Chapitre 7

Langages décidables et reconnaissables

Définition 7.1. On dit d'un langage L qu'il est décidable si il existe une MT M telle que :

- $\forall w \in L, M$ accepte w et
- $\forall w \notin L, M$ rejette w.

Dans ce cas on dira aussi que la machine M décide le langage L. ▲

Définition 7.2. La classe des langages décidables est notée par DEC. ▲

Rappel : On dit qu'un langage L est décidable si il existe une MT M telle que :

- $\forall x \in L$: M accepte x et
- $\forall x \notin L$: M rejette x.

Définition 7.3. On dit qu'un langage L est reconnaissable si il existe une MT M telle que :

- $\forall x \in L$: M accepte x et
- $\forall x \notin L$: M rejette x ou M boucle sur x.

Dans ce cas on dira aussi que la machine M reconnaît le langage L. ▲

Définition 7.4. La classe des langages reconnaissables est notée par REC. ▲

Paradoxes

“Cette phrase est fausse !”

La phrase est-elle vraie ?

“A) L’énoncé B est vrai !”
“B) L’énoncé A est faux !”

L’énoncé A est-il vrai ?

“Le barbier des îles Mouk-mouk coupe les cheveux de tous les insulaires qui ne se coupent pas les cheveux eux-mêmes, et uniquement de ceux-là.”

Le barbier se coupe-t-il ses cheveux ?

Notation 7.5. Si M est une MT alors $\langle M \rangle$ est un mot qui encode une description complète de M selon une certaine convention. ▲

Définition 7.6.

$$A_{\mathrm{MT}} = \{\langle M, w\rangle \mid M \text{ est une MT et } M \text{ accepte le mot } w\}.$$

▲

Théorème 7.7. Le langage A_{MT} est indécidable.

Preuve. Supposons au contraire qu'une MT H décide le langage A_{MT}.

Considérons la MT D suivante :

Prendre $\langle M \rangle$ en entrée;
donner $\langle M, \langle M \rangle \rangle$ en entrée à H;
simuler H jusqu'à son arrêt;
accepter si, et seulement si H rejette.

Que fait D sur entrée $\langle D \rangle$?

- Si D accepte $\langle D \rangle$, alors H rejette $\langle D, \langle D \rangle \rangle$;
- donc $\langle D, \langle D \rangle \rangle \notin A_{\mathrm{MT}}$;
- donc D rejette $\langle D \rangle$.

- Si D rejette $\langle D \rangle$, alors H accepte $\langle D, \langle D \rangle \rangle$;
- donc $\langle D, \langle D \rangle \rangle \in A_{\mathrm{MT}}$;
- donc D accepte $\langle D \rangle$.

Dans les deux cas on obtient une contradiction. ■

Considérons un tableau indiquant si la MT M_i accepte l'entrée $\langle M_j \rangle$:

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	$\cdots$	$\langle D \rangle$	$\cdots$
M_1	1		1			1	
M_2	1	1	1	1		1	
M_3				1			
M_4	1	1					
$\vdots$							
D			1	1			
$\vdots$							

La sortie de la MT hypothétique H qui décide A_{MT} sur entrée $\langle M_i, \langle M_j \rangle \rangle$ devrait donc être :

	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$	$\cdots$	$\langle D \rangle$	$\cdots$
M_1	1	0	1	0		1	
M_2	1	1	1	1		1	
M_3	0	0	0	1		0	
M_4	1	1	0	0		0	
$\vdots$							
D	0	0	1	1		?	
$\vdots$							

Que doit-on écrire à la case $(D, \langle D \rangle)$?

Théorème 7.8. Un langage L est décidable si, et seulement si L est reconnaissable et $\overline{L}$ est reconnaissable.

Preuve. Clairement L décidable implique L reconnaissable, et L décidable implique $\overline{L}$ décidable qui implique $\overline{L}$ reconnaissable.

D'autre part, supposons qu'il existe des MT M_1 et M_2 qui reconnaissent respectivement L et $\overline{L}$.

Considérons la MT M suivante :

Prendre un mot w en entrée;

simuler en parallèle M_1 et M_2 sur w;

accepter dès que M_1 accepte w;

rejeter dès que M_2 accepte w.

Montrons que M décide L :

- $w \in L \Rightarrow M_1$ accepte $w \Rightarrow M$ accepte w ;
- $w \notin L \Rightarrow w \in \overline{L} \Rightarrow M_2$ accepte $w \Rightarrow M$ rejette w.

■

Corollaire 7.9. Le langage $\overline{A_{\mathrm{MT}}}$ n'est pas reconnaissable.

Preuve. Tout d'abord A_{MT} est reconnaissable par la MT suivante :

Prendre un mot x en entrée;
vérifier que x est de la forme $\langle M, w\rangle$
où M est une MT valide, sinon rejeter;
simuler M sur w;
accepter si M accepte;
rejeter si M rejette;
(et boucler si M boucle).

