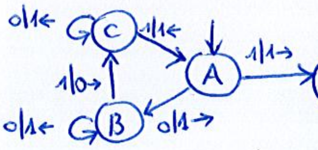
M1 - THÉORIE DE LA COMPLEXITÉ - 2024-2025



$BB(3) = 21$
$BB(4) = 107$
$BB(5) = 47.176.870$
$BB(6) \geq 10 \uparrow\uparrow 15$

DÉF : MT D À $k \geq 2$ RUBANS $M = (\Sigma, \Gamma, B, Q, q_0, q_a, q_r, \delta)$
(IN-RO, OUT-WO, TRAVAIL)
AVEC $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma^{k-1} \to Q \times \Gamma^{k-1} \times \{\leftarrow, \cdot, \to\}^k$.

MT ND AVEC $\delta \subseteq \left((Q \setminus \{q_a, q_r\}) \times \Gamma^{k-1}\right) \times \left(Q \times \Gamma^{k-1} \times \{\leftarrow, \circ, \to\}^k\right)$.
↳ ARBRE DE CALCUL, EXÉCUTION = CHEMIN DE LA RACINE À UNE FEUILLE.

EXO : FACTEUR abaa AVEC MTD ET MTND.

RMK : AU PLUS 2 TRANSITIONS ND SUFFISENT (PSEUDO CODE : GUESS(0, 1) OU DEVINER(0, 1))

CONFIGURATIONS : $Q \times (\Gamma^k)^{\mathbb{Z}} \times \mathbb{Z}^k$, FINALE SI q_a OU q_r (ARRÊT : ACCEPTE OU REJETTE).

RECONNAISSANCE DE LANGAGE (= PB DÉCISION) : $L(M) \subseteq \Sigma^*$ L'ENSEMBLE DES MOTS D'ENTRÉE POUR LESQUELS :
- D : LE CALCUL ACCEPTE.
- ND : IL EXISTE UN CALCUL QUI ACCEPTE. ⚠

RMK : MT D CALCULE $M : \Sigma^* \to \Gamma^*$.

TEMPS $t_M(x)$:
- D : NOMBRE D'ÉTAPES DE CALCUL.
- ND : NOMBRE MAXIMAL D'ÉTAPES DE CALCUL. ET $t_M(n) = \max_{x \in \Sigma^n} t_M(x)$.

ESPACE $s_M(x)$:
- D : NOMBRE DE CASES UTILISÉES SUR RUBANS DE TRAVAIL.
- ND : NOMBRE MAXIMAL DE CASES ″ .

CODE $\langle M \rangle$.

THM [1-S] (MTD UNIVERSELLE AVEC PERTE EN TEMPS LOG) : $\exists$ UNE MTD U T.Q.
$\forall M : \exists \varphi_M : \Sigma_M^* \to \Sigma_U^* : \forall x \in \Sigma_M^* : U(\langle M \rangle, \varphi_M(x))$ SIMULE $M(x)$,
ET $\exists \alpha_M : \forall x \in \Sigma_M^* : M(x)$ TEMPS t ESPACE $s \Rightarrow U(\langle M \rangle, \varphi_M(x))$ TEMPS $\leq \alpha_M(1 + t.\log t)$ ESPACE $\leq \alpha_M(s + \log t)$.

THM [2-AB] (MTND UNIVERSELLE OPTIMALE) : $\exists$ UNE MTND U T.Q.
$\forall N : \exists \varphi_N : \Sigma_N^* \to \Sigma_U^* : \forall x \in \Sigma_N^* : U(\langle N \rangle, \varphi_N(x))$ ACCEPTE SSI $N(x)$ ACCEPTE,
ET $\exists \alpha_N : \forall x \in \Sigma_N^* : N(x)$ TEMPS $t \Rightarrow U(\langle N \rangle, \varphi_N(x))$ TEMPS $\leq \alpha_N t$ (ESPACE POTENTIELLEMENT TRÈS GRAND).

THM [2-E] (ACCÉLÉRATION LINÉAIRE) : $\forall \varepsilon > 0$: SI $L(M) = L$ EN TEMPS $\leq t(n)$ AVEC M UNE MTD OU MTND,
ALORS $\exists M' : L(M') = L$ EN TEMPS $\leq (1 + \varepsilon)n + \varepsilon t(n)$. SI $n = o(t(n))$ ALORS FACTEUR MULTIPLICATIF.

