914 : Décidabilité et indécidabilité. Exemples

Antoine Dequay Louis Noizet

24 novembre 2020

I Définitions

Definition 1. *Un problème de décision est la donnée d'un langage L et d'un sous-langage $P \subseteq L$. Le problème est de déterminer, étant donné un mot $w \in L$, si $w \in P$.*

Definition 2. *Un codage du langage L est une fonction injective $i : L \to \Sigma^*$ où Σ est un alphabet fini. On notera souvent $< x >$ ou $\lceil x \rceil$ pour $i(x)$.*

Definition 3. *Une machine de Turing à n bandes sur l'alphabet Σ est la donné d'un quintuplet $(Q, \Gamma, \delta, q_0, Q_f)$ tel que $\Gamma \supseteq \Sigma \sqcup \{\triangleright, \Box\}$, $q_0 \in Q, Q_f \subseteq Q$ et $\delta : Q \times \Gamma^n \to Q \times \Gamma^n \times \{-1, 0, 1\}^n$*

Remarque 4. *De nombreux modèles de machines de Turing sont équivalents. Le nombre de bandes peut être arbitrairement choisi par exemple ($n \geq 1$). On peut prendre des bandes infinies ou semi-infines, etc. . .*

Definition 5. *Un ensemble $L \subset \Sigma^*$ est dit récursivement énumérable (RE) si il existe une machine de Turing qui accepte un mot w ssi $w \in L$. Il est dit récursif si de plus, la machine termine sur toutes ses entrées.*

On dit qu'un langage L est décidable (resp. semi-décidable) si il existe un codage de ce langage tel que $\{< x >| x \in L\}$ est récursif (resp. récursivement énumérable).

Proposition 6. *$R \subsetneq RE$*

Definition 7. *co-RE=$\{A, \bar{A} \in RE\}$ où $\bar{A}$ est le problème "inverse" de A : il accepte un mot ssi A ne l'accepte pas.*

Proposition 8. *co-RE $\cap$ RE = R*

Proposition 9. *R et RE sont stables par union et intersection. R est également stable par complémentaire.*

Definition 10. *Une fonction $f : \Sigma^* \longrightarrow \Sigma^*$ est dite calculable ssi il existe $\mathcal{M}$ une machine de Turing telle que pour toute entrée $w \in \Sigma^*$ de $\mathcal{M}$, $f(w)$ apparaît sur le ruban de sortie de $\mathcal{M}$.*

Definition 11. *Une réduction d'un problème A à un problème B est une fonction calculable tr telle que pour toute instance w de A, w est une instance positive de A ssi $tr(w)$ est une instance positive de B.Faire schéma réduction en annexe.*

Remarque 12. *Si A se réduit à B, alors $A \notin R \Rightarrow B \notin R$ et $B \in R \Rightarrow A \in R$.*

II Machines de Turing

Théorème 13. *Étant donnés une machine $\mathcal{M}$ et un mot w, le problème de l'*ARRET *consiste à déterminer si $\mathcal{M}$ s'arrête sur w. Le problème de l'arrêt est indécidable.*

Théorème 14. *Le problème* ACCEPT *(déterminer si une machine $\mathcal{M}$ accepte un mot w) est indécidable.*

Remarque 15. *Dans le cas d'un automate fini, d'un automate à pile ou d'une machine de Turing linéairement bornée, le problème* ACCEPT *est décidable.*

Théorème 16. *Le problème de correspondance de* POST *(PCP) est semi-décidable, où le problème est définit par :*
- *Entrée : Σ un alphabet fini et un ensemble fini de tuiles $(u_i, v_i)_i$ à valeurs dans $\Sigma \backslash \{\varepsilon\}$,*
- *Sortie : vrai s'il existe $i_1, \ldots, i_p$ tels que $u_{i_1} \ldots u_{i_p} = v_{i_1} \ldots v_{i_p}$.*

Definition 17. *Soit p un prédicat sur RE (i.e. une partie de RE). p est dite triviale si $p = \emptyset$ ou $p =$RE.*

Dans ce cas, on définit le problème P_p par :
- *Entrée : $\mathcal{M}$ une machine de Turing,*
- *Sortie : Oui si Lang$(\mathcal{M}) \in p$, non sinon.*

Théorème 18 (Rice)**.** *Si p est un prédicat non-trivial sur RE, alors P_p est indécidable.*

III Logique

Definition 19. *Une théorie est un ensemble de formules closes appelées axiomes.*

Definition 20. *Une théorie T est dite décidable si le problème "une formule φ est conséquence logique de T" est décidable.*

Definition 21 (Arithmétique de Presburger)**.** *C'est le langage engendré par $\{0, 1, +, =\}$, correspondant à la théorie du premier ordre des entiers munis de l'addition mais pas de la multiplication.*

Théorème 22 (Presburger, DVP 1)**.** *L'arithmétique de* PRESBURGER *est décidable.*

Definition 23 (Arithmétique de Péano)**.** *C'est le langage engendré par $\{0, 1, +, \times, =\}$, correspondant à la théorie du premier ordre des entiers munis de l'addition et de la multiplication.*

Théorème 24. *Le problème qui prends en entrée une formule close pour le langage de l'arithmétique de Peano et l'accepte si $\mathbb{N}$ est un modèle de cette formule est indécidable.*

Théorème 25 (Premier ordre, Tarski)**.** *L'arithmétique de Peano est indécidable.*

Théorème 26 (Indécidabilité de la satisfiabilité d'une requête en logique du premier ordre, DVP 2)**.** *Le problème* VALIDFO *:*
- *Entrée : φ une formule close du premier ordre,*
- *Sortie : Oui si φ est valide, non sinon.*

est indécidable.

Théorème 27 (10^e problème de Hilbert, admis)**.** *Le problème :*
- *Entrée : $P \in \mathbb{Z}[X_1, \ldots, X_n]$,*
- *Sortie : Oui si P admet une racine entière.*

est indécidable.

IV Langages

Definition 28 (ACCEPT)**.**
- *Entrée : L un langage, w un mot,*
- *Sortie : Oui si $w \in L$, non sinon.*

Definition 29 (EMPTY)**.**
- *Entrée : L un langage,*
- *Sortie : Oui si $L = \emptyset$, non sinon.*

Definition 30 (UNIV)**.**
- *Entrée : L un langage,*
- *Sortie : Oui si $L = \Sigma^*$, non sinon.*

Definition 31 (EMPTY-INTERSECTION)**.**

- *Entrée : L_1, L_2 deux langages,*
- *Sortie : Oui si $L_1 \cap L_2 = \emptyset$, non sinon.*

Definition 32 (Egal).

- *Entrée : L_1, L_2 deux langages,*
- *Sortie : Oui si $L_1 = L_2$, non sinon.*

Proposition 33. *Dans le cas d'un langage rationnel, on a :*

- Accept *est décidable,*
- Empty *est décidable,*
- Univ *est décidable,*
- Empty-Intersection *est (in)décidable,*
- Egal *est décidable.*

Proposition 34. *Dans le cas d'un langage algébrique, on a :*

- Accept *est décidable,*
- Empty *est décidable,*
- Univ *est indécidable,*
- Empty-Intersection *est indécidable,*
- Egal *est indécidable.*