922

Ensembles récursifs, récursivement énumérables. Exemples

On se fixe un alphabet Σ, $|\Sigma| \geq 2$. L désignera un langage sur Σ.

I. Définitions

De manière informelle, le problème que l'on cherche à résoudre est de savoir si un mot $w \in \Sigma^*$ est dans L.

Rq: Le problème se pose de manière plus générale pour une partie P d'un ensemble E quelconque, mais on peut en général se ramener au cas présent en codant les éléments de E par des mots de Σ^*.

Exemple: On peut coder une machine de Turing sur Σ, on notera $\langle M \rangle$ le codage de la machine M.

Déf: Un mot $w \in \Sigma^*$ est dit accepté par une machine de Turing M si il existe un calcul acceptant avec w initialement sur le ruban.

On note $L(M)$ le langage des mots acceptés par M.

Déf: Un langage L est dit récursivement énumérable si il existe une MT M telle que $L = L(M)$. On note RE la classe des langages récursivement énumérables.

Déf: On note co-RE l'ensemble des langages L tels que $\bar{L} := \Sigma^* \setminus L$ vérifie $\bar{L} \in RE$.

Déf: Un langage L est dit décidable si il existe une MT M sans calculs infinis telle que $L = L(M)$. On note R la classe des langages décidables.

Rq: On a $R \subset RE \cap$ co-RE

Exemple: L'ensemble $P \subset \mathbb{N}$ des nombres premiers est décidable.

II. Caractérisations et propriétés

1/ Autres caractérisations des langages R et RE

Déf: Un énumérateur est une MT déterministe qui écrit sur une bande de sortie des mots de Σ^* séparés par un symbole n'appartenant pas à Σ. La tête de lecture de la bande de sortie ne se déplace jamais vers la gauche.

Prop: L est récursivement énumérable si et seulement si L est l'ensemble des mots énumérés par un énumérateur.

Prop: $L \in R$ si et seulement si L est énuméré par un énumérateur dans l'ordre hiérarchique (ie d'abord les mots les plus courts, et à taille donnée, par ordre lexicographique).

Déf: Le langage calculé par une machine de Turing M est
$\{ w \in \Sigma^* \mid \exists u \in \Sigma^*, M$ s'arrête sur u et w est écrit à la fin de l'exécution $\}$

Prop: $L \in RE$ si et seulement si L est calculé par une MT.

Prop: Une partie $A \subset \mathbb{N}^k$ est décidable si et seulement si χ_A est μ-récursive.

A est récursivement énumérable si et seulement si χ_A est μ-récursive partielle.

2/ Propriétés des langages R et RE

Prop: $L \in R \Leftrightarrow \overline{L} \in R$

Prop: * Si $L_1, L_2 \in RE$, alors $L_1 \cup L_2 \in RE$ et $L_1 \cap L_2 \in RE$

* Si $L_1, L_2 \in R$, alors $L_1 \cup L_2 \in R$, $L_1 \cap L_2 \in R$.

Prop: $RE \cap \text{co-}RE = R$

III. Preuves d'indécidabilité

1/ La preuve par réduction

Déf: Soient L_1 et L_2 deux langages sur des alphabets Σ_1, Σ_2.
Une réduction de L_1 à L_2 est une fonction $f : \Sigma_1^* \to \Sigma_2^*$ calculable par MT telle que $w \in L_1 \Leftrightarrow f(w) \in L_2$.

Si une telle réduction existe, on notera $L_1 \leq L_2$.

Prop: La relation $\leq$ est transitive.

Prop: Supposons $L_1 \leq L_2$, alors $L_2 \in R \Rightarrow L_1 \in R$, et $L_2 \in RE \Rightarrow L_1 \in RE$.
En particulier, la contraposée dit que $L_1 \notin R \Rightarrow L_2 \notin R$.

2/ Exemples de langages indécidables

On considère une énumération (w_i) des mots de Σ^* et (M_i) des MT sur l'alphabet Σ.

Soit $L_0 = \{ w \in \Sigma^* \mid \text{si } w = w_i,\ M_i \text{ n'accepte pas } w_i \}$

Prop: $L_0 \notin R$

Rq: On a $L_0 \in \text{co-}RE$, donc $L_0 \notin RE$.

Déf: Soit $L_\epsilon = \{ \langle M, w \rangle \mid M \text{ accepte } w \}$. L_ϵ est appelé le langage universel.

Prop: $L_\epsilon \notin R$ mais $L_\epsilon \in RE$

Ces deux langages permettent de prouver l'indécidabilité d'autres langages.

exemples : - le problème de l'arrêt : $H = \{ \langle M, w \rangle \mid M \text{ s'arrête sur } w \}$
$H \in RE \setminus R$

- le problème du langage accepté vide : $L_\emptyset = \{ \langle M \rangle \mid L(M) = \emptyset \}$
$L_\emptyset \in \text{co-}RE \setminus R$

- égalité des langages : $L_{\neq} = \{ \langle M_1, M_2 \rangle \mid L(M_1) \neq L(M_2) \}$
$L_{\neq} \notin R$

DÉV

Th: (Rice)
Soit P une propriété non triviale sur les langages récursivement énumérables, le problème de savoir si le langage $L(M)$ d'une MT M vérifie P est indécidable.

IV. Autres problèmes

1/ Problème de correspondance de Post (PCP) et applicat°

a) présentat° du pb

entrée: Une suite $(u_1, v_1), \dots, (u_m, v_m)$ de paires de mots de Σ^*.

question: Existe-t-il une suite d'indices $i_1, \dots, i_n$ telle que $u_{i_1} \cdots u_{i_n} = v_{i_1} \cdots v_{i_n}$

ex: Pour la suite (a, ba), (b, ba), (aba, a), on a une solution : $\boxed{\frac{aba}{a}}\ \boxed{\frac{b}{ba}}\ \boxed{\frac{a}{ba}}$

DÉV

Th: PCP est indécidable

b) Application de Post aux grammaires algébriques

Prop: Soient G et G' deux grammaires algébriques. Les problèmes suivants sont indécidables:
- Est-ce que $L_G(S) \cap L_{G'}(S') = \emptyset$?
- Est-ce que $L_G(S) = L_{G'}(S')$?
- Est-ce que $L_G(S) = \Sigma^*$?
- Est-ce que G est ambiguë ?

2) Décidabilité en logique

On dit qu'une théorie logique est décidable si l'ensemble des formules closes valides est décidable.

Th: La théorie du 1er ordre des entiers munis de l'addition est décidable.

Prop: La logique du 1er ordre est dans $RE \setminus R$

Réf:
- Carton
- Hopcroft-Ullman
- Sipser
- Wolper