DEF : $\mathrm{DTIME}(t(n)) = \{ L \mid \exists M$ une MTD avec $L(M) = L$ en temps $O(t(n)) \}$

$\mathrm{NTIME}(t(n)) = \{ L \mid \exists N$ une MTND avec $L(N) = L$ en temps $O(t(n)) \}$.

THM [2-5] (hiérarchie temps dét) : soit $g(n)$ constructible en temps et $f(n)$ t.q. $f(n).\log(f(n)) \in o(g(n))$, alors $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$.

Corollaire : $\forall k \in \mathbb{N}$: $\mathrm{DTIME}(n^k) \subsetneq \mathrm{DTIME}(n^{k+1})$.

THM [2-A7] (hiérarchie temps non-dét) : soit $g(n)$ croissante et constructible en temps et $f(n)$ t.q. $f(n) \neq 0$ et $f(n+1) = o(g(n))$, alors $\mathrm{NTIME}(f(n)) \subsetneq \mathrm{NTIME}(g(n))$.

Corollaire : $\forall k \in \mathbb{N}$: $\mathrm{NTIME}(n^k) \subsetneq \mathrm{NTIME}(n^{k+1})$.

DEF : $P = \bigcup_{k \in \mathbb{N}} \mathrm{DTIME}(n^k)$ $\qquad NP = \bigcup_{k \in \mathbb{N}} \mathrm{NTIME}(n^k)$

$EXP = \bigcup_{k \in \mathbb{N}} \mathrm{DTIME}(2^{n^k})$ $\qquad NEXP = \bigcup_{k \in \mathbb{N}} \mathrm{NTIME}(2^{n^k})$.

THM [2-A0] (caractérisation existentielle de NP)

$A \in NP$ ssi $\exists$ un polynôme $p(n)$ et $B \in P$ t.q. $x \in A \Leftrightarrow \exists y \in \{0,1\}^{p(|x|)} : (x,y) \in B$.

NB : aussi possible pour NEXP.

IDÉE : le certificat y correspond au chemin acceptant de la MTND pour A sur x.

Preuve : $\Rightarrow$: Soit N reconnaissant A en temps $q(n)$.

À chaque étape, N a au plus r choix (ne dépend pas de l'entrée).

Une suite de choix (chemin dans l'arbre de calcul) de A sur une entrée x peut donc être encodé comme un mot $y \in \{0,1\}^*$ de taille $q(|x|).\lceil \log_2(r) \rceil$.

Soit $p(n) = q(n).\lceil \log_2(r) \rceil$ et $B = \{ (x,y) \mid y \in \{0,1\}^{p(|x|)}$ encode un chemin de $N(x)$ qui accepte $\}$.

Par définition de l'acceptation d'une MTND, on a $x \in A \Leftrightarrow \exists\, y \in \{0,1\}^{p(|x|)} : (x,y) \in B$.

On a aussi $B \in P$ puisqu'avec y il s'agit de simuler $N(x)$ sur un chemin ($\rightsquigarrow$ DET).

$\Leftarrow$: Soit M une MTD pour B en temps poly $q(n)$.

Voici une MTND pour A, sur l'entrée x : $\begin{cases} \text{- deviner } y \in \{0,1\}^{p(|x|)} \\ \text{- accepter ssi } M(x,y) \text{ accepte.} \end{cases}$

A fonctionne en temps poly : $p(n) + q(n + p(n))$. Donc $A \in NP$. $\square$

Morale : tous les "deviner" au début, puis déterministe.

P = trouver efficacement (thèse de Cobham-Edmonds, robuste).

NP = vérifier une solution efficacement.

THM [2-AG] : $\forall t : \mathbb{N} \to \mathbb{N}$: $\mathrm{DTIME}(t(n)) \underset{\uparrow \text{ IMMÉDIAT}}{\subseteq} \mathrm{NTIME}(t(n)) \subseteq \mathrm{DTIME}(2^{O(t(n))})$.

IDÉE : UNE MTD SIMULE UNE MTND EN PARCOURANT UN À UN TOUS SES CHEMINS DE CALCUL.

PREUVE : SOIT N UNE MTND EN TEMPS $\alpha t(n)$. ON LA SIMULE AVEC LA MTD SUIVANTE, SUR L'ENTRÉE x :

- POUR TOUT CHEMIN y DE TAILLE $\alpha t(n)$ FAIRE :) $r^{\alpha t(n)} = 2^{\alpha t(n) \log_2 r}$ CHEMINS
  - SIMULER $N(x)$ SUR LE CHEMIN y) TEMPS $O(t(n))$
  - SI LA SIMULATION ACCEPTE ALORS ACCEPTER
- REJETER.

