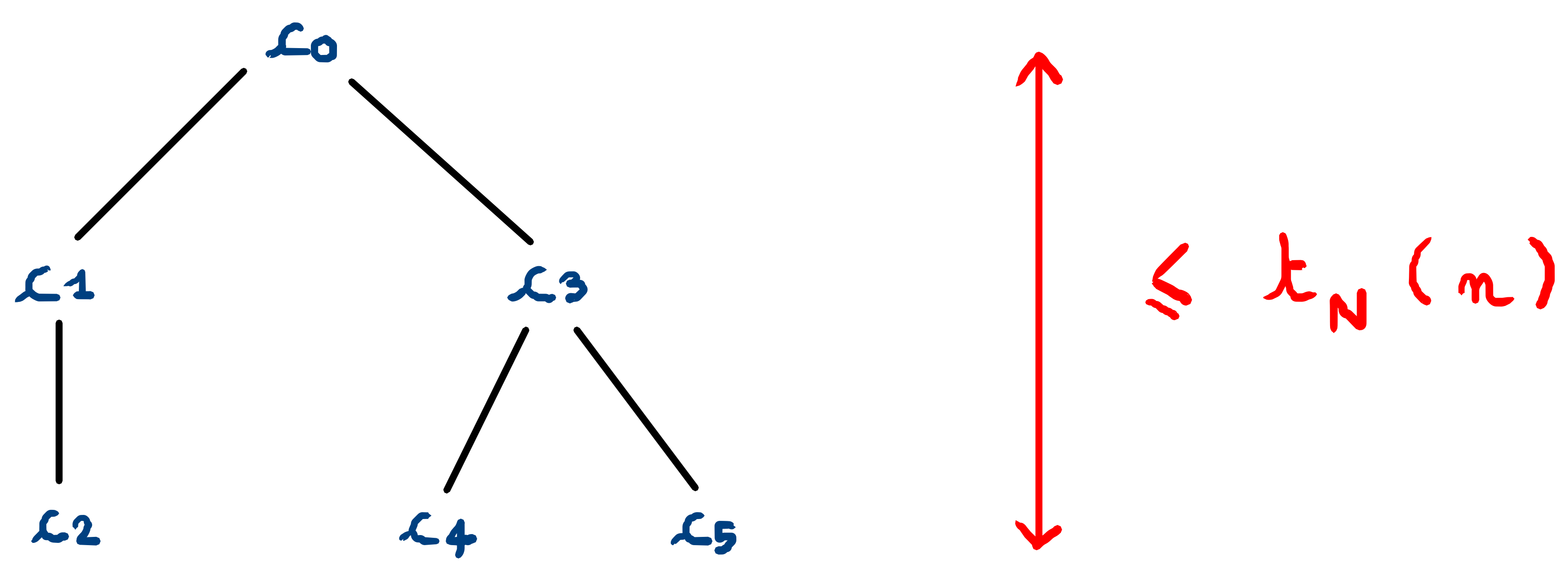
complexité et non-déterminisme

soit N NMT qui s'arrête toujours sur tout run

la complexité t_N de N est une fonction sur $\mathbb{N}$ tq $t_N(n)$ est le plus petit entier tq $N(x)$ s'arrête en moins de $t_N(n)$ étapes sur tout run sur toute entrée x de taille $\leq n$

notons alors que la profondeur de l'arbre d'exécution sur toute entrée x de taille $\leq n$ est alors $\leq t_N(n)$



classes de complexité

soit N NMT à k rubans

si $t_N = O(f)$ alors on écrit

$\mathcal{L}(N) \in NTIME_k(f)$

on note $NTIME_*(f) = \bigcup_{k \geq 1} NTIME_k(f)$

classe des langages reconnaissables en temps non-déterministe f

propriétés

clairement :

$$\mathrm{DTIME}_k(f) \subseteq \mathrm{NTIME}_k(f)$$

de plus, si $N \in \mathrm{NTIME}_k(f)$, alors $\exists\, M \in \mathrm{DTIME}_k(2^{O(f)})$ tel que $M \sim N$.

semi-équivalence

notons que le nombre maximal de transitions

possibles depuis une configuration est borné $\leq a$

car δ est finie

donc arbre d'exécution d'arité $\leq a$ et de

profondeur $\leq t_N(n)$

$\Rightarrow$ moins de $a^{t_N(n)}$ noeuds

$$= a^{\Theta(f(n))}$$

d'où une simulation déterministe exponentielle

la NMT universelle

il existe $\mathcal{U}'$ NMT à 3 rubans telle que pour toute NMT N et entrée x,

$$\mathcal{U}'(\langle N \rangle \# x) \sim N(x)$$

de plus il faut $O(|\langle N \rangle| \cdot n)$ étapes pour simuler n étapes de N.

idée $\mathcal{U}'$ a 3 rubans

1) entrée $\langle N \rangle \# x$

2) état simulé de N

3) ruban de travail de N

comment exécuter la simulation ?