Supposons que $\overline{A_{\mathrm{MT}}}$ est reconnaissable. On aurait, par le théorème 7.8, que A_{MT} est décidable ce qui contredit le théorème 7.7.

Donc $\overline{A_{\mathrm{MT}}}$ n'est pas reconnaissable. ■

Lemme 7.10. Si $A \leq B$ et B est décidable, alors A est décidable.

Preuve. Soit

$$f \ : \ \Sigma^* \to \Sigma^*$$

une fonction calculable telle que

$$\forall w \in \Sigma^* \ : \ w \in A \Leftrightarrow f(w) \in B.$$

Soit M_B une MT qui décide B.

Alors la machine M_A suivante décide le langage A :

Prendre un mot w en entrée;

calculer $f(w)$;

simuler M_B sur $f(w)$.

■

Lemme 7.11. Si $A \leq B$ et B est reconnaissable, alors A est reconnaissable.

Preuve. Ce lemme se prouve comme le lemme 7.10, *mutatis mutandis*. ■

Les lemmes suivants sont les contraposées des lemmes 7.10 et 7.11.

Lemme 7.12. Si $A \leq B$ et A n'est pas décidable, alors B n'est pas décidable. ■

Lemme 7.13. Si $A \leq B$ et A n'est pas reconnaissable, alors B n'est pas reconnaissable. ■

Le problème d'arrêt

Étant donnés une MT M et un mot w, M s'arrête-t-elle sur entrée w ?

Le problème d'arrêt sous forme de langage :

Définition 7.14.

$$HALTE_{\mathrm{MT}} = \{\langle M, w\rangle \mid \text{la MT } M \text{ ne boucle pas sur entrée } w\}.$$

▲

De façon équivalente :

$$HALTE_{\mathrm{MT}} = \{\langle M, w\rangle \mid \text{la MT } M, \text{ sur entrée } w, \text{ accepte ou rejette}\}.$$

Théorème 7.15. $HALTE_{\mathrm{MT}}$ est indécidable.

Preuve. Montrons que $A_{\mathrm{MT}} \leq HALTE_{\mathrm{MT}}$.

Soit la fonction calculable

$$f \ : \ \Sigma^* \to \Sigma^*$$

telle que

- si y n'est pas de la forme $\langle M, w \rangle$, alors $f(y) = \varepsilon$;
- si $y = \langle M, w \rangle$, alors $f(y) = \langle M', w \rangle$ où M' est la MT suivante :

  Simuler M;

  si M entre dans son état rejetant, alors boucler.

On a :

$$\begin{aligned}
\langle M, w\rangle \in A_{\mathrm{MT}} &\Rightarrow M \text{ accepte } w \\
&\Rightarrow M' \text{ accepte } w \\
&\Rightarrow \langle M', w\rangle \in HALTE_{\mathrm{MT}} \\
&\Rightarrow f(\langle M, w\rangle) \in HALTE_{\mathrm{MT}}.
\end{aligned}$$

D'autre part :

$$\begin{aligned}
\langle M, w\rangle \notin A_{\mathrm{MT}} &\Rightarrow M \text{ rejette ou boucle sur } w \\
&\Rightarrow M' \text{ boucle sur } w \\
&\Rightarrow \langle M', w\rangle \notin HALTE_{\mathrm{MT}} \\
&\Rightarrow f(\langle M, w\rangle) \notin HALTE_{\mathrm{MT}}.
\end{aligned}$$

■

Définition 7.16.

$$TOUT_{\mathrm{MT}} = \{\langle M \rangle \mid L(M) = \Sigma^*\}.$$

▲

Théorème 7.17. $TOUT_{\mathrm{MT}}$ est indécidable.

Preuve. Montrons que $A_{\mathrm{MT}} \leq TOUT_{\mathrm{MT}}$.

Soit la fonction calculable

$$f \ : \ \Sigma^* \to \Sigma^*$$

telle que

- si y n'est pas de la forme $\langle M, w \rangle$, alors $f(y) = \varepsilon$;
- si $y = \langle M, w \rangle$, alors $f(y) = \langle M' \rangle$ où M' est la MT suivante :

Effacer le ruban et y écrire w;

simuler M.

On a :

$$\begin{aligned}
\langle M, w\rangle \in A_{\mathrm{MT}} &\Rightarrow M \text{ accepte } w \\
&\Rightarrow M' \text{ accepte tout} \\
&\Rightarrow \langle M'\rangle \in TOUT_{\mathrm{MT}} \\
&\Rightarrow f(\langle M, w\rangle) \in TOUT_{\mathrm{MT}}.
\end{aligned}$$

D'autre part :

$$\begin{aligned}
\langle M, w\rangle \notin A_{\mathrm{MT}} &\Rightarrow M \text{ rejette ou boucle sur } w \\
&\Rightarrow M' \text{ rejette ou boucle sur tout} \\
&\Rightarrow \langle M'\rangle \notin TOUT_{\mathrm{MT}} \\
&\Rightarrow f(\langle M, w\rangle) \notin TOUT_{\mathrm{MT}}.
\end{aligned}$$

■

Définition 7.18.

$$REG_{\mathrm{MT}} = \{\langle M \rangle \mid L(M) \in \mathsf{REG}\}.$$

▲

Théorème 7.19. REG_{MT} est indécidable.