DONC $2^{\alpha t(n) \log_2 r} \times O(t(n)) = 2^{O(t(n))}$. □

COROLLAIRE : $P \underset{\uparrow \text{ IMMÉDIAT}}{\subseteq} NP \overset{\text{LÀ} \downarrow}{\subseteq} EXP \underset{\uparrow \text{ IMMÉDIAT}}{\subseteq} NEXP$. (HIÉRARCHIE $\Rightarrow P \subsetneq EXP$ ET $NP \subsetneq NEXP$)

THM [2-AU] : $P = NP \Rightarrow EXP = NEXP$. NB : LA RÉCIPROQUE EST OUVERTE.

PREUVE : ON SUPPOSE $P = NP$. SOIT $L \in NEXP$ RECONNU PAR UNE MTND N EN TEMPS 2^{n^k}.

SOIT $\tilde{L} = \{(x, 1^{2^{|x|^k}}) \mid x \in L\}$ (PADDING = REMBOURRAGE).

ENTRÉE DE TAILLE $m \geq 2^{|x|^k}$. VOICI UNE MTND $\tilde{N}$ POUR $\tilde{L}$:

- VÉRIFIER QUE L'ENTRÉE EST DE LA FORME (x,y) AVEC $y = 1^{2^{|x|^k}}$, SINON REJETER.
- EXÉCUTER $N(x)$.

$L(\tilde{N}) = \tilde{L}$ EN TEMPS $O(2^{n^k})$, LINÉAIRE EN m, DONC $\tilde{L} \in NP$.

PAR HYPOTHÈSE, ALORS $\tilde{L} \in P$ RECONNU PAR UNE MTD $\tilde{M}$ EN TEMPS POLY $m^{k'}$.

VOICI UNE MTD M POUR L, SUR L'ENTRÉE x :

- ÉCRIRE $(x, 1^{2^{|x|^k}})$ SUR UN RUBAN DE TRAVAIL.) TEMPS $O(2^{n^k})$
- EXÉCUTER $\tilde{M}(x, 1^{2^{|x|^k}})$.) TEMPS $m^{k'}$ AVEC $m \leq 2.2^{n^k}$

DONC AU TOTAL $O(2^{n^{k.k'}})$, D'OÙ $L \in EXP$. □

DEF : POUR UNE CLASSE DE COMPLEXITÉ $\mathcal{C}$, ON NOTE $co\mathcal{C} = \{ \underbrace{\Sigma^* \setminus A}_{{}^cA} \mid A \in \mathcal{C} \}$. ⚠ ON SUPPRIME LES ENTRÉES MAL FORMÉES.

THM : $P = coP$. (PREUVE ?) DONC $P \subseteq coNP$.

OUVERT : $NP = coNP$? $P = NP$?

THM : $P = NP \Rightarrow NP = coNP$. PREUVE : CAR $P = coP$. □

THM [2-BA] (CARACTÉRISATION UNIVERSELLE DE coNP) :

$A \in coNP$ SSI $\exists$ UN POLYNÔME $p(n)$ ET $B \in P$ T.Q. $x \in A \Leftrightarrow \forall y \in \{0,1\}^{p(|x|)} : (x,y) \in B$.

PREUVE : ${}^cA \in NP$ DONC $\exists\, p(n)$ ET $B' \in P$ T.Q. $x \in {}^cA \Leftrightarrow \exists y : (x,y) \in B'$.

DONC $x \in A \Leftrightarrow \forall y : (x,y) \notin B'$.

ON PREND $B = {}^cB' \in P$ CAR $P = coP$. □

♥ DEF [3-A] : UNE RÉDUCTION MANY-ONE POLYNOMIALE DE $A \subseteq \Sigma_A^*$ À $B \subseteq \Sigma_B^*$ EST UNE FONCTION $f : \Sigma_A^* \to \Sigma_B^*$ CALCULABLE EN TEMPS POLYNOMIAL (DÉTERMINISTE) TELLE QUE $\forall x \in \Sigma_A^* : x \in A \iff f(x) \in B$.

ON DIT ALORS QUE A SE RÉDUIT À B, QUE L'ON NOTE $A \leq_m^P B$.

