914 Décidabilité et indécidabilité. Exemples.

Objectif : déterminer les problèmes que l'on peut résoudre par un algorithme

I. Des problèmes aux machines de Turing

Déf. 1 : un problème de décision est la donnée d'un ensemble E de ses instances et d'un sous-ensemble $P \subseteq E$ de ses instances positives (pour lesquelles la réponse est "oui")

Ex 1 "Être premier" :
$E = \mathbb{N}$ l'ensemble des entiers
$P =$ l'ensemble des nombres premiers

Déf. 2 : soit $P \subseteq E$ un problème, Σ un alphabet. On appelle codage une fonction injective $f : E \to \Sigma^*$.
Pour $x \in E$ on note $\langle x \rangle = f(x)$.
Le langage associé au problème P est :
$$L_P = \{\langle x \rangle / x \in P\}$$

Ex. 2 : $f : \begin{cases} \mathbb{N} \to \{0,1\}^* \\ x \mapsto a_1 \ldots a_n \,/\, a_n = 0 \text{ et } \sum a_i 2^i = x \end{cases}$
est un codage du problème "Être premier"

Déf. 3 : une machine de Turing déterministe (M.T.D) est un septuplet $(\Sigma, \#, \Gamma, Q, q_0, F, \Delta)$ où :
- Σ est l'alphabet (fini) d'entrée
- $\#$ est le symbole blanc
- $\Gamma \supset \Sigma \cup \{\#\}$ est l'alphabet de bande
- Q (fini) est l'ensemble des états
- $q_0 \in Q$ est l'état initial
- $F \subset Q$ est l'ensemble des états finaux
- $\Delta : (Q \times \Gamma) \to (Q \times \Gamma \times \{g, d\})$ la fonction de transition.

Déf. 4 : on appelle langage accepté par une M.T.D $\mathcal{M}$ et l'on note $L(\mathcal{M})$:
$L(\mathcal{M}) = \{$ensembles des $w \in \Sigma^* /$ exécuté sur w, $\mathcal{M}$ termine dans un état final$\}$.

Déf. 5 : Soit $L \subset \Sigma^*$ un langage.
L est dit décidable s'il existe $\mathcal{M}$ M.T.D / $L(\mathcal{M}) = L$ et que $\mathcal{M}$ n'a pas d'exécution infinie. ($L \in R$)
S'il existe $\mathcal{M} / L(\mathcal{M}) = L$, L est dit récursivement énumérable ($L \in RE$)

Prop 1 : - si $L, L' \in R$, alors $L \cup L'$, $L \cap L'$ et $\Sigma^* \setminus L \in R$.
- Si : $L \in RE$ et $\Sigma^* \setminus L \in RE$, alors $L \in R$

Déf 6 : un problème de décision d'instances $x \in E$ est dit décidable s'il existe un codage $f : E \to \Sigma^*$, $\mathcal{M}$ M.T.D d'alphabet Σ / $L_P = L(\mathcal{M})$.

Prop 2 (Thèse de Turing-Church) les langages reconnus par une procédure effective sont ceux décidés par une M.T.D.

II. Prouver l'indécidabilité

Rem 1 : pour prouver la décidabilité d'un problème, on peut exhiber un algorithme qui le résout. En général, prouver l'indécidabilité est plus compliqué.

. Un langage dans RE qui n'est pas dans R.

Déf.7 (langage d'acceptation). Soit $\mathcal{M}$ une M.T.D. On note $\langle \mathcal{M} \rangle$ un codage de $\mathcal{M}$, et pour $w \in \Sigma^*$, $\langle \mathcal{M}, w \rangle$ un codage de $(\mathcal{M}, w)$. On note

$$L_\in = \{\langle \mathcal{M}, w \rangle / w \in L(\mathcal{M})\}$$

Prop.3 : $L_\in \in RE$ mais $L_\in \notin R$.

Déf 8 (calculable) $f : \Sigma^* \to T^*$ est dite calculable s'il existe $\mathcal{M}$ M.T.D qui pour toute entrée $w \in \Sigma^*$ termine dans une configuration où $f(w)$ est écrit sur la bande.

Déf.9 (Réduction). Soient A, B deux problèmes d'alphabet Σ_A, Σ_B. Une réduction de A à B est une fonction calculable $f : \Sigma_A^* \to \Sigma_B^*$ /

$$w \in L_A \iff f(w) \in L_B$$

On note $A \leq_m B$.