Preuve. Comme $REG_{\mathrm{MT}} \in$ DEC si, et seulement si $\overline{REG_{\mathrm{MT}}} \in$ DEC, alors montrons que $A_{\mathrm{MT}} \leq \overline{REG_{\mathrm{MT}}}$.

Soit la fonction calculable

$$f \ : \ \Sigma^* \to \Sigma^*$$

telle que

- si y n'est pas de la forme $\langle M, w \rangle$, alors $f(y) = \varepsilon$;
- si $y = \langle M, w \rangle$, alors $f(y) = \langle M' \rangle$ où M' est la MT suivante :

    Prendre un mot x en entrée;

    simuler M sur w;

    si M accepte w alors

        si x est de la forme $\mathtt{a}^n\mathtt{b}^n$ alors accepter, sinon rejeter.

On a :

$$\begin{aligned}
\langle M, w\rangle \in A_{\mathrm{MT}} &\Rightarrow M \text{ accepte } w \\
&\Rightarrow L(M') = \{\mathtt{a}^n\mathtt{b}^n \mid n \geq 0\} \\
&\Rightarrow \langle M'\rangle \in \overline{REG_{\mathrm{MT}}} \\
&\Rightarrow f(\langle M, w\rangle) \in \overline{REG_{\mathrm{MT}}}.
\end{aligned}$$

D'autre part :

$$\begin{aligned}
\langle M, w\rangle \notin A_{\mathrm{MT}} &\Rightarrow M \text{ rejette ou boucle sur } w \\
&\Rightarrow L(M') = \emptyset \\
&\Rightarrow \langle M'\rangle \notin \overline{REG_{\mathrm{MT}}} \\
&\Rightarrow f(\langle M, w\rangle) \notin \overline{REG_{\mathrm{MT}}}.
\end{aligned}$$

■

Théorème de Rice

Définition 7.20. $I \subseteq \Sigma^*$ est un ensemble d'indices si pour toute paire $\langle M_1 \rangle$ et $\langle M_2 \rangle$ telle que M_1 et M_2 sont des MT équivalentes, c'est-à-dire $L(M_1) = L(M_2)$, on a :

$$\langle M_1 \rangle \in I \Leftrightarrow \langle M_2 \rangle \in I.$$

▲

Autrement dit, le fait que $\langle M \rangle$ soit dans I ou non dépend uniquement du langage de M.

Exemples 7.21. Les ensembles suivants sont des ensembles d'indices :

- $\{\langle M \rangle \mid L(M) = \Sigma^*\}$,
- $\{\langle M \rangle \mid L(M) \in \mathsf{DEC} \text{ et } 110011 \notin L(M)\}$,
- $\{\langle M \rangle \mid L(M) \in \mathsf{REG}\}$.

▲

Exemples 7.22. Les ensembles suivants ne sont pas des ensembles d'indices :

- $\{\langle M \rangle \mid M$ passe plus de 5 fois par son état q_0 sur entrée $\texttt{110011}\}$,
- $\{\langle M \rangle \mid M$ ne quitte pas les $|w|$ premières cellules de son ruban sur entrée $w\}$,
- $\{\langle M \rangle \mid M$ possède plus de 1000 états$\}$.

▲

Théorème 7.23 (*Rice*). Soit I est un ensemble d'indices non trivial, c'est-à-dire :

- il existe une MT M^* telle que $\langle M^* \rangle \in I$,
- il existe une MT $M^\dagger$ telle que $\langle M^\dagger \rangle \notin I$,

alors I est indécidable.

Preuve.

Premier cas : pour toute MT $\mathcal{M}$ telle que $L(\mathcal{M}) = \emptyset$, on a : $\langle \mathcal{M} \rangle \notin I$.

Montrons que $A_{\mathrm{MT}} \leq I$.

Soit la fonction calculable

$$f \ : \ \Sigma^* \to \Sigma^*$$

telle que

- si y n'est pas de la forme $\langle M, w \rangle$, alors $f(y) = \langle M^\dagger \rangle$;
- si $y = \langle M, w \rangle$, alors $f(y) = \langle M' \rangle$ où M' est la MT suivante :

Prendre un mot x en entrée;
simuler M sur w;
si M accepte w alors
    simuler M^* sur x.