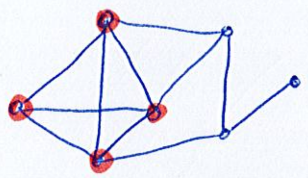
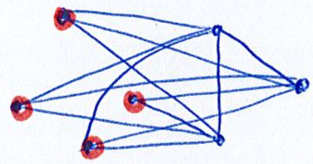
NB : IL EXISTE D'AUTRES TYPES DE RÉDUCTIONS ($\leq_T^P$, $\leq_{tt}^P$, $\leq_m^L$ ...).

EXEMPLE DE RÉDUCTION

CLIQUE
ENTRÉE : $G=(V,E)$ NON ORIENTÉ
$k \in \mathbb{N}$
QUESTION : G A-T-IL UNE CLIQUE DE TAILLE k ?

ENSEMBLE-INDÉPENDANT
ENTRÉE : $G=(V,E)$ NON ORIENTÉ
$k \in \mathbb{N}$
QUESTION : G A-T-IL UN ENSEMBLE INDÉPENDANT DE TAILLE k ?

$$\begin{matrix} G=(V,E) \\ k \end{matrix} \quad \overset{f}{\longmapsto} \quad \begin{matrix} G'=(V, V^2 \setminus E) \text{ SANS BOUCLES.} \\ k'=k \end{matrix}$$

G A UNE CLIQUE DE TAILLE k $\Leftrightarrow$ G' A UN ENS. IND. DE TAILLE k'

f EST CALCULABLE EN TEMPS POLYNOMIAL, DONC CLIQUE $\leqslant_m^P$ ENS. IND.

REMARQUE : ENS. IND $\leqslant_m^P$ CLIQUE AVEC LA MÊME RÉDUCTION, CE QUI EST EXCEPTIONNEL !

PROPRIÉTÉS DE $\leqslant_m^P$

LEMME [PERIFEL 3-G PAGE 66] : $\leqslant_m^P$ EST RÉFLEXIVE ET TRANSITIVE.

PREUVE : IDENTITÉ ET $g \circ f \leqslant_m^P$ (TEMPS : f EN $O(n^c)$ ET g EN $O(n^{c'})$ $\Rightarrow$ $g \circ f$ EN $O(n^c + n^{c.c'})$) $\square$

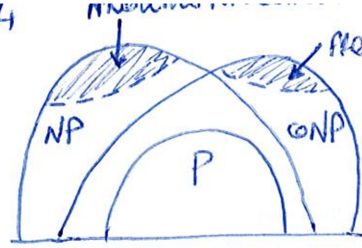
LEMME [PERIFEL 3-C PAGE 64] : P EST CLOSE POUR $\leqslant_m^P$ (SI $A \leqslant_m^P B$ ET $B \in P$ ALORS $A \in P$)
NP EST CLOSE POUR $\leqslant_m^P$ (SI $A \leqslant_m^P B$ ET $B \in NP$ ALORS $A \in NP$)

PREUVE : P : $M_A \circ f$ RÉSOUT A EN TEMPS POLYNOMIAL DÉTERMINISTE
NP : $M_A \circ f$ RÉSOUT A EN TEMPS POLYNOMIAL NON-DÉTERMINISTE $\square$

CORRESPOND À L'INTUITION DE "A PAS PLUS DIFFICILE QUE B"
$\Leftrightarrow$ "B AU MOINS AUSSI DIFFICILE QUE A".
(RÉSOLUTION EFFICACE (P) OU VÉRIFICATION EFFICACE (NP))

DÉF : SI $A \leqslant_m^P B$ ET $B \leqslant_m^P A$ ALORS $A \equiv_m^P B$ (C'EST UNE RELATION D'ÉQUIVALENCE : RÉFLEXIVE, TRANSITIVE, SYMÉTRIQUE).

NP-COMPLÉTUDE



DEF : POUR UNE CLASSE DE COMPLEXITÉ $\mathcal{C}$ ET UN PROBLÈME / LANGAGE L, ON DIT QUE :

- L EST $\mathcal{C}$-DIFFICILE SSI $\forall L' \in \mathcal{C} : L' \leq_m^p L$.
- L EST $\mathcal{C}$-COMPLET SSI $L \in \mathcal{C}$ ET L EST $\mathcal{C}$-DIFFICILE.

NB : C'EST TRÈS FORTE ! $\underbrace{\text{TOUS}}_{\forall L'}$ SE RAMÈNENT À $\underbrace{\text{UN}}_{L}$.

PROPOSITION [PERIFEL 3-L PAGE 68] : TOUT $L \in P$ NON TRIVIAL ($L \neq \emptyset$ ET $L \neq \Sigma^*$) EST P-DIFFICILE POUR $\leq_m^p$.