- copier x sur 3)

  $q_0 = 0$ 2)

- simuler N en lisant 2), 3) puis en cherchant dans $\langle N \rangle$ sur 1) de manière non-déterministe une transition applicable remarque : cette recherche doit terminer donc après avoir tout lu, si l'on a rien choisi, on prend la dernière règle applicable lue.

classes connues

temps polynomial non-déterministe

$$NP = NPTIME = \bigcup_{k \geq 1} NTIME_*(n \to n^k)$$

temps exponentiel non-déterministe

$$NEXP = NEXPTIME = \bigcup_{k \geq 1} NTIME_*(n \to 2^{n^k})$$

évidemment, $P \subseteq NP$ et $EXP \subseteq NEXP$

exemples

SAT = { φ | formule booléenne satisfiable } $\in$ NP

- quel encodage pour la formule ?

  par exemple en notation polonaise

- s'il y a $k \leq |\varphi|$ variables ?

  deviner k valuations, ie écrire de manière non déterministe un mot binaire de longueur k

- tester la valuation pour si elle satisfait φ

  en temps polynomial

$TSP = \{ G, w \mid G$ graphe pondéré

admettant un chemin hamiltonien de

chaque sommet visité une fois exactement

poids $\leq w \}$

$\in NP$ en devinant puis testant un chemin propriétés

NP $\subseteq$ NEXP

stricte ?

NP $\subseteq$ EXP par la propriété prouvée plus tôt

NP et NEXP sont stables par $\cup$ $\cap$

trivial car on parle de NMTs qui terminent toujours

pas besoin d'entrelacement

on ne sait en revanche pas pour ^{c}

on note donc coX la classe telle que

$L \in coX$ ssi $^cL \in X$

$ANTILOGY = \{ \varphi \mid$ formule booléenne toujours fausse $\}$

$\in coNP$

c'est le complémentaire de $SAT \in NP$

Théorème de hiérarchie non-déterministe en temps

soient f et g constructibles en temps tq

$$(n \longrightarrow f(n+1)) = o(g)$$

alors

$$\mathrm{NTIME}_*(f) \underset{\text{stricte}}{\subset} \mathrm{NTIME}_*(g)$$

conséquence

$NP \subset NEXP$

stricte

considérer $f(n) = 2^n$

$g(n) = 2^{3n}$

on a

$$NTIME_*(f) \subset NTIME_*(g)$$

$NP \subseteq$ $\subseteq NEXP$

Théorème de certification

$L \in NP$ (i)

ssi

$\exists L' \in P$ sur un alphabet Σ' et un polynôme

π tels que

$x \in L \iff \exists y \in \Sigma'^{\leq \pi(|x|)}$ dit certificat (ii)

$$x \# y \in L'$$

(ii) $\Rightarrow$ (i)

soit M acceptant L' en temps P

considérer N qui :

- calcule $\pi(|x|)$ P
- devine un mot y de taille $\leq \pi(|x|)$ NP
- simule M sur $x \# y$ P

N accepte L en temps NP

(i) $\Rightarrow$ (ii)

soit N acceptant L en temps NP

idée : $\Sigma' = \delta$

y est la suite de transitions d'un run de N sur x

(de taille P), $\pi = t_N$

soit M qui sur l'entrée $x \# y$ simule le run y

de N sur x

$L' = \mathcal{L}(M) \in P$ et convient

on peut dire que les problèmes NP ont des solutions compactes et faciles (polynomiales) à vérifier mais difficiles à trouver

problèmes	certificats
SAT	une valuation
TSP	un chemin hamiltonien
CLIQUE	une clique

effondrement de la hiérarchie

on a $P \subseteq NP \subseteq EXP \subseteq NEXP$

et $P \neq EXP$

$NP \neq NEXP$

si $P = NP$ alors $EXP = NEXP$

en utilisant le padding theorem cf TD 4

de plus $NP = coNP$