(1)

GROSPELLIGA Antoine

914 : Décidabilité et indécidabilité : Exemples.

Ref : [1] J-M. Autebert "Calculabilité et décidabilité"
[2] : Arto Salomaa : "Introduction à l'informatique théorique".
[3] : P. Dehornoy : "Complexité et Décidabilité"
[4] : R. Lassaigne, M. de Rougemont : "Logique et fondements de l'informatique"

But : Déterminer ce qui peut être calculé par un système physique, une machine, l'Homme.

I Définitions [1], [2], [3], [4].

Def 1 : Définition d'une machine de Turing (MT) et de ses différentes variantes (+ équivalences) :
- Nombre de rubans
- Déterministe / non-déterministe
- Alphabet Σ.
- Ruban semi-infini.

Def 2 : • Si une MT notée M a un état d'acceptation on note $\mathcal{L}(M) \subseteq \Sigma^*$ l'ensemble des mots acceptés par M (si $w \notin L(M)$ alors $M(w)$ peut boucler).
• Une fonction calculable est une fonction calculée par une MT (éventuellement partielle)

Def 3 : • Un langage $L \subseteq \Sigma^*$ est semi-décidable (ou récursivement énumérable) ssi L est reconnu par une MT.
• Un langage $L \subseteq \Sigma^*$ est décidable (ou récursif) ssi L est reconnu par une MT notée M et M s'arrête sur toute entrée de Σ^*.

[1] **Prop 4 :** • L est décidable ssi L et $(\Sigma^* \setminus L)$ sont récursivement énumérables.
• L est récursivement énumérable ssi existe une MT qui énumère L
• L est décidable ssi il existe une MT qui énumère L dans l'ordre lexicographique.

Ex 5 : Sont décidables :
• $\{(w,n) \in \Sigma^* \times \mathbb{N} \mid w \text{ est de taille } n\}$
• Ayant fixé l'encodage d'une fonction $f : A \to B$ où A et B sont finis est décidable :
$\{w \in \Sigma^* \mid w \text{ code une fonction de } A \text{ dans } B\}$.

Prop 5 : • Les langages rationnels et algébriques sont décidables.
• $\{a^n b^n c^n \mid n \in \mathbb{N}\} \subseteq \{a,b,c\}^*$ est décidable mais non algébrique.

Def 6 : • Réduction de Karp : $L_1 \leq_K L_2$.

Prop 7 : Si $L_1 \leq_K L_2$ et L_2 est semi-décidable (resp décidable) alors L_1 est semi-décidable (resp décidable).

Lemme 8 (fondamental) : On peut représenter une MT par son code $\langle M \rangle \in \Sigma^*$ et la donner en entrée d'une autre machine de Turing.

Rq 9 : C'est à dire que les programmes et les données qu'ils manipulent sont de même nature.

Def 10 : MT Universelle.

Prop 11 : Le problème de l'arrêt est indécidable :
Entrée : Un couple $(\langle M \rangle, w)$ où M est une MT.
Sortie : Est-ce que M s'arrête sur w.

Rq 12 : • Le problème de l'arrêt est semi-décidable
• C'est un argument de diagonalisation qui peut à priori être appliqué pour tous les modèles de calculs

• La thèse de Church (admise par la plupart des informaticiens) est que l'ensemble des fonctions mécaniquement calculable coïncide avec l'ensemble des fonctions calculables par MT.

II) Les différents modèles de calcul [1]

Def 13 : L'ensemble des fonctions récursives primitives

Ex 14 : • L'addition de deux entiers, la multiplication.
• La fonction d'Ackermann n'est pas récursive primitive mais calculable.
• On peut se ramener à un problème de décision avec des fonctions de $\mathbb{N}$ dans $\{0,1\}$.
• Cas des fonctions partielles.

Def 15 : Les fonctions récursives.

[1] Prop 16 : Soit $\phi : \Sigma^* \to \mathbb{N}$ un codage calculable par MT. Alors $L \subseteq \Sigma^*$ est décidable ssi la fonction caractéristique de $\phi(L)$ est récursive.

[1] Def 17 : Les Machines RAM sont composées de :
- Une bande d'entrée en lecture seule (contient des entiers) infinie
- Une bande de sortie en écriture seule (contient des entiers) infinie
- Des registres (contient des entiers) en nombre arbitrairement grand auxquels on accède à tout moment
- Le programme de la machine qui contient des instructions (charger, lire, incrémenter, saut ...).

Rq 18 : C'est un ordinateur pour lequel la bande d'entrée et de sortie est infinie.

Prop 19 : Les MT et les machine RAM sont équivalentes.

III) Problèmes indécidables

a) Problèmes portant sur les Machines de Turing. [1]

Rappel : le problème de l'arrêt est indécidable.

Prop 20 : Le problème de l'arrêt uniforme est indécidable.
Entrée : $\langle M \rangle$ le code d'une MT
Sortie : Est-ce que M s'arrête sur toute entrée ?

Prop 21 : Le problème du langage vide est indécidable.
Entrée : $\langle M \rangle$ le code d'une MT
Sortie : Est-ce que $L(M) = \emptyset$?

