Chapitre 4.

Calculabilité, Décidabilité, et Complexité

I. Problèmes de décision

Un problème de *décision* Q est un problème dont la sortie est **V** ou **F**.
On le décrit sous la forme :

$$Q : \left| \begin{array}{ll} \textbf{Entrée.} & \text{Quelque chose} \\ \textbf{Sortie.} & \text{Est-ce que ... ?} \end{array} \right.$$

Un problème est différent selon "l'encodage" des entrées.

II. Problèmes décidables

Un problème Q est *décidable* dès lors qu'il existe une machine $\mathscr{M}$ qui dit si une instance est positive ***et*** si une instance est négative :

$$x \in Q^+ \iff x \xrightarrow[\mathscr{M}]{} \textbf{V} \qquad \textit{et} \qquad x \in Q^- \iff x \xrightarrow[\mathscr{M}]{} \textbf{F}.$$

Ainsi, la machine n'aura pas de boucles infinies (ou d'erreurs) sur une entrée du problème Q.

Un langage L est *décidable* si $\textsc{Appartient}_L$ l'est.

La classe des langages décidables est stable par complémentaire, intersection, union, concaténation, et étoile de Kleene.

Les langages finis, réguliers (et non-contextuels) sont décidables.

vu plus tard dans l'année...

III. Sérialisations

Une fonction `f : t -> string` est une *sérialisation* (calculable) de `t` si :

- `f` est injective,
- `(f e)` est bien parenthésée, pour tout `e : t`,
- on peut coder `g : string -> t` telle que `g (f e) = e`.
  (*i.e.* inversible sur Im(`f`))

Une machine $\mathscr{M}$ est sérialisable en $\langle\mathscr{M}\rangle$, c'est déjà une chaîne de caractères.

IV. Fonction calculable

Une fonction $f : \mathscr{E} \overset{\text{fonction partielle}}{\rightharpoonup} \mathscr{S}$ est *calculée* par $\mathscr{M}$ si

$$\forall e \in \text{def}(f), \quad e \xrightarrow[\mathscr{M}]{} f(e)$$

Comportement spécifié *uniquement* sur $\text{def}(f)$, pas sur les autres valeurs de e

V. Machine universelle

Ensemble des sérialisations des programmes OCaml

On définit `interprète` : $\mathscr{O} \times \Sigma^* \rightharpoonup \Sigma^*$ par :

$$\texttt{interprète}(\langle \mathscr{M} \rangle, w) = w' \iff w \xrightarrow[\mathscr{M}]{} w'$$

La fonction interprète est *calculable* par une *machine universelle* $\mathscr{U}$.

VI. Théorème de l'Arrêt

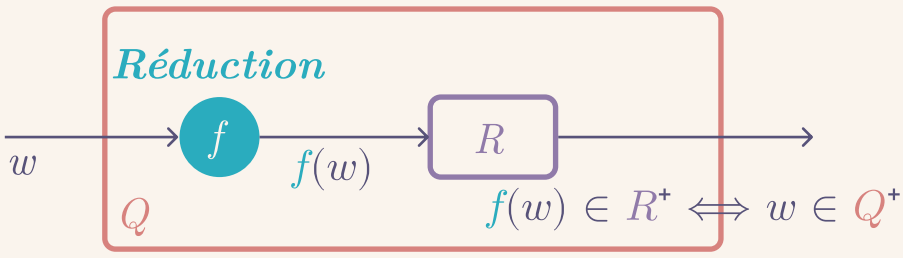
Il existe des problèmes indécidables,
le problème de l'Arrêt en est un exemple.

ARRÊT : **Entrée.** Une machine $\mathscr{M}$ et un mot w
Sortie. Est-ce que $\mathscr{M}$ s'arrête sur w ?

VII. Indécidabilité par réduction

On dit que Q *se réduit à* R, que l'on note $Q \preccurlyeq R$, dès lors qu'il existe $f : \mathscr{E}_Q \to \mathscr{E}_R$ calculable telle que :

$$f(w) \in R^+ \iff w \in Q^+$$



Si $Q \preccurlyeq R$ et que R est décidable, alors Q aussi.
Si $Q \preccurlyeq R$ et que Q est indécidable, alors R aussi.

VIII. Classe P

On nomme **P** la classe des problèmes décidables en temps polynomial.
Cette classe est stable par union, intersection et complémentaire.

On pourra dire qu'une fonction est *calculable en temps polynomial.*
L'ensemble des fonctions calculables en temps polynomial est stable par composition et opérations simples (addition, multiplication, ...).

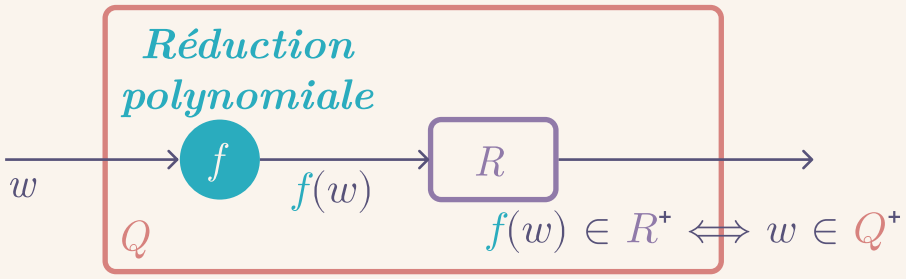
IX. Classe **NP** et **NP**-difficulté

On nomme **NP** la classe des problèmes *vérifiables* en temps polynomial.
Un problème Q est **NP**-*difficile* si tout problème de **NP** se réduit en temps polynomial à Q.
Un problème est **NP**-*complet* s'il est dans la classe des problèmes **NP** et qu'il est **NP**-difficile.

X. Réduction en temps polynomial

On dit que Q *se réduit en temps polynomial au problème* R, que l'on note $Q \preccurlyeq_{\mathrm{p}} R$, dès lors qu'il existe $f : \mathscr{E}_Q \to \mathscr{E}_R$ calculable *en temps polynomial* telle que :

$$f(w) \in R^+ \iff w \in Q^+$$



Si $Q \preccurlyeq_{\mathrm{p}} R$ et que $R \in \mathbf{P}$, alors $Q \in \mathbf{P}$.
Si $Q \preccurlyeq_{\mathrm{p}} R$ et que Q est **NP**-difficile, alors R aussi.

Le problème SAT est **NP**-complet. (admis)
Le problème n-CNF-SAT est **NP**-complet, pour $n \geq 3$. (par réduction)