On a :

$$\begin{aligned} \langle M, w\rangle \in A_{\mathrm{MT}} &\Rightarrow M \text{ accepte } w \\ &\Rightarrow L(M') = L(M^*) \\ &\Rightarrow \langle M'\rangle \in I \\ &\Rightarrow f(\langle M, w\rangle) \in I. \end{aligned}$$

D'autre part :

$$\begin{aligned} \langle M, w\rangle \notin A_{\mathrm{MT}} &\Rightarrow M \text{ rejette ou boucle sur } w \\ &\Rightarrow L(M') = \emptyset \\ &\Rightarrow \langle M'\rangle \notin I \\ &\Rightarrow f(\langle M, w\rangle) \notin I. \end{aligned}$$

Deuxième cas : pour toute MT $\mathcal{M}$ telle que $L(\mathcal{M}) = \emptyset$, on a : $\langle \mathcal{M} \rangle \in I$.

On sait que $\overline{I}$ est indécidable par le premier cas. Donc I est indécidable parce que la classe DEC est fermée par rapport à la complémentation. ■

Quelques conséquences du théorème de Rice

$VIDE_{\mathrm{MT}} = \{\langle M \rangle \mid L(M) = \emptyset\}$ est indécidable car

- il existe une MT M^* telle que $\langle M^* \rangle \in VIDE_{\mathrm{MT}}$,
- il existe une MT $M^\dagger$ telle que $\langle M^\dagger \rangle \notin VIDE_{\mathrm{MT}}$,
- pour toutes MT M_1 et M_2 telles que $L(M_1) = L(M_2)$ on a :

$$\langle M_1 \rangle \in VIDE_{\mathrm{MT}} \Leftrightarrow \langle M_2 \rangle \in VIDE_{\mathrm{MT}}.$$

$FINI_{\mathrm{MT}} = \{\langle M \rangle \mid L(M) \text{ est fini } \}$ est indécidable car

- il existe une MT M^* telle que $\langle M^* \rangle \in FINI_{\mathrm{MT}}$,
- il existe une MT $M^\dagger$ telle que $\langle M^\dagger \rangle \notin FINI_{\mathrm{MT}}$,
- pour toutes MT M_1 et M_2 telles que $L(M_1) = L(M_2)$ on a :

$$\langle M_1 \rangle \in FINI_{\mathrm{MT}} \;\Leftrightarrow\; \langle M_2 \rangle \in FINI_{\mathrm{MT}}.$$

$MAQUISARD_{\mathrm{MT}} = \{\, \langle M \rangle \mid L(M) = \{\texttt{Vive la résistance !}\}\, \}$ est indécidable.

$REG_{\mathrm{MT}} = \{\langle M \rangle \mid L(M)$ est régulier$\}$ est indécidable.

$HC_{\mathrm{MT}} = \{\langle M \rangle \mid L(M)$ est hors contexte$\}$ est indécidable.

Etc.

Exemple de calcul d'une MT :

q_0	a	a	b	b	⊔	⊔
d	q_4	a	b	b	⊔	⊔
d	c	q_6	b	b	⊔	⊔
d	q_3	c	b	b	⊔	⊔
d	a	q_5	b	b	⊔	⊔
d	a	b	q_8	b	⊔	⊔
d	a	b	f	q_{12}	⊔	⊔
d	a	b	f	g	q_7	⊔
d	a	b	f	q_a	g	a

Fixons une MT M et un mot w.

Soit $C(M, w)$ l'ensemble des mots

$$\#C_1\#{C_2}^{\mathrm{R}}\#C_3\#{C_4}^{\mathrm{R}}\#\cdots\#C_l\# \quad \text{ou} \quad \#C_1\#{C_2}^{\mathrm{R}}\#C_3\#{C_4}^{\mathrm{R}}\#\cdots\#{C_l}^{\mathrm{R}}\#$$

tels que

- chaque C_i est une configuration de M ;
- C_1 est la configuration initiale de M sur w ;
- l'état de M en configuration C_l est q_a ;
- $C_1 \vdash C_2 \vdash C_3 \vdash \cdots \vdash C_l$.

Le langage $C(M, w)$ est-il décidable ?

Le langage $\overline{C(M, w)}$ est-il décidable ?

Le langage $\overline{C(M,w)}$ contient l'ensemble des mots qui ne commencent pas par $\#$, ou qui ne se terminent pas par $\#$, ou qui sont de la forme

$$\#C_1\#{C_2}^{\mathrm{R}}\#C_3\#{C_4}^{\mathrm{R}}\#\cdots\#C_l\# \quad \text{ou} \quad \#C_1\#{C_2}^{\mathrm{R}}\#C_3\#{C_4}^{\mathrm{R}}\#\cdots\#{C_l}^{\mathrm{R}}\#$$

mais tels qu'au moins l'une des conditions suivantes est vérifiée :

- il existe un C_i qui n'est pas une configuration de M ;
- C_1 n'est pas la configuration initiale de M sur w ;
- l'état de M en configuration C_l n'est pas q_a ;
- il existe un i tel que $C_i \not\vdash C_{i+1}$.

