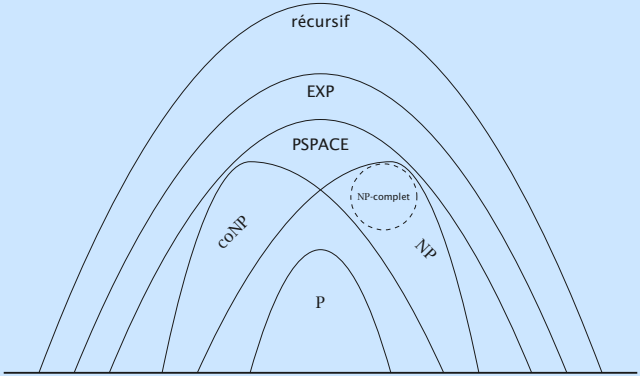
Calculabilité & Complexité

Complexité (4/4) : théorème de Cook-Levin

Nicolas Ollinger (LIFO, Université d'Orléans)

M1 info, Université d'Orléans — S2 2024/2025



1. Dans l'épisode précédent...

Réductions many-one polynomiales

En complexité, on s'intéresse à des réductions qui préservent la complexité des problèmes.

Définition Soient $A \subseteq \Sigma^*$ et $B \subseteq \Gamma^*$ deux langages. Une **réduction** (many-one) **polynomiale** de A à B est une fonction totale **calculable en temps polynomial** $f : \Sigma^* \to \Gamma^*$ telle que

$$u \in A \Leftrightarrow f(u) \in B \qquad \forall u \in \Sigma^* \quad .$$

Le langage A **se réduit en temps polynomial** au langage B, noté $A \leqslant_m^P B$ s'il existe une réduction polynomiale de A à B.

Proposition La relation $\leqslant_m^P$ est une relation de **pré-ordre**.

Complétude

Proposition Les classe P, NP, EXP et NEXP sont **stables** par réductions polynomiales.

Définition Deux languages A et B sont **équivalents pour les réductions polynomiales**, noté $A \equiv_m^P B$, si $A \leqslant_m^P B$ et $B \leqslant_m^P A$.

Définition Un langage A est C**-difficile** pour une classe de complexité C si pour tout $B \in C$ on a $B \leqslant_m^P A$.

Définition Un langage A est C**-complet** pour une classe de complexité C si A est C-difficile et $A \in C$.

Exemple

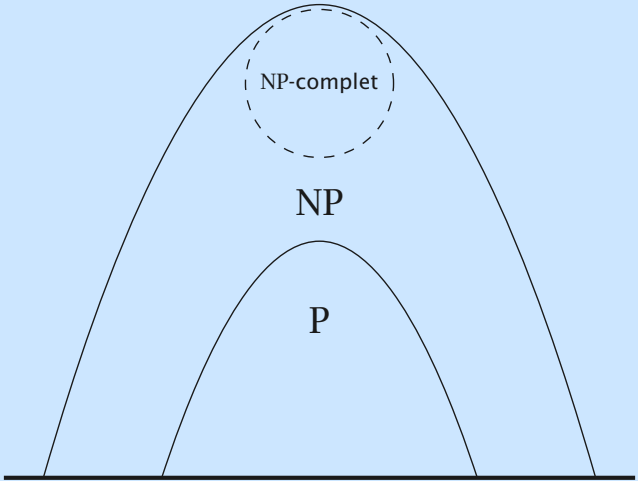
CLIQUE

entrée : *un graphe non orienté G et un entier k*
question : *le graphe G contient-il une clique de taille k ?*

ENSEMBLE INDÉPENDANT

entrée : *un graphe non orienté G et un entier k*
question : *G contient-il un ensemble indépendant de taille k ?*

CLIQUE $\equiv_m^P$ ENSEMBLE INDÉPENDANT



2. NP-complétude

Premier contact

Proposition Tout problème **non trivial** (ni vide ni plein) est **P-difficile** pour les réductions en temps polynomial.

$$\text{ADHOC} = \left\{ \left\langle \mathcal{N}, x, 1^t \right\rangle \,\middle|\, \text{la MTND } \mathcal{N} \text{ accepte } x \text{ en temps } \leqslant t \right\}$$

Proposition ADHOC est **NP-complet**.

Existence

Proposition Les affirmations suivantes sont équivalentes :

1. $\mathrm{P} = \mathrm{NP}$;
2. tout problème NP-complet est dans P ;
3. il existe un problème NP-complet dans P.

Il nous faut identifier des problèmes NP-complets **naturels** !

Lemme Si $A \leqslant_m^P B$ avec A un problème NP-complet et $B \in \mathrm{NP}$ alors B est NP-complet.