Théo 22 De Rice : Soit $\mathcal{P}$ une propriété sur les langages de Σ^*. Si il existe une MT notée M telle que $L(M) \in \mathcal{P}$ et M' telle que $L(M') \notin \mathcal{P}$ alors $\{\langle M \rangle \mid L(M) \in \mathcal{P}\}$ est indécidable. — Dev 1 + Pb de l'arrêt

Rq 23 : • $\mathcal{P}$ porte sur les langages et non sur les machines $\{\langle M \rangle \mid M \text{ a 3 états}\}$ est décidables.
• il existe $L, L' \subseteq \Sigma^*$ tels que $L \in \mathcal{P}$ et $L' \notin \mathcal{P}$ ne suffit pas : $\{\langle M \rangle \mid L(M) \text{ est récursivement énumérable}\} = \Sigma^*$ est décidable.

Ex 24 : • Pb de l'arrêt uniforme, du langage vide.

3

Dev 2

(b) Problème de correspondance de Post [1].

Prop 25 : Le problème de correspondance de Post est indécidable :

Entrée : X un alphabet et une suite de couples de mots $(u_1,v_1),\dots,(u_k,v_k)$.

Sortie : Existe-t-il $i_1,\dots,i_r \in \{1,\dots,k\}$ tels que $u_{i_1}\cdots u_{i_r} = v_{i_1}\cdots v_{i_r}$.

Prop 26 : Le problème du zéro dans les matrices 3×3.

Entrée : Un ensemble $\{M_1 \dots M_k\}$ de matrices à coefficients dans $\mathbb{Z}$, de taille 3×3.

Sortie : Existe-t-il un produit fini $M = M_{i_1}\cdots M_{i_r}$ tel que $M_{(3,2)} = 0$?

Démo : $\varphi(u_i,v_i) = \begin{bmatrix} el(u_i) & el(v_i)-el(u_i) & 0 \\ 0 & el(v_i) & 0 \\ nu(u_i) & nu(v_i)-nu(v_i) & 1 \end{bmatrix}$

où $\begin{cases} n = \#X. \\ el(u) = n^{|u|} \\ nu(u) : \text{le numéro dans l'ordre lexicographique.} \end{cases}$

(c) Le $10^{\text{ème}}$ problème de Hilbert [2]

De la possibilité de résoudre une équation diophantienne.
Soit la donnée d'une équation diophantienne à un nombre quelconque d'inconnues et à coefficients entiers rationnels : on doit trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra décider si l'équation est résoluble en nombres entiers rationnels.

Entrée : $n \in \mathbb{N}$ et $P \in \mathbb{Z}[X_1 \dots X_n]$

Sortie : Existe-t-il $(x_1 \dots x_n) \in \mathbb{Z}^n$ tel que $P(x_1 \dots x_n) = 0$.

Prop 27 : La décidabilité du problème est équivalente à la décidabilité du problème où $(x_1 \dots x_n) \in (\mathbb{N}^*)^n$

Def 28 : Soit $S \subseteq (\mathbb{N})^n$. S est diophantien si $\exists m \in \mathbb{N}$ et $P \in \mathbb{Z}[X_1 \dots X_{n+m}]$ tel que :
$(*\{S,P\}) : (x_1 \dots x_n) \in S \iff \exists y_1 \geq 0 \dots y_m \geq 0$ tq $P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$

Théo 29 : Soit $S \subseteq \mathbb{N}^*$ diophantien $(n=1)$ et $P \in \mathbb{Z}[X, Y_1 \dots Y_m]$ tels que $(*\{S,P\})$. Alors $Q(x, y_1 \dots y_m) = x[1 - P(x, y_1 \dots y_m)^2]$ vérifie : $S = \{Q(x, y_1 \dots y_m) \mid (x, y_1 \dots y_m) \in (\mathbb{N}^*)^{m+1}\}$.

Prop 30 : Soit S diophantien et P tel que $(*\{S,P\})$ alors il existe $\hat{P}$ tel que $(*\{S,\hat{P}\})$ et $\deg \hat{P} \leq 4$.

Ex 31 : $P(x, y_1, y_2) = x^3 y_1^2 - 3y_2^2$

$x \in S$ (ssi) $\exists (y_1, y_2) [x^3 y_1^2 - 3y_2^2 = 0]$

(ssi) $\exists (y_1, y_2, y_3, y_4, y_5) [y_3 = x^2 \wedge y_4 = x y_3 \wedge y_5 = y_4 y_1 \wedge y_5 y_1 - 3y_2^2 = 0]$

(ssi) $\exists (y_1 \dots y_5) [\hat{P}(x, y_1 \dots y_5) = 0]$ où :

$(P_1(x, y_1 \dots y_5) = y_3 - x^3) \wedge (P_2(x, y_1 \dots y_5) = y_4 - x y_3) \wedge (P_3(x, y_1 \dots y_5) = y_5 - y_4 y_1)$
$\wedge (P_4(x, y_1 \dots y_5) = y_5 y_1 - 3y_2^2) \wedge (\hat{P} = P_1^2 + P_2^2 + P_3^2 + P_4^2)$.

Théo (admis) 32 : $S \subseteq \mathbb{N}$ est diophantien $\iff$ il est récursivement énumérable.

Théo 33 : il existe $m \in \mathbb{N}$ et $P_u \in \mathbb{Z}[I, X, Y_1 \dots Y_m]$ un polynôme universel tel que $x \in S_i$ (ssi) $\exists (y_1 \dots y_m)$ tq $P_u(i, x, y_1 \dots y_m) = 0$.

Théo 34 : Le $10^{\text{ème}}$ pb de Hilbert est indécidable $\begin{cases} \leq \deg 2 : \text{décidable} \\ = \deg 3 : \text{ouvert} \\ \geq \deg 4 : \text{indécidable}. \end{cases}$

3