Prop.4 : si $A \leq_m B$ et A est indécidable, alors B l'est aussi (si B est décidable, alors A l'est)

Ex les langages $L_\emptyset = \{\langle M \rangle / L(\mathcal{M}) = \emptyset\}$ (1)
et $L_{\neq} = \{\langle \mathcal{M}, \mathcal{M}' \rangle / L(\mathcal{M}) \neq L(\mathcal{M}')\}$ (2)
sont indécidables.

Preuve : (1) on peut réduire $L_\in$ à $L_\emptyset$

$f : (\mathcal{M}, w) \to \mathcal{M}_w$: - rejette $\Sigma^* \setminus \{w\}$
- applique $\mathcal{M}$ à w.

Ainsi $\langle \mathcal{M}, w \rangle \in L_\in \iff f(\mathcal{M}, w) \in L_\emptyset$.

III. Exemples de problèmes

1) En théorie des langages

Langages réguliers : problème du mot

Instances : $(w, \mathcal{A})$, $w \in \Sigma^*$, $\mathcal{A}$ automate "$w \in L(\mathcal{A})$?"
déterministe $\to$ décidable
indéterministe $\to$ décidable

-(w, R) où R est une expression régulière : idem

Langage-vide : Instance : $\mathcal{A}$ un automate
Réponse : "oui" si $L(\mathcal{A}) = \emptyset$. DÉCIDABLE

Égalité : Instances : $\mathcal{A}, \mathcal{A}'$
Réponse : "oui" ssi $L(\mathcal{A}) = L(\mathcal{A}')$ DÉCIDABLE

Langages algébriques :

problème du mot : instances : $(w, \mathcal{A})$ (ou (w, G))
Réponse oui ssi $L(\mathcal{A}) \ni w$ (ou $L_G(S) \ni w$) DÉCIDABLE

-Étant donné G, G' deux grammaires algébriques (d'axiomes S, S') les problèmes suivants sont indécidables :

- $L_G(S) \cap L_{G'}(S') = \emptyset$
- $L_G(S) = L_{G'}(S')$
- $L_G(S) = \Sigma^*$
- G est ambiguë

DÉV. 1

Grammaire contextuelle

Déf 10 : une grammaire est contextuelle si toutes ses règles sont de la forme $uTv \to uwv$ $w \in (A + V \setminus \{S\})^+$ ou $S \to \varepsilon$

Thm 1 : un langage est engendré par une grammaire contextuelle ssi il est accepté par une M.T linéairement bornée.
- Le problème du mot est décidable.
- $L(\mathcal{M}) = \emptyset$ est indécidable

Langage récursivement énumérable

Thm 2 (de Rice) soit $\mathcal{P}$ une propriété non triviale sur R.E. Le problème "$L(\mathcal{M})$ satisfait P" est indécidable

Ex : "$L(\mathcal{M}) = \emptyset$", "$L(\mathcal{M}) = \Sigma^*$" sont indécidables.

2) Problème de correspondance de Post (PCP)

Déf 11 : le PCP est le suivant :

- Instance : n_uplets de paires de mots ($\in \Sigma^*$) $(u_i, v_i)_{i \in [\![1,n]\!]}$
- Réponse : "oui" ssi $\exists N \in \mathbb{N}$ et $(i_1, \dots, i_N) \in \mathbb{N}$ / $u_{i_1} \dots u_{i_N} = v_{i_1} \dots v_{i_N}$

$$\boxed{\begin{matrix}u_1\\v_1\end{matrix}} \quad \boxed{\begin{matrix}u_2\\v_2\end{matrix}} \quad \dots \quad \boxed{\begin{matrix}u_n\\v_n\end{matrix}}$$

- PCP modifié (PCPM) : même énoncé, en imposant $i_1 = 1$
- PCP avec k paires : même énoncé, en imposant $N = k$.
- Prop 5 : PCP $\leq_m$ PCPM et PCPM $\leq_m$ PCP

Thm 3 : PCPM est indécidable, dès que $\mathrm{Card}(\Sigma) \geq 2$

Donc PCP l'est également.

Rem : en revanche, $\forall k \in \mathbb{N}$, PCP_k est décidable.

3) 10e Problème de Hilbert :

Instance : $P \in \mathbb{Z}[X_1, \dots X_n]$

Réponse : oui ssi $\exists (x_1, \dots x_n) \in \mathbb{Z}^n$ / $P(x_1, \dots x_n) = 0$

est indécidable

4) La décidabilité en logique

Déf 12 : on dit qu'une théorie logique T est décidable (semi-décidable, resp.) si l'ensemble des conséquences est décidable (resp. Récursivement énumérable)

Thm 4 (Presburger) la théorie au premier ordre des entiers munis de l'addition est décidable

DÉV.2

Thm 5 (Tarski) la théorie du premier ordre des entiers munis de l'addition et de la multiplication est indécidable.