Formules booléennes

Définition L'ensembles des **formules booléennes** à n variables $x_1, \ldots, x_n$ est défini **inductivement** par :

$$\begin{aligned} \varphi(x_1,\ldots,x_n) \quad ::= \quad & x_i \\ \mid \quad & \neg\varphi(x_1,\ldots,x_n) \\ \mid \quad & \varphi_1(x_1,\ldots,x_n) \vee \varphi_2(x_1,\ldots,x_n) \\ \mid \quad & \varphi_1(x_1,\ldots,x_n) \wedge \varphi_2(x_1,\ldots,x_n) \end{aligned}$$

Définition La **valeur de vérité** $\varphi(a_1,\ldots,a_n)$ d'une formule est définie inductivement pour toute **assignation** $a_1,\ldots,a_n \in \{0,1\}$:

$$\begin{aligned} x_i(a_1,\ldots,a_n) &= a_i \\ (\neg\varphi)(a_1,\ldots,a_n) &= 1 - \varphi(a_1,\ldots,a_n) \\ (\varphi_1 \vee \varphi_2)(a_1,\ldots,a_n) &= \max_i(\varphi_i(a_1,\ldots,a_n)) \\ (\varphi_1 \wedge \varphi_2)(a_1,\ldots,a_n) &= \prod_i(\varphi_i(a_1,\ldots,a_n)) \end{aligned}$$

Sucre syntaxique

Remarque Par abus de langage on confondra allégrement 0, F et FAUX d'une part ; 1, V et VRAI d'autre part.

Quelques abbréviations utiles :

$$
\begin{aligned}
1 &\equiv x_1 \vee \neg x_1 \\
0 &\equiv x_1 \wedge \neg x_1 \\
\varphi \to \psi &\equiv \neg\varphi \vee \psi \\
\varphi \leftrightarrow \psi &\equiv (\varphi \to \psi) \wedge (\psi \to \varphi) \\
x_i = x_j &\equiv x_i \leftrightarrow x_j
\end{aligned}
$$

Évaluation de formules

Proposition Étant données une formule φ et une assignation $a_1, \ldots, a_n$, on peut décider en **temps polynomial** si celle-ci **satisfait** la formule, *i.e.* si $\varphi(a_1, \ldots, a_n) = 1$.

Définition Une formule est **satisfaisable** s'il existe une assignation qui la **satisfait**.

SAT

entrée : *une formule booléenne* $\varphi(x_1, \ldots, x_n)$
question : φ *est-elle satisfaisable ?*

Théorème de Cook-Levin

Théorème[Cook 71, Levin 73] Le problème SAT est NP-**complet**.

SAT

entrée : *une formule booléenne* $\varphi(x_1, \ldots, x_n)$
question : φ *est-elle satisfaisable ?*

Idée Associer à toute instance x d'un problème de NP une **formule booléenne** calculable en temps polynomial et dont les assignations qui la satisfont codent les chemins de calcul acceptants.

De SAT à 3SAT

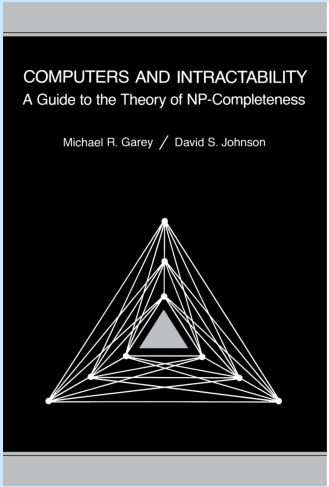
Définition Formules booléennes en **forme normale conjonctive** :

- un **littéral** l est une variable x_i ou sa négation $\neg x_i$ (ou $\overline{x_i}$) ;
- une **clause** C est une disjonction de littéraux $C = \bigvee_i l_i$;
- une **formule en CNF** est une conjonction de clauses $\varphi = \bigwedge_i C_i$;
- une **formule k-CNF** est une formule en CNF avec au plus k littéraux par clause.

3SAT

entrée : *une formule* 3*-CNF* $\varphi(x_1, \ldots, x_n)$
question : φ *est-elle satisfaisable ?*

Théorème Le problème 3SAT est NP-**complet**.



3. NP-complétude partout !

CIRCUIT-SAT

Proposition CIRCUIT-SAT est NP-complet.

CIRCUIT-SAT

entrée : *un circuit booléen* G
question : G *est-il satisfaisable ?*

Un circuit booléen est un DAG dont les sources portent les entrées du circuit et dont les autres sommets sont étiquetés par des fonctions booléennes (ET, OU, NON). Un puits est identifié comme sortie du circuit et le circuit est évalué des sources vers le puits.

SOMME PARTIELLE

Proposition SOMME PARTIELLE est NP-complet.

SOMME PARTIELLE

entrée : *une liste d'entiers* $a_1, \ldots, a_m$ *et un entier cible* s
question : *existe-t-il une sous-liste dont la somme vaut* s*, c'est-à-dire* $S \subseteq \{1, \ldots, m\}$ *telle que* $\sum_{i \in S} a_i = s$ *?*

Idée Montrer que 3SAT $\leqslant_m^P$ SOMME PARTIELLE.

CLIQUE

Proposition CLIQUE est NP-complet.

CLIQUE

entrée : *un graphe non orienté G et un entier k*
question : *le graphe G contient-il une clique de taille k ?*

ENSEMBLE INDÉPENDANT

entrée : *un graphe non orienté G et un entier k*
question : *G contient-il un ensemble indépendant de taille k ?*

Idée Montrer que 3SAT $\leqslant_m^P$ ENSEMBLE INDÉPENDANT.

Théorème de Ladner

Théorème Si $\mathrm{P} \neq \mathrm{NP}$ alors il existe un problème $A \in \mathrm{NP}$ tel que :

- $A \notin \mathrm{P}$;
- A n'est pas NP-complet.