJETTE si elle arrive dans l'état q_{REJ}

Machines de Turing



B = blanc.

X	X	X	1	1	...	0	0	X	X	X

$$\mathcal{L}(M) = \{ 1^n 0^n \mid n \geqslant 0 \}$$

Exercices

1. Donner une machine de Turing qui décide le langage

$$L_{0=1} = \{ w \mid w \text{ est un palindrome} \}$$

2. Montrer que si L est décidable par une Machine de Turing qui s'arrête au bout de $t(n)$ étapes sur toute donnée de taille n, alors $\overline{L}$ l'est aussi.

La classe P

Modèle de calcul : Machine de Turing

Ressource : Nombre de transitions

Borne : polynomial en la taille de la donnée.

$L \in P \Leftrightarrow \exists$ une Machine de Turing M, polynôme $p(\cdot)$:

$\forall x \in \Sigma^*$:

(1) M accepte $x \Leftrightarrow x \in L$

(2) Le nombre de transitions de M sur entrée x $T_M(x) = O(p(|x|))$

taille de

"L est décidable en temps $O(p(n))$"

Temps et espace

Def Pour une fonction $t : \mathbb{N} \to \mathbb{R}$, on définit

$$\mathrm{DTIME}(t) = \{ L : L \text{ est décidable en temps } O(t(n)) \}$$

$$\mathrm{DSPACE}(t) = \{ L : L \text{ est décidable en espace } O(t(n)) \}$$

M s'arrête sur toutes les entrées ; sur entrée x, M touche au plus $t(|x|)$ cases du ruban.

Ex

$$P = \bigcup_{c \geq 0} \mathrm{DTIME}(n^c)$$

$$\mathrm{PSPACE} = \bigcup_{c \geq 0} \mathrm{DSPACE}(n^c)$$

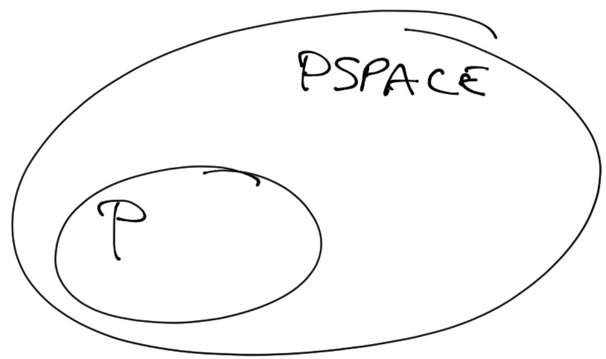
Temps et espace

Thm $\forall t : \mathbb{N} \to \mathbb{R}$

$$\mathrm{DTIME}(t) \subseteq \mathrm{DSPACE}(t)$$

Preuve En temps t, on ne peut pas toucher plus de t cases du ruban.