Théorème 7.24. Le langage $\overline{C(M,w)}$ est hors contexte.

Aperçu de la preuve. On peut montrer facilement que $\overline{C(M,w)}$ est la réunion de langages hors contexte qui correspondent aux conditions énumérées plus haut.

Notamment, pour la dernière condition, c'est-à-dire qu'il existe un i tel que $C_i \not\vdash C_{i+1}$, une GHC pour engendrer les mots

$$\#C_i\#{C_{i+1}}^{\mathrm{R}}\#$$

s'apparente à une GHC qui engendre des mots de la forme ${ww'}^{\mathrm{R}}$ tels que $|w| = |w'|$ et $w \neq w'$.

Une grammaire pour le langage

$$\{ww'^{\mathrm{R}} \in \{\mathtt{a},\mathtt{b}\}^* \mid |w| = |w'| \text{ et } w \neq w'\}$$

est donnée par les règles suivantes :

$$\begin{aligned} S &\rightarrow \mathtt{a}S\mathtt{a} \mid \mathtt{a}S\mathtt{b} \mid \mathtt{b}S\mathtt{a} \mid \mathtt{b}S\mathtt{b} \mid E \\ E &\rightarrow \mathtt{a}F\mathtt{b} \mid \mathtt{b}F\mathtt{a} \\ F &\rightarrow \mathtt{a}F\mathtt{a} \mid \mathtt{a}F\mathtt{b} \mid \mathtt{b}F\mathtt{a} \mid \mathtt{b}F\mathtt{b} \mid \varepsilon \end{aligned}$$

On laisse en exercice le problème de modifier cette GHC afin d'engendrer le langage

$\{\#C\#C'^{\mathrm{R}}\# \mid C$ et C'sont des configurations de $M,$ mais telles que $C \not\vdash C'\}$.

■

Théorème 7.25. Le langage

$$TOUT_{\mathrm{GHC}} = \{\langle G \rangle \mid L(G) = \Sigma^*\}$$

est indécidable.

Preuve. Nous allons montrer que si on peut décider $TOUT_{\mathrm{GHC}}$ alors on peut décider A_{MT}.

Supposons qu'une MT M_t décide $TOUT_{\mathrm{GHC}}$.

Alors la MT suivante décide A_{MT} :

Prendre un mot x en entrée;

vérifier que x est de la forme $\langle M, w \rangle$

où M est une MT valide, sinon rejeter;

construire une GHC G qui engendre le langage $\overline{C(M, w)}$;

simuler M_t sur $\langle G \rangle$;

si $M_t$accepte alors rejeter, et si $M_t$rejette alors accepter.

■

Le problème de l'équivalence de deux GHC

Théorème 7.26. Le langage

$$EQ_{\mathrm{GHC}} = \{\langle G_1, G_2\rangle \mid G_1 \text{ et } G_2 \text{ sont des GHC, et } L(G_1) = L(G_2)\}$$

est indécidable.

Preuve. Soit G_t une GHC telle que $L(G_t) = \Sigma^*$.

Soit la fonction

$$f \ : \ \Sigma^* \to \Sigma^*$$

telle que

- si y n'est pas de la forme $\langle G\rangle$ pour une GHC G, alors $f(y) = \varepsilon$;
- si $y = \langle G\rangle$, alors $f(y) = \langle G, G_t\rangle$.

La fonction f est calculable et vérifie

$$y \in TOUT_{\mathrm{GHC}} \Leftrightarrow f(y) \in EQ_{\mathrm{GHC}},$$

d'où $TOUT_{\mathrm{GHC}} \leq EQ_{\mathrm{GHC}}$.

Donc EQ_{GHC} n'est pas décidable puisque $TOUT_{\mathrm{GHC}}$ n'est pas décidable. ■

Les grammaires généralisées

Définition 7.27. Une grammaire généralisée (GG) ou grammaire de type 0 est un quadruplet $G = (V, \Sigma, R, S)$ où

- V est un ensemble fini de variables ;
- Σ est un alphabet, c'est-à-dire un ensemble non vide et fini de symboles appelés terminaux, $V \cap \Sigma = \emptyset$;
- R est un ensemble fini de règles de la forme $v \to z$ où $v \in (V \cup \Sigma)^*$, $v \neq \varepsilon$, et $z \in (V \cup \Sigma)^*$;
- $S \in V$ est la variable initiale.

Le langage engendré par G, noté $L(G)$, est défini comme pour les GHC. ▲

Exemple 7.28. Soit la GG G suivante :

$$\begin{aligned} V &= \{A, B, C, D, E, S\} \\ \Sigma &= \{\mathtt{a}\} \end{aligned}$$

$$\begin{array}{lll} S \to ACaB & Ca \to aaC & CB \to DB \\ aD \to Da & AD \to AC & AE \to \varepsilon \\ CB \to E & aE \to Ea & \end{array}$$

On a :

$$L(G) = \{\mathtt{a}^{2^k} \mid k = 1, 2, \ldots\}.$$

▲

Théorème 7.29. Si M est une MT, alors il existe une GG G telle que $L(G) = L(M)$.