NB : CELA VEUT DIRE QUE $\leq_m^p$ NE SONT PAS ADAPTÉES POUR PARLER DES PB DIFFICILES POUR LA CLASSE P.

PREUVE : L NON TRIVIAL DONC $\exists a \in L$ ET $\exists b \notin L$.
$\forall L' \in P$, LA FONCTION $f(x) = \begin{cases} a & \text{si } x \in L' \\ b & \text{si } x \notin L' \end{cases}$ EST UNE RÉDUCTION POLYNOMIALE DE L' À L. □

PROPOSITION [PERIFEL 3-M PAGE 68] : $S = \{ (\underbrace{\langle N \rangle}_{\text{MTND}}, \underbrace{x}_{\text{ENTRÉE POUR } N}, \underbrace{1^t}_{t \text{ EN UNAIRE}}) \mid N(x) \text{ ACCEPTE EN TEMPS} \leq t \}$ EST NP-COMPLET.

PREUVE :
- $S \in NP$ AVEC UN ALGO QUI UTILISE UNE MTND UNIVERSELLE (TAILLE CONSTANTE, CF TP1.3) POUR SIMULER $N(x)$ POUR t ÉTAPES, ET ACCEPTER SSI $N(x)$ A ACCEPTÉ.
- POUR TOUT $L \in NP$, SOIT N_L UNE MTND QUI RECONNAÎT L EN TEMPS $p(n)$.
  $f(x) = (\langle N_L \rangle, x, 1^{p(|x|)})$ EST CALCULABLE EN TEMPS POLY, ET $x \in L \Leftrightarrow f(x) \in S$.
  DONC $L \leq_m^p S$. □

NB : CE PROBLÈME N'EST PAS TRÈS INTÉRESSANT (AU MOINS POUR VOUS). SAT BIENTÔT...

PROPOSITION [PERIFEL 3-P PAGE 69] : LES AFFIRMATIONS SUIVANTES SONT ÉQUIVALENTES :

1. $P = NP$,
2. TOUT PROBLÈME NP-COMPLET EST DANS P,
3. IL EXISTE UN PROBLÈME NP-COMPLET DANS P.

PREUVE : $1 \Rightarrow NP \subseteq P \Rightarrow 2$.
2 ET IL EXISTE S NP-COMPLET $\rightarrow 3$.
$3 \Leftrightarrow \exists Z : Z \in P$ ET Z EST NP-COMPLET $\Rightarrow \forall L \in NP : L \leq_m^p Z$ ET PAR CLÔTURE DE P POUR $\leq_m^p$, ON A $L \in P$. □

+++ PROPOSITION [PERIFEL 3-W PAGE 76]. SOIT C UN PROBLÈME NP-COMPLET ET $A \in NP$. SI $C \leq_m^p A$ ALORS A EST NP-COMPLET.

PREUVE : C NP-COMPLET $\Rightarrow \forall L \in NP : L \leq_m^p C \leq_m^p A$ ET $\leq_m^p$ TRANSITIVE. □

NB : LA NP-COMPLÉTUDE EST UN PATCH POUR PARLER DES PROBLÈMES "LES PLUS DIFFICILES DE LA CLASSE NP", DONT ON PENSE QU'ILS NE SONT PAS DANS P (MAIS PERSONNE NE SAIT PROUVER CELA ...).

- $\leqslant_m^P$, NP-COMPLÉTUDE, $S = \{(\langle N\rangle, x, 1^t) \mid N(x)$ ACCEPTE EN TEMPS $\leqslant t\}$ EST NP-COMPLET.
- SI C NP-COMPLET, $A \in NP$ ET $C \leqslant_m^P A$ ALORS A EST NP-COMPLET.

> **SAT**
> ENTRÉE : UNE FORMULE BOOLÉENNE φ. (PAS FORCÉMENT EN CNF)
> QUESTION : φ EST-ELLE SATISFAISABLE ?

THÉORÈME DE COOK (1971) - LEVIN (1973) [PERIFEL 3-V PAGE 72] : SAT EST NP-COMPLET.

$\longrightarrow$ AU PROCHAIN ÉPISODE

> **3-SAT**
> ENTRÉE : UNE FORMULE BOOLÉENNE φ EN 3-CNF $\rightarrow$ AU PLUS TROIS LITTÉRAUX PAR CLAUSE.
> QUESTION : φ EST-ELLE SATISFAISABLE ?