Cor $P \subseteq \mathrm{PSPACE}$



Temps et espace

Thm $\forall t : \mathbb{N} \to \mathbb{R}$

$$\mathrm{DSPACE}(t) \subseteq \mathrm{DTIME}(\ ?\ ) \quad \ldots$$

Def Une configuration d'une Machine de Turing

est constituée de

- l'état
- la position de la tête
- le contenu du ruban

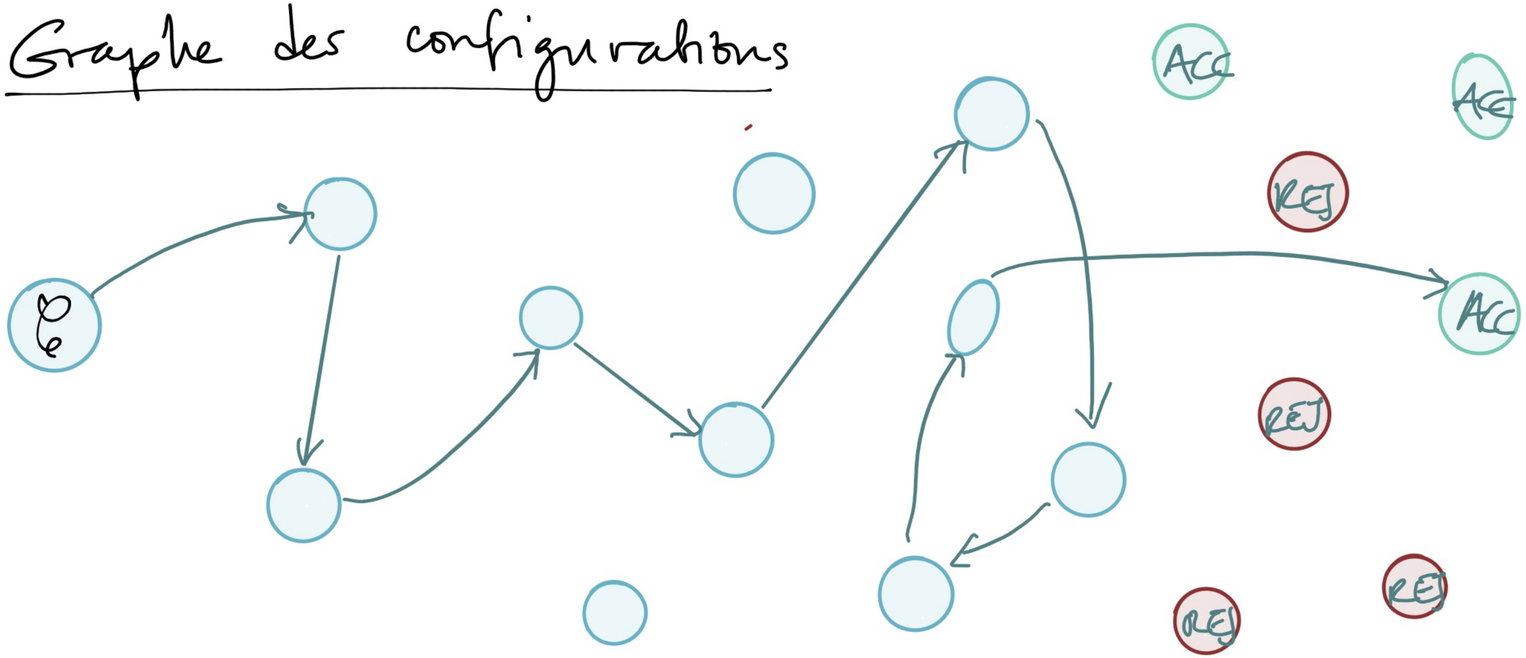
$\mathcal{C} = u\,q\,v$

$$\mathcal{C}_{init} \vdash \mathcal{C}_1 \vdash \mathcal{C}_2 \vdash \ldots\ldots \vdash \mathcal{C}_T$$

$\mathcal{C}_{init} = q_0 x$

Temps et espace

Graphe des configurations



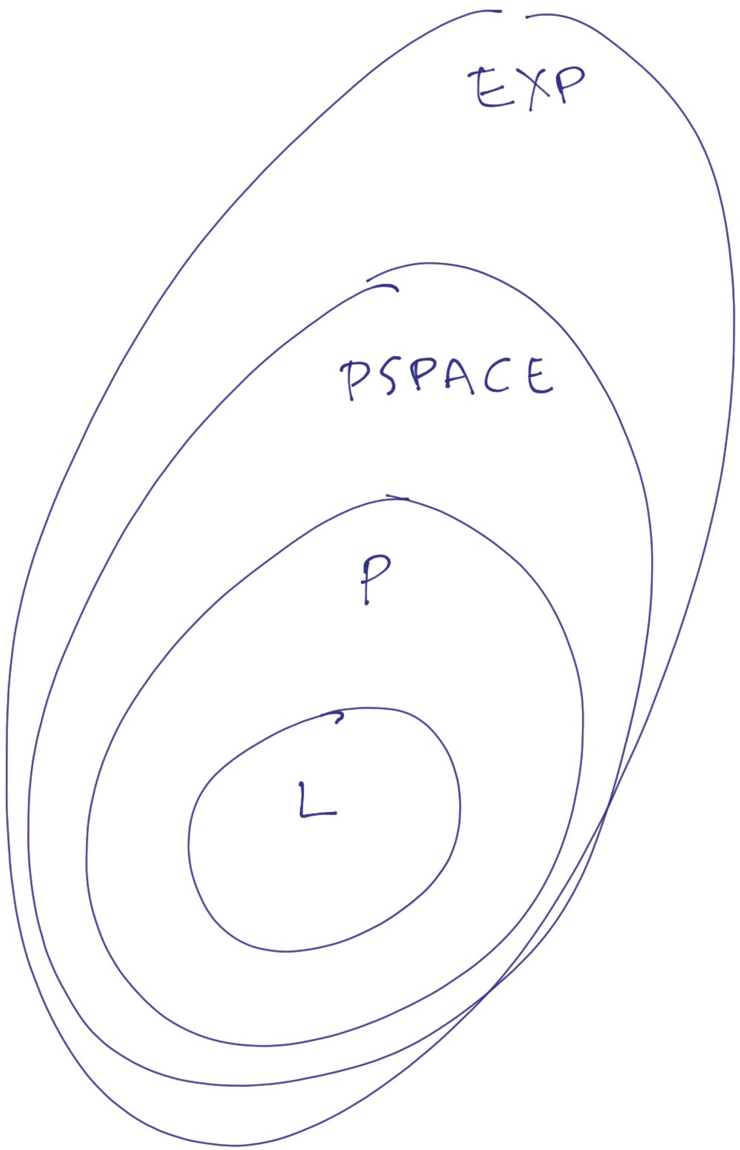
Si L est décidable en espace $O(t(n))$:

- # Configurations = ________ .

- Temps $\leq$ ________

$\Rightarrow$ $DSPACE(t(n)) \subseteq DTIME($ ________ $)$

Temps et espace



$$EXP = \bigcup_{c>0} DTIME(2^{n^c})$$

$$PSPACE = \bigcup_{c>0} DSPACE(n^c)$$

$$P = \bigcup_{c>0} DTIME(n^c)$$

$$L = DSPACE(\log n)$$

Ex
USTCONN $\in$ L
PRIMES $\in$ P [2004]
TQBF $\in$ PSPACE

Théorèmes de hiérarchie

Hartmanis.

<u>Thm</u> [Hartmanis & Stearns 1965]

Si $g(n) = o\left(\frac{f(n)}{\log(f(n))}\right)$

alors $\mathrm{DTIME}(g(n)) \subsetneq \mathrm{DTIME}(f(n))$

<u>Thm</u> Si $g(n) = o(f(n))$

alors $\mathrm{DSPACE}(g(n)) \subsetneq \mathrm{DSPACE}(f(n))$

<u>Preuve</u>. Par diagonalisation...

<u>Cor</u> $P \neq EXP$

$L \neq PSPACE$

Classes nondéterministes

Deux façons de définir les classes non-déterministes.

(1) Modèle de calcul :

Remplacer la fonction de transition par une relation de transition (plusieurs transitions sont possibles.)

Une machine nondéterministe ACCEPTE x s'il existe une suite de transitions légales qui mène à un état acceptant.

Classes nondéterministes

Deux façons de définir les classes non-déterministes.

(1) Modèle de calcul :

Remplacer la <u>fonction</u> de transition par une <u>relation</u> de transition (plusieurs transitions sont possibles.)

(2) De façon abstraite : pour toute classe $\mathcal{C}$:

$L \in N \circ \mathcal{C}$ ssi

$\exists L' \in \mathcal{C}$, polynôme $p(\cdot)$

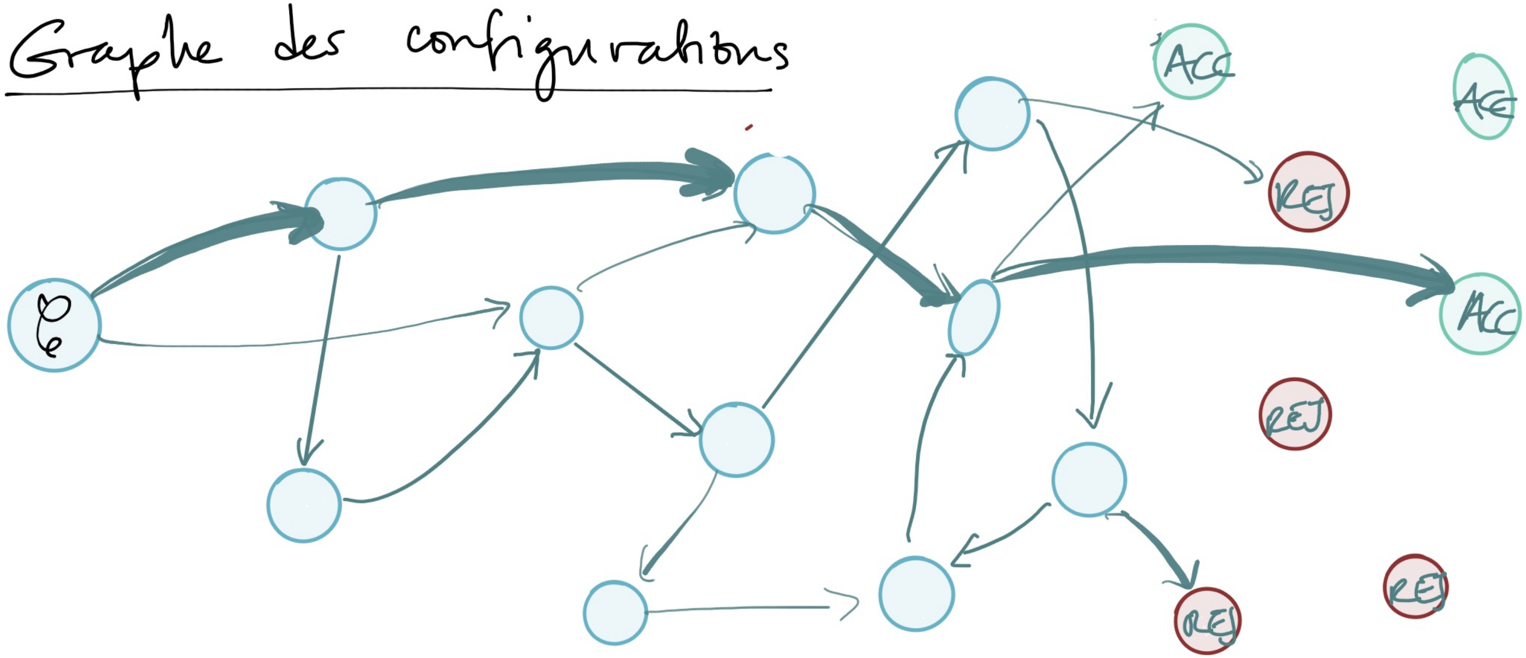
$$x \in L \leftrightarrow \exists y \in \Sigma^{\leq p(|x|)} \ (x,y) \in L'$$

L' = " prédicat de vérification d'appartenance à L

y = témoin ou preuve que $x \in L$

Classes non déterministes

Graphe des configurations



$x \in L \iff$ Il existe un chemin dans le graphe des configurations qui mène de l'état initial ($C_0 = q_0 x$) à une configuration acceptante.

Classes nondéterministes

Def Pour une fonction $t : \mathbb{N} \to \mathbb{R}$, on définit

$$\mathbf{N}TIME(t) = \{ L : L \text{ est décidable en temps } O(t(n)) \text{ sur une M.T nondéterministe} \}$$

$$\mathbf{N}SPACE(t) \quad \{ L : L \text{ est décidable en espace } O(t(n)) \text{ sur une M.T. non éterministe} \}$$

Ex

$$\mathbf{N}P = \bigcup_{c>0} \mathbf{N}TIME(n^c)$$

$$PSPACE = \bigcup_{c>0} DSPACE(n^c)$$

Classes nondéterministes

Définition équivalente

$\boxed{L \in NP}$ ssi $\exists L' \in P$, polynôme p

t.q. $x \in L \Leftrightarrow \exists y \in \Sigma^{p(|x|)}$

$(x, y) \in L'$

Ex $CLIQUE = \{ (G, k) : G$ contient une clique de taille $\geq k \}$

témoin ou preuve

prédicat de vérification.

$((G, k), S) \in V_{CLIQUE} \Leftrightarrow S$ est un sous-ensemble de sommets de G qui forme une clique de taille $\geq k$

V_{CLIQUE} est décidable en temps polynomial.

$\Rightarrow CLIQUE \in NP$