Hiérarchie polynomiale.

Définition 1. Étant donnée une classe de langages $\mathscr{C}$, on définit

$$\mathsf{co}\mathscr{C} := \{\, A \subseteq \Sigma^\star \mid \Sigma^\star \setminus A \in \mathscr{C} \,\}.$$

Définition 2. Les classes Σ_i^{P}, pour $i \geq 0$, sont définies par induction :

- ▷ $\Sigma_0^{\mathrm{P}} := \mathsf{P}$;
- ▷ $\Sigma_{i+1}^{\mathrm{P}} := \mathsf{NP}^{\Sigma_i^{\mathrm{P}}}$.

On pose $\mathsf{PH} := \bigcup_{i \geq 0} \Sigma_i^{\mathrm{P}}$.

On définit aussi $\Pi_i^{\mathrm{P}} = \mathsf{co}\Sigma_i^{\mathrm{P}}$ et $\Delta_i^{\mathrm{P}} := \mathsf{P}^{\Sigma_{i-1}^{\mathrm{P}}}$.

Exemple 1. On a

- ▷ $\Sigma_1^{\mathrm{P}} = \mathsf{NP}^{\mathsf{P}} = \mathsf{NP}$,
- ▷ $\Pi_1^{\mathrm{P}} = \mathsf{coNP}$,
- ▷ $\Delta_2^{\mathrm{P}} = \mathsf{P}^{\mathsf{NP}}$,
- ▷ $\Sigma_2^{\mathrm{P}} = \mathsf{NP}^{\mathsf{NP}}$,
- ▷ *etc.*

En général, on a les inclusions suivantes :

$$\begin{tikzcd}[column sep=small]
 & \Sigma_1^{\mathrm{P}} = \mathsf{NP} \arrow[dr, phantom, sloped, "\subseteq"] & & \Sigma_2^{\mathrm{P}} \arrow[dr, phantom, sloped, "\subseteq"] & & \Sigma_3^{\mathrm{P}} \arrow[dr, phantom, sloped, "\subseteq"] & & & \\
\mathsf{P} \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \Delta_2^{\mathrm{P}} \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \Delta_3^{\mathrm{P}} \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \cdots & \subseteq & \mathsf{PSPACE}. \\
 & \Pi_1^{\mathrm{P}} = \mathsf{NP} \arrow[ur, phantom, sloped, "\subseteq"] & & \Pi_2^{\mathrm{P}} \arrow[ur, phantom, sloped, "\subseteq"] & & \Pi_3^{\mathrm{P}} \arrow[ur, phantom, sloped, "\subseteq"] & & &
\end{tikzcd}$$

Remarque 1. On a que $\Delta_i^{\mathrm{P}} = \mathsf{P}^{\Sigma_{i-1}^{\mathrm{P}}} = \mathsf{P}^{\Pi_{i-1}^{\mathrm{P}}}$. Par exemple, on a que $\Delta_2^{\mathrm{P}} = \mathsf{P}^{\mathsf{NP}} = \mathsf{P}^{\mathsf{coNP}}$.

Les classes Δ_i^{P} sont closes par complément. Par exemple, $\Delta_2^{\mathrm{P}} \subseteq \Pi_2^{\mathrm{P}}$ découle de la clôture par complément et de $\Delta_2^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$.

On omet parfois l'exposant P (mais attention, il existe une hiérarchie Σ_i en calculabilité).

Proposition 1. On a $\mathsf{PH} \subseteq \mathsf{PSPACE}$.

Preuve. On montre par récurrence sur i que $\Sigma_i^{\mathrm{P}} \subseteq \mathsf{PSPACE}$.

- ▷ On a $\Sigma_0^{\mathrm{P}} = \mathsf{P} \subseteq \mathsf{PSPACE}$.
- ▷ Supposons $\Sigma_{i-1}^{\mathrm{P}} \subseteq \mathsf{PSPACE}$. On a

$$\Sigma_i^{\mathrm{P}} = \mathsf{NP}^{\Sigma_{i-1}^{\mathrm{P}}} \subseteq \mathsf{NP}^{\mathsf{PSPACE}} = \mathsf{PSPACE},$$

car $\mathsf{NP}^{\mathrm{QBF}} = \mathsf{PSPACE}$.