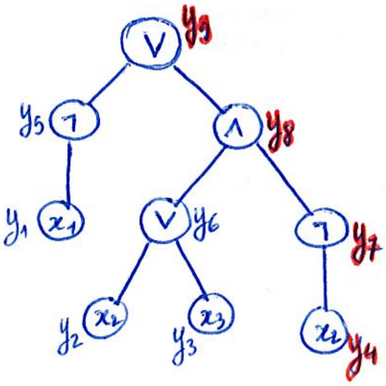
THÉORÈME [PERIFEL 3-Z PAGE 77]. 3SAT EST NP-COMPLET.

PREUVE : $\in NP$: TESTER SI φ EST EN 3-CNF, PUIS DEVINER (NON-DÉTERMINISTIQUEMENT) UNE VALUATION.

SAT $\leqslant_m^P$ 3-SAT : ÉTANT DONNÉE $\varphi(x_1, \dots, x_n)$, ON CONSTRUIT $\psi(x_1, \dots, x_n, y_1, \dots, y_m)$ TELLE QUE φ SATISFAISABLE $\Leftrightarrow$ ψ SATISFAISABLE.

IDÉE : VOIR φ COMME UN ARBRE,
AJOUTER UNE VARIABLE y_j POUR CHAQUE NOEUD DE CET ARBRE,
AJOUTER DES CLAUSES POUR FORCER LES y_j À ÊTRE COHÉRENTS AVEC LES x_i.
COMME LE DEGRÉ DES NOEUDS DE L'ARBRE EST AU PLUS 3, ON AURA ψ EN 3-CNF.

$\varphi(x_1, x_2, x_3) = (\neg x_1) \vee ((x_2 \vee x_3) \wedge (\neg x_2))$



- $y_4 \Leftrightarrow x_2 \equiv (y_4 \Rightarrow x_2) \wedge (x_2 \Rightarrow y_4) \equiv (\neg y_4 \vee x_2) \wedge (\neg x_2 \Rightarrow y_4)$
- $y_7 \Leftrightarrow \neg y_4 \equiv (y_7 \Rightarrow \neg y_4) \wedge (\neg y_4 \Rightarrow y_7) \equiv (\neg y_1 \vee \neg y_4) \wedge (y_4 \vee y_7)$
- $y_8 \Leftrightarrow (y_6 \wedge y_7) \equiv (y_8 \Rightarrow (y_6 \wedge y_7)) \wedge ((y_6 \wedge y_7) \Rightarrow y_8)$
$\equiv (\neg y_8 \vee (y_6 \wedge y_7)) \wedge (\neg(y_6 \wedge y_7) \vee y_8)$
$\equiv (\neg y_8 \vee y_6) \wedge (\neg y_8 \vee y_7) \wedge (\neg y_6 \vee \neg y_7 \vee y_8)$.
- $y_9 \Leftrightarrow (y_5 \vee y_8) \equiv (y_9 \Rightarrow (y_5 \vee y_8)) \wedge ((y_5 \vee y_8) \Rightarrow y_9)$
$\equiv (\neg y_9 \vee y_5 \vee y_8) \wedge (\neg(y_5 \vee y_8) \vee y_9)$
$\equiv (\neg y_9 \vee y_5 \vee y_8) \wedge (\neg y_5 \vee y_9) \wedge (\neg y_8 \vee y_9)$

POUR CHAQUE NOEUD $j \in \{1, \dots, m\}$ ON A C_j EN 3-CNF.

SOIT y_m LE NOEUD À LA RACINE, ON CONSTRUIT $\psi(x_1, \dots, x_n, y_1, \dots, y_m) = y_m \wedge \bigwedge_{j=1}^{m} C_j$.

ON A : φ SATISFAISABLE $\iff$ ψ SATISFAISABLE.

LA TRANSFORMATION DE φ À ψ EST CALCULABLE EN TEMPS POLYNOMIAL (DÉTERMINISTE).

DONC SAT $\leq_m^P$ 3-SAT. PUISQUE SAT EST NP-DIFFICILE, 3-SAT EST NP-DIFFICILE. □

⚠ 2-SAT SE RÉSOUT EN TEMPS POLYNOMIAL (VU EN TD).

REMARQUE: 3-SAT EST TRÈS PRATIQUE POUR RÉDUIRE 3-SAT $\leq$ L.

REMARQUE : PLEIN D'AUTRES VARIANTES DE SAT SONT NP-COMPLÈTES : 1-IN-3-SAT, HALF-SAT ($=\frac{1}{2}$ DES CLAUSES) ... THÉORÈME DE DICHOTOMIE DE SCHAEFER.