Preuve. Soit $M = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

On construit une GG $G = (V, \Sigma, R, S)$ qui simule un calcul acceptant de M, mais en sens inverse, de telle sorte que G engendre un mot w à partir de la variable S si, et seulement si M arrive à q_a à partir de w.

La grammaire $G = (V, \Sigma, R, S)$ est définie par

$$V = Q \ \cup \ (\Gamma \setminus \Sigma) \ \cup \ \{S, V_{[}, V_{]}\},$$

et les règles suivantes.

1. Pour simuler une configuration acceptante de M :

$$S \rightarrow V_{[}\ q_a\ V_{]}$$
$$\forall x \in \Gamma\ :\ q_a \rightarrow q_a x$$
$$\forall x \in \Gamma\ :\ q_a \rightarrow x q_a$$

2. Pour simuler une transition de M vers la gauche :

$$\forall x, x', y \in \Gamma,\ \forall q, q' \in Q \text{ tels que } \delta(q,x) = (q', x', \langle \textsc{Gauche} \rangle)\ :$$
$$q' y x' \rightarrow y q x$$

3. Pour simuler une transition de M vers la gauche lorsque la tête est à l'extrémité gauche du ruban :

$$\forall x, x' \in \Gamma,\ \forall q, q' \in Q \text{ tels que } \delta(q, x) = (q', x', \langle \textsc{Gauche} \rangle)\ :$$
$$V_{\lfloor}\ q'x'\ \rightarrow\ V_{\lfloor}\ qx$$

4. Pour simuler une transition de M vers la droite :

$$\forall x, x' \in \Gamma,\ \forall q, q' \in Q \text{ tels que } \delta(q, x) = (q', x', \langle \textsc{Droite} \rangle)\ :$$
$$x'q'\ \rightarrow\ qx$$

5. Pour simuler une transition de M vers la droite lorsque la tête est déjà à l'extrémité droite dans la configuration :

$$\forall y \in \Gamma,\ \forall q, q' \in Q \text{ tels que } \delta(q, \sqcup) = (q', y, \langle \textsc{Droite} \rangle)\ :$$
$$y q'\ V_{]}\ \rightarrow\ q\ V_{]}$$

6. Pour simuler une configuration initiale de M :

$$V_{[}\ q_0\ \rightarrow\ V_{[}$$
$$\forall x \in \Sigma\ :\ V_{[}\ x\ \rightarrow\ x V_{[}$$
$$V_{[}\ V_{]}\ \rightarrow\ \varepsilon$$

■

Théorème 7.30. Si $G = (V, \Sigma, R, S)$ est une GG, alors il existe une MT M telle que $L(M) = L(G)$.

Aperçu de la preuve.

- La machine M prend en entrée un mot w et le garde en mémoire pour fin de comparaison avec le *mot courant* décrit ci-dessous.

- La variable S devient le mot courant.

- On essaie à tour de rôle chacune des règle dans R, de toutes les façons possibles, sur le mot courant. Ce procédé est appliqué itérativement de façon à simuler une recherche en largeur dans un arbre. Les mots courants antérieurs doivent donc être conservés en mémoire afin d'implanter le *retour-arrière* nécessaire à la fouille.

- Aussitôt que le mot courant est identique à w, M s'arrête et accepte.

■

Théorème 7.31. Le langage

$$A_{\mathrm{GG}} = \{\langle G, w\rangle \mid G \text{ est une GG et } w \in L(G)\}$$

est indécidable.

Preuve. Montrons que $A_{\mathrm{MT}} \leq A_{\mathrm{GG}}$.

La fonction calculable qui définit la réduction est la suivante :

$$f \ : \ \Sigma^* \to \Sigma^*$$

telle que

- si y n'est pas de la forme $\langle M, w\rangle$, alors $f(y) = \varepsilon$;
- si $y = \langle M, w\rangle$, alors $f(y) = \langle G, w\rangle$ où G est la GG qui simule M, telle que construite au théorème 7.29.

■

D'autres problèmes

Est-ce que tous les problèmes indécidables concernent la théorie des langages ?

Non :

- PCP : le problème de correspondance de Post ;
- le 10e problème de Hilbert sur les équations diophantiennes : si $p(x_1, \ldots, x_n)$ est un polynôme à coefficients entiers et à n variables, est-ce que $p(x_1, \ldots, x_n) = 0$ a une solution entière ? (Matiyasevich, 1970) ;
- problème de compression : sur entrée w trouver le plus court mot $\langle M \rangle$ tel que la machine M imprime w et s'arrête ;
- etc.