□

Proposition 2. Si $\mathsf{P} = \mathsf{NP}$ alors $\mathsf{PH} = \mathsf{P}$.

Plus généralement, pour tout $i \geq 0$, si

$$\Sigma_i^{\mathrm{P}} = \Sigma_{i+1}^{\mathrm{P}},$$

alors $\mathsf{PH} = \Sigma_i^{\mathrm{P}}$. On dit alors que « *la hiérarchie polynomiale s'effondre au i-ème niveau* ».

Preuve. Supposons $\Sigma_i^{\mathrm{P}} = \Sigma_{i+1}^{\mathrm{P}}$.

On montre par récurrence que $\Sigma_j^{\mathrm{P}} = \Sigma_i^{\mathrm{P}}$ pour tout $j \geq i+1$. L'initialisation est vraie par hypothèse. L'étape de récurrence est : supposons $\Sigma_{j-1}^{\mathrm{P}} = \Sigma_i^{\mathrm{P}}$ alors

$$\Sigma_j^{\mathrm{P}} = \mathsf{NP}^{\Sigma_{j-1}^{\mathrm{P}}} = \mathsf{NP}^{\Sigma_i^{\mathrm{P}}} = \Sigma_{i+1}^{\mathrm{P}} = \Sigma_i^{\mathrm{P}}.$$

□

1 Caractérisation par quantificateurs.

Théorème 1. Un langage A est dans Σ_i^{P} si, et seulement si, il existe $B \in \mathsf{P}$ et un polynôme p tel que, pour tout $x \in \{\mathtt{0},\mathtt{1}\}^\star$,

$$x \in A \iff \begin{pmatrix} \exists y_1 \in \{\mathtt{0},\mathtt{1}\}^{p(n)} \\ \forall y_2 \in \{\mathtt{0},\mathtt{1}\}^{p(n)} \\ \exists y_3 \in \{\mathtt{0},\mathtt{1}\}^{p(n)} \\ \vdots \\ \mathsf{Q}_i y_i \in \{\mathtt{0},\mathtt{1}\}^{p(n)} \\ \langle x, y_1, y_2, \ldots, y_i \rangle \in B \end{pmatrix}.$$

□

Remarque 2.

1. Cette caractérisation est similaire (c'est une généralisation) à la caractérisation de NP avec des certificats.
2. On peut quantifier sur des blocs de taille variables (des chaînes de tailles $p_1(n), p_2(n), \ldots, p_i(n)$). On peut aussi enchaîner plusieurs blocs existentiels sans augmenter le i (il suffit de concaténer les chaînes).
3. On pourrait aussi quantifier sur $y_k \in \{\mathtt{0},\mathtt{1}\}^{\leq p(n)}$.

4. On a une caractérisation similaire pour la classe Π_i^{P} où on commence par « $\forall y_1 \in \{\mathtt{0}, \mathtt{1}\}^{p(n)}$ ».

Proposition 3. Si $\Sigma_i^{\mathrm{P}} = \Pi_i^{\mathrm{P}}$ alors on a que $\Sigma_i^{\mathrm{P}} = \mathsf{PH}$.

Preuve. Montrons $\Sigma_i^{\mathrm{P}} = \Sigma_{i+1}^{\mathrm{P}}$. Soit $A \in \Sigma_{i+1}^{\mathrm{P}}$. On a

$$x \in A \iff \exists y_1\, \forall y_2 \ldots \mathsf{Q}_{i+1} y_{i+1} \langle x, y_1, \ldots, y_{i+1} \in B \rangle,$$

avec $B \in \mathsf{P}$. Et, le langage

$$\{\, \langle x, y_1 \rangle \mid \forall y_2 \ldots \mathsf{Q}_{i+1} y_{i+1} \langle x, y_1, \ldots, y_{i+1} \in B \rangle \,\}$$

est dans Π_i^{P}, donc dans Σ_i^{P}. D'où, par caractérisation,

$$x \in A \iff \exists y_1\, \exists z_1\, \forall z_2\, \ldots\, \mathsf{Q}_i z_i\, \langle x, y_1, z_1, \ldots, z_i \rangle \in C,$$

et ainsi A est un problème de Σ_i^{P} avec la remarque précédente. □

Remarque 3 (Propriétés supplémentaires).