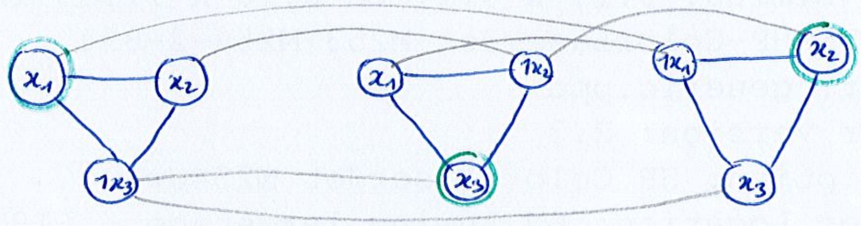
> **ENSEMBLE INDÉPENDANT**
>
> ENTRÉE : UN GRAPHE $G = (V, E)$ NON ORIENTÉ,
> UN ENTIER $k \in \mathbb{N}$.
>
> QUESTION : G A-T-IL UN ENSEMBLE INDÉPENDANT DE TAILLE k ?

THÉORÈME [PERIFEL 3-AE PAGE 80] : ENSEMBLE INDÉPENDANT EST NP-COMPLET.

PREUVE : $\in$NP : DEVINER UN SOUS-ENSEMBLE DE k SOMMETS ET VÉRIFIER.

3-SAT $\leq_m^P$ E.I. : $\varphi \longmapsto (G, k)$.

$\varphi = (x_1 \vee x_2 \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3)$



ON CONSTRUIT UN TRIANGLE PAR CLAUSE,
ET ON AJOUTE TOUS LES ARCS ENTRE x_i ET $\neg x_i$.
ON CHOISIT $k = m$ LE NOMBRE DE CLAUSES DE φ.

TEMPS POLY ($3m$ SOMMETS ET $< 3m + 3m(m-1)$ ARRÊTES).

$\varphi \in$ 3-SAT $\Rightarrow$ SOIT UN MODÈLE, IL SATISFAIT (AU MOINS) UN LITTÉRAL PAR CLAUSE ; CE QUI DONNE UN ENSEMBLE DE $m = k$ SOMMETS DANS DES TRIANGLES DIFFÉRENTS ET SANS AVOIR CHOISI x_i ET $\neg x_i$ $\Rightarrow (G, k) \in$ E.I.

$(G, k) \in$ E.I. $\Rightarrow$ PUISQUE $k = m$ DANS L'E.I. ON A UN LITTÉRAL PAR CLAUSE (TRIANGLE) ET SANS AVOIR CHOISI x_i ET $\neg x_i$, CE QUI DONNE UN MODÈLE DE φ $\Rightarrow \varphi \in$ 3-SAT.

DONC 3-SAT $\leqslant_m^P$ E.I. PUISQUE 3-SAT EST NP-DIFFICILE, E.I. EST NP-DIFFICILE. $\square$

<u>COROLLAIRE</u> : CLIQUE EST NP-COMPLET.

<u>PREUVE</u> : E.I. NP-COMPLET, E.I. $\leqslant_m^P$ CLIQUE, ET CLIQUE ∈ NP. $\square$

REMARQUE : SI k EST FIXÉ (PLUTÔT QUE DONNÉ EN ENTRÉE) ALORS TEMPS POLY $O(n^k)$.

SUPER PLOMBIERS ITALIENS ⇐

THÉORÈME DE LADNER (1975) [PERIFEL 3-AK] : Si $P \neq NP$ alors il existe $A \in NP$ tel que :
- $A \notin P$, et
- A n'est pas NP-complet.

"NP-intermédiaires". Candidats :
- isomorphisme de graphes.
- factorisation : entrées : n, i en binaire.
  question : est-ce que n a un $1 < \text{facteur} \leq i$?

$\in NP$: deviner le facteur et diviser.

$\in coNP$: deviner la décomposition en facteurs premiers + AKS (2002)

donc $\in NP \cap coNP$ ... $\in P$??

Remarque : KARP's 21 problems (1972) = ce cours, en 19 pages.

①. Théorème de dichotomie de Schaefer

②. Super plombier italien est NP-difficile.

③. Problèmes complets pour PH, PSPACE, NEXP, P.

$\exists SAT = SAT$, $\exists\forall SAT$, $\exists\forall\exists SAT$; QSAT ; SUCCINCT-SAT ; SAT-EVAL $\leq_m^L$

④. Un algo poly pour SAT si $P = NP$.

