rappel sur les réductions

A est Turing-réductible à B ssi

$x \in A \iff f(x) \in B$

f calculable

on note $A \leq_T B$

réductions polynomiales

A est polynomialement réductible à B ssi

$x \in A \iff f(x) \in B$

f calculable en temps polynomial

on note $A \leq_T^P B$

un exemple

CLIQUE $=$ $\{ (G, k) \mid G$ admet une k-clique $\}$

IS $=$ $\{ (G, k) \mid G$ a k sommets indépendants $\}$

CLIQUE $\leq_T^P$ IS

considérer $f : (G, k) \longrightarrow ({}^c G, k)$

propriétés

- transitivité : $A \leq_T^P B$ et $B \leq_T^P C$

  $\Rightarrow A \leq_T^P C$

- si $A \leq_T^P B$ et $B \in P$ (resp. NP)

  alors $A \in P$ (resp. NP)

difficulté et complétude

soit X une classe de complexité

un langage A est dit X-dur ssi $\forall L \in X$,

$L \leq_T^P A$

de plus si $A \in X$ alors A est X-complet

notons que si $A \leq_T^P B$ et A est X-dur,

alors B est aussi X-dur

P-complétude

L P-complet ssi $L \in P$ et L non trivial
$\neq \emptyset, \Sigma^*$

$\Rightarrow$ $L \in P$ évident

$\emptyset$ ne peut être P dur, sans quoi $\forall A \in P$
resp Σ^*
$\exists f$ réduction polynomiale,

$x \in A$ ssi $f(x) \in \emptyset$
resp Σ^*

donc $A = \emptyset$ absurde
resp Σ^*

$\Leftarrow$ soient $x_1 \in L$

$x_2 \notin L$

soit $A \in P$

soit $f : y \longrightarrow \begin{cases} x_1 & \text{si } y \in A \\ x_2 & \text{sinon} \end{cases}$

f est calculable en temps polynomial car

$y \in A$? l'est

et f est bien une réduction

un problème NP-dur

$\mathcal{H}' = \{ \langle N \rangle \# x \mid N$ est une NMT s'arrêtant sur $x \}$

est NP-dur

bien sûr, pas NP-complet car indécidable soit $L \in NP$ accepté par N

soit N' semblable à N mais qui accepte quand N

s'arrête et boucle sinon

$$f : x \longrightarrow \langle N' \rangle \# x$$

est une réduction polynomiale

donc $L \leq_T^P \mathcal{H}'$

un problème NP-complet

$\mathcal{A}^t = \{ \langle N \rangle \# x \# 0^t \mid N$ est une NMT acceptant x en t étapes ou moins $\}$

est NP-complet

déjà, $\mathcal{A}^t$ est NP

considérez une machine qui sur l'entrée $\langle N \rangle \# x \# 0^t$ simule $N(x)$ de manière non déterministe sur t étapes soit $L \in NP$ accepté par N de complexité

$t_N \leqslant \pi$ où π polynôme

considérons

$$f : x \longrightarrow \langle N \rangle \# x \# 0^{\pi(|x|)}$$

f est calculable en temps polynomial car π aussi

f est une réduction car $N(x)$ accepte en moins

de $\pi(|x|)$ étapes

donc $L \leqslant^P_T \mathcal{H}^t$

théorème de Cook

SAT est NP-complet

en pratique les SAT-solvers ont beaucoup d'applications

notons que SAT $\in$ NP

une ébauche de preuve

soit $L \in NP$ accepté par N de complexité

$t_N \leqslant \pi$ où π polynôme

pour un x donné il faut trouver φx telle que

$x \in L$ ssi φx satisfiable

remarquons que l'exécution de N sur x utilise

au plus $2\pi(|x|)+1$ cellules

$$\big|\ -\pi(|x|)\ \big|\ \ldots\ \big|0\big|\ \ldots\ \big|\ \pi(|x|)\ \big|$$

on va représenter chaque configuration de chacune des $\pi(|x|)$ étapes du calcul par des variables booléennes