1. La classe Σ_i^{P} est *close par réduction polynomiale*, c'est-à-dire si $B \in \Sigma_i^{\mathrm{P}}$ et $A \le_{\mathrm{P}} B$ alors $A \in \Sigma_i^{\mathrm{P}}$.
2. Le problème de décision QBF-Σ_i^{P} est Σ_i^{P}-complet, où

QBF-Σ_i^{P}

Entrée. Une formule booléenne quantifiée F avec i quantificateurs et commençant par un bloc existentiel
Sortie. Est-ce que F est vraie ?

3. De même, le problème de décision QBF-Π_i^{P} est Π_i^{P}-complet, où

QBF-Π_i^{P}

Entrée. Une formule booléenne quantifiée F avec i quantificateurs et commençant par un bloc universel
Sortie. Est-ce que F est vraie ?

2 Théorème de Karp-Lipton.

Théorème 2 (Karp-Lipton). Si $\mathsf{NP} \subseteq \mathsf{P/poly}$, alors $\Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$.

Définition 3. Un circuit booléen à s entrées décide SAT si, étant donnée une formule booléenne F de taille s, le circuit C décide si F est satisfiable.

La preuve de ce théorème repose sur deux lemmes.

Lemme 1. L'ensemble des (codages de) circuits qui décident SAT est dans coNP.

Preuve. On utilise le fait que SAT est auto-réductible[1] : une formule booléenne $F(v_1, \ldots, v_n)$ est satisfiable si et seulement si l'une des deux formules booléennes

$$F(v_1, \ldots, v_{n-1}, \mathtt{0}) \quad \text{ou} \quad F(v_1, \ldots, v_{n-1}, \mathtt{1})$$

est satisfiable.

Un circuit C décide SAT ssi pour toute formule F de taille s

1. si F n'a pas de variable, alors $C(F) = \mathtt{1}$ ssi $F \equiv \mathtt{1}$;
2. si F dépend de $n \geq 1$ variables $v_1, \ldots, v_n$ alors $C(F) = \mathtt{1}$ ssi
$$C(F[v_n := \mathtt{0}]) = \mathtt{1} \text{ ou } C(F[v_n := \mathtt{1}]) = \mathtt{1}.$$

Étant donnée F, les conditions ci-dessous peuvent être vérifiées en temps polynomial (car VALCIRC est dans P).

Cette caractérisation commence par un « pour toute formule » et on considère ensuite un problème dans P, d'où le langage est bien dans coNP. □

1. *self-reductible* en anglais.

Lemme 2. Si $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly}$, alors SAT peut être décidé par une famille de circuits booléens de taille polynomiale. □

Preuve (du théorème de Karp-Lipton). On suppose avoir l'inclusion des classes $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly}$. Il suffit de montrer que $\Pi_2^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$. En effet, avec ça on a que

$$\Sigma_2^{\mathrm{P}} = \mathsf{co}\Pi_2^{\mathrm{P}} \subseteq \mathsf{co}\Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}.$$

Il suffit de montrer que le problème de décision QBF-Π_2^{P} est dans Σ_2^{P}. Soit F une formule booléen de taille s, alors

$$\forall u\, \exists v\, F(u, v),$$

est équivalente à

$$\exists C\, \forall u\, C(F(u, \cdot)) = \mathtt{1} \quad \text{et } C \text{ décide } \textsc{Sat},$$

où C est un circuit booléen avec s entrées. Il suffit de quantifier sur des circuits de taille polynomiale d'après le lemme 2. Ceci est équivalent à

$$\exists C\, \forall u\, C(F(u, \cdot)) = \mathtt{1} \text{ et } \forall y \in \{\mathtt{0}, \mathtt{1}\}^{p(s)}\, \langle C, y\rangle \in A,$$

avec $A \in \mathsf{P}$ d'après le lemme 1. On en déduit que ceci est équivalent à

$$\exists C\, \forall u\, \forall y\, C(F(u, \cdot)) = \mathtt{1} \text{ et } \langle C, y\rangle \in A,$$

qui est vérifiable en temps polynomial, donc dans Σ_2^{P} grâce à la caractérisation par quantificateurs. □