⑤. Complexité de comptage : #P, réductions parcimonieuses.

⑥. Problèmes faiblement et fortement NP-complets.

THÉORÈME DE COOK-LEVIN [PERIFEL 3-V] : SAT EST NP-COMPLET.
1971 1973 (PAS EN CNF).

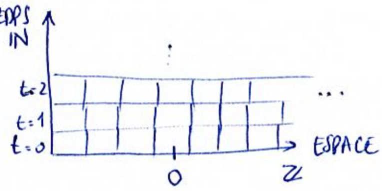
PROOF : SAT $\in$ NP ... SAT EST NP-DIFFICILE : SOIT $L \in$ NP. $\exists$ MTND N EN TEMPS $p(n)$ POLY.

MONTRONS $L \leq$ SAT.

SOIT $x \in \Sigma^*$ UNE INSTANCE DU PROBLÈME L. ON CONSTRUIT φ_x SATISFAISABLE $\Leftrightarrow$ N ACCEPTE $x \Leftrightarrow x \in L$.

DIAGRAMME ESPACE-TEMPS DE $N(x)$ DE TAILLE POLY :

- TEMPS : $t(|x|)+1$
- ESPACE : $2t(|x|)+1$



VARIABLES (k RUBANS) :

- $c^{r}_{\gamma,i,j}$ VRAI SSI CASE i AU TEMPS j DU RUBAN r CONTIENT LE SYMBOLE γ.
- $p^{r}_{i,j}$ VRAI SSI TÊTE DU RUBAN r EN POSITION i AU TEMPS j.
- $e_{q,j}$ VRAI SSI ÉTAT q AU TEMPS j.

QUANTITÉ POLY...

FORMULE φ_x : COHÉRENCE ET DÉBUT ET TRANSITION ET ACCEPTE.

- COHÉRENCE :
  - PARTOUT UN SYMBOLE : $\bigwedge_{r,i,j} \bigvee_{\gamma} \left(c^{r}_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c^{r}_{\gamma',i,j}\right)$
  - TOUJOURS UNE TÊTE : $\bigwedge_{r,j} \bigvee_{i} \left(p^{r}_{i,j} \wedge \bigwedge_{i' \neq i} \neg p^{r}_{i',j}\right)$
  - TOUJOURS UN ÉTAT : $\bigwedge_{j} \bigvee_{q} \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j}\right)$.
- DÉBUT :
  - ÉTAT INITIAL q_0 : $e_{q_0,0}$.
  - RUBANS $r>1$ VIDES : $\bigwedge_{r>1,i} c^{r}_{B,i,0}$
  - x SUR RUBAN LECTURE : SOIT $n=|x|$. $\left(\bigwedge_{0\leq i<n} c^{1}_{x_i,i,0}\right) \wedge \left(\bigwedge_{i<0 \vee i\geq n} c^{1}_{B,i,0}\right)$.
  - TÊTES POSITION 0 : $\bigwedge_{r} p^{r}_{0,0}$ ON ABUSE DE LA NOTATION

SIMPLIFICATION : ARRÊT $\Rightarrow$ RESTER DANS L'ÉTAT : $\forall \gamma \in \Gamma^{k-1}$, $\delta(q_A,\gamma) = \{(q_A, B^{k-1}, \circ^{k})\}$ ET $\delta(q_R,\gamma)=\{(q_R,B^{k-1},\circ^{k})\}$.

- ACCEPTE : $e_{q_A,t(|x|)}$
- TRANSITION :

$$\bigwedge_{j,q,\bar{i},\bar{\gamma}} \left(\left[e_{q,j} \wedge \bigwedge_{r} \left(p^{r}_{\bar{i}_r,j} \wedge c^{r}_{\bar{\gamma}_r,\bar{i}_r,j}\right)\right] \Rightarrow \bigvee_{(q',\bar{\gamma}',\bar{d}') \in \delta(q,\bar{\gamma})} \left[e_{q',j+1} \wedge \bigwedge_{r} \left(c^{r}_{\bar{\gamma}'_r,\bar{i}_r,j+1} \wedge p^{r}_{\bar{i}_r+\bar{d}'_r,j+1} \right) \right] \right).$$

$\Rightarrow$ ET SI PAS LA TÊTE ALORS RUBAN INCHANGÉ

IL Y A UNE BIJECTION ENTRE LES MODÈLES DE φ_x ET LES CHEMINS ACCEPTANT DANS $N(x)$. $\square$