$x_{i,j,a} = 1$ ssi la case i à l'étape j contient la lettre a $\qquad O(|\Gamma| \times \pi(|x|)^2)$ variables

idem pour l'état et la position de la tête

$y_{q,j}$ $\qquad z_{i,j}$

il faut que φx assure que l'enchaînement des configurations corresponde bien à un run de N

si on a une transition $p, a \longrightarrow q, b, L$

pour l'appliquer à la case i à l'étape j

$x_{i,j,a} \wedge y_{p,j} \wedge z_{i,j}$ case i à l'étape j

$x_{i,j+1,b} \wedge y_{q,j+1} \wedge z_{i-1,j+1}$ étape $j+1$

au final en combinant différentes contraintes

(enchaînement des configurations , exclusion

mutuelle des règles , bon ruban de départ ,

acceptation , etc ...) on aboutit à

φ_x de taille polynomiale en x

des variations

$CSAT = \{ \varphi \mid \varphi$ en CNF satisfiable $\}$

$\wedge \ \vee$ $\qquad \neg$ sur les variables seulement

$3SAT = \{ \varphi \mid \varphi$ en 3-CNF satisfiable $\}$

$\wedge (\cdot \vee \cdot \vee \cdot)$

CSAT et 3SAT sont NP-complets

par réduction de SAT

et non à SAT

applications

IS est NP-complet

déjà, IS est NP

certificat : un ensemble indépendant de taille k

vérifiable en temps P

montrons que $3SAT \leq_T^P IS$

soit $\varphi = \bigwedge_{i=1}^{m} (y_1^i \vee y_2^i \vee y_3^i)$ $\quad y_i^j = x_k$ ou $\neg x_k$

construisons G tel que G admet un m I.S.

ssi φ satisfiable

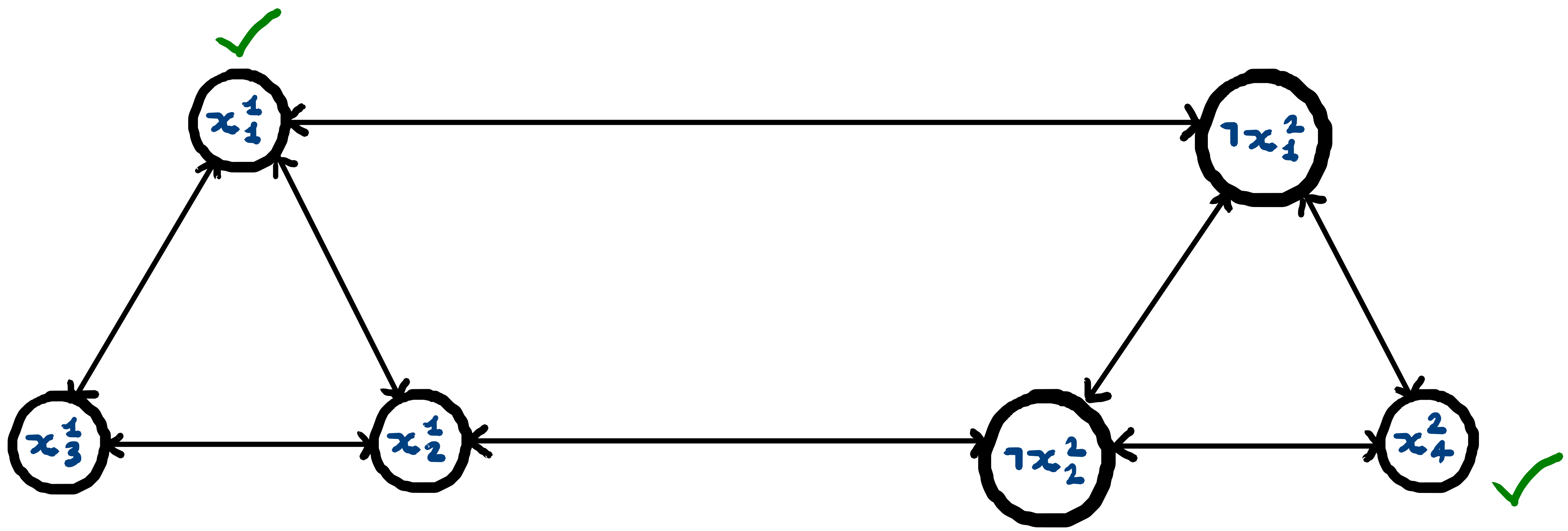
. $3m$ sommets, un sommet par litéral y_i^j

. on relie les litéraux opposés x_k et $\neg x_k$

et ceux dans une même clause

m I.S. ssi un litéral vrai par clause ie φ vraie

$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee x_4)$$



d'autres exemples

CLIQUE est NP-complet

en réduisant IS à CLIQUE par complémentation

VERTEXCOVER = { (G, k) | G a une vertex cover de taille k }

sommets passant par toutes les arêtes

de même

i.s. de taille k dans G

ssi

v.c. de taille n - k dans G

un effondrement

si un langage L qui est NP complet est aussi P

alors $P = NP$

en effet, pour tout A NP, par complétude

$A \leq_P^T L$ aussi P

donc A est P