Les 10 problèmes de Hilbert

1 Problème de M. Cantor relatif à la puissance du continu.

2 De la non-contradiction des axiomes de l'arithmétique.

3 De l'égalité en volume de deux tétraèdres de bases et de hauteurs égales.

4 Problème de la ligne droite, plus court chemin d'un point à un autre.

5 De la notion des groupes continus de transformations de Lie, en faisant abstraction de l'hypothèse que les fonctions définissant les groupes sont susceptibles de différentiation.

6 Le traitement mathématique des axiomes de la physique.

7 Irrationalité et transcendance de certains nombres.

8 Problèmes sur les nombres premiers, hypothèse de Riemann.

9 Démonstration de la loi de réciprocité la plus générale dans un corps de nombres quelconque.

10 De la possibilité de résoudre une équation de Diophante.

Les problèmes 7, 8 et 9 n'ont pas encore été résolus.

Problème 2

DE LA NON-CONTRADICTION DES AXIOMES DE L'ARITHMÉTIQUE.

Version plus faible : existe-t-il un algorithme qui permet de décider si un énoncé mathématique est vrai ou faux ?

$$VRAI = \{w \mid w \text{ est un énoncé mathématique vrai}\}$$

Réponse : NON ! (Gödel, 1931)

Une machine qui décide $VRAI$ peut être utilisée pour décider A_{MT}, car le fait qu'une machine donnée s'arrête sur un mot donné peut être formulé comme un énoncé mathématique.

Problème 10

DE LA POSSIBILITÉ DE RÉSOUDRE UNE ÉQUATION DE DIOPHANTE.

Existe-t-il un algorithme qui permet de décider si une équation diophantienne possède une solution entière ?

$$DIOPHANTE = \{\langle p(x_1, \ldots, x_n)\rangle \mid$$
$$p \text{ est un polynôme à coefficients entiers}$$
$$\text{et } p(x_1, \ldots, x_n) = 0 \text{ a une solution dans } \mathbb{N}\}$$

$$\langle x^2 + 2xy + y^2 + 1 \rangle \notin DIOPHANTE$$

$$\langle x^2 + y^2 - z^2 \rangle \in DIOPHANTE, \text{ puisque } 3^2 + 4^2 - 5^2 = 0$$

$$\langle (x+1)^3 + (y+1)^3 - (z+1)^3 \rangle \notin DIOPHANTE$$

Le dernier théorème de Fermat énoncé au XVIIe sciècle et résolu en 1993 par Wiles :

$$\forall k > 2 \ : \ \langle (x+1)^k + (y+1)^k - (z+1)^k \rangle \notin DIOPHANTE.$$

Le langage $DIOPHANTE$ est reconnaissable par la MT suivante :

Prendre un mot w en entrée;
vérifier que w est de la forme $\langle p(x_1, \ldots, x_n) \rangle$, sinon rejeter;
pour i allant de 0 à l'infini faire :
pour tous les $x_j \in \{0, \ldots, i\}$:
vérifier si $p(x_1, \ldots, x_n) = 0$ est une solution,
si oui alors accepter.

Le 10e problème de Hilbert est :

$DIOPHANTE$ est-il décidable ?

Définition 7.32. Un sous-ensemble L de $\mathbb{N}$ est diophantien s'il existe un polynôme $p(a, x_1, \ldots, x_n)$ à coefficients dans $\mathbb{Z}$ tel que

$$\forall a,\ \exists x_1, \ldots, x_n\ :\ p(a, x_1, \ldots, x_n) = 0 \Leftrightarrow a \in L.$$

L'équation $p(a, x_1, \ldots, x_n) = 0$ est appelée une équation diophantienne. ▲

Exemples 7.33. $L = \{a \in \mathbb{N} \mid a = b^2\}$ est diophantien :

$$a - x_1^2 = 0.$$

$L = \{a \in \mathbb{N} \mid a$ est composé $\}$ est diophantien :

$$a - (x_1 + 2)(x_2 + 2) = 0.$$

$L = \{a \in \mathbb{N} \mid a \neq 2^k\}$ est diophantien :

$$a(2x_1 + 3)x_2 = 0.$$

▲

L'ensemble des nombres premiers est diophantien :

$$
\begin{aligned}
\alpha - (k+2)(1 \quad & - \quad [wz + h + j - q]^2 \\
& - \quad [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
& - \quad [2n + p + q + z - e]^2 \\
& - \quad [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\
& - \quad [e^3(e+2)(a+1)^2 + 1 - o^2]^2 \\
& - \quad [(a^2 - 1)y^2 + 1 - x^2]^2 \\
& - \quad [16r^2y^4(a^2 - 1) + 1 - u^2]^2 \\
& - \quad [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\
& - \quad [n + l + v - y]^2 \\
& - \quad [(a2 - 1)l^2 + 1 - m^2]^2 \\
& - \quad [ai + k + 1 - l - i]^2 \\
& - \quad [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
& - \quad [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
& - \quad [z + pl(a - p) + t(2ap - p2 - 1) - pm]^2)
\end{aligned}
$$

Pour tout alphabet Σ, il existe une bijection entre $\mathbb{N}$ et Σ^*. Cette bijection est donnée par l'ordre lexicographique.

Tout langage reconnaissable est diophantien.

En fait, pour toute MT M on peut construire une équation diophantienne

$$p(a, x_1, \ldots, x_n) = 0$$

telle que $p(a, x_1, \ldots, x_n) = 0$ ssi $a \in L(M)$.

Si on pouvait décider le 10e problème de Hilbert, alors on pourrait décider $VIDE_{\mathrm{MT}}$.

Pavages du plan

Étant donné un ensemble fini de tuiles on s'intéresse au pavage du plan.

De combien de façons peut-on paver le plan de façon périodique ?

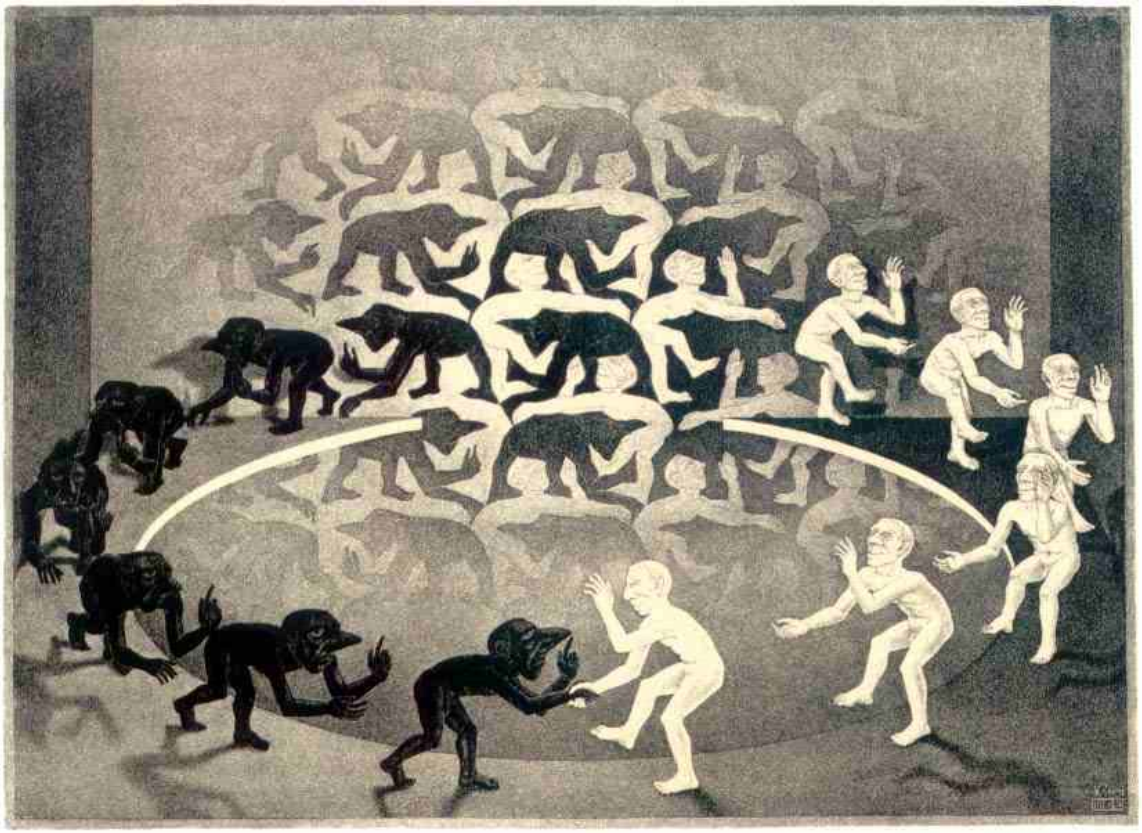
Peut-on paver le plan de façon apériodique ?

Existe-t-il des ensembles de tuiles ne pouvant paver le plan que de façon apériodique ?

Étant donné un ensemble de tuiles, peut-on décider s'il existe une façon de paver le plan avec elles ?

Reptiles de Escher

Encounter de Escher



Pavages du plan

Plusieurs des caractéristiques d'un ensemble donné de tuiles donnnent lieu à des problèmes indécidables...

...car on peut simuler une MT avec un nombre fini de tuiles.

La jeu de la vie de Conway
Conways's game of life

Sur une grille infinie les individus sont représentés par des points noirs.

À chaque étape du jeu, la survie, la mort ou la naissance d'un individu dépend du nombre de ses voisins.

- Dans une case vide avec exactement trois voisins un individu naît ;
- un individu qui a deux ou trois voisins survit ;
- sinon l'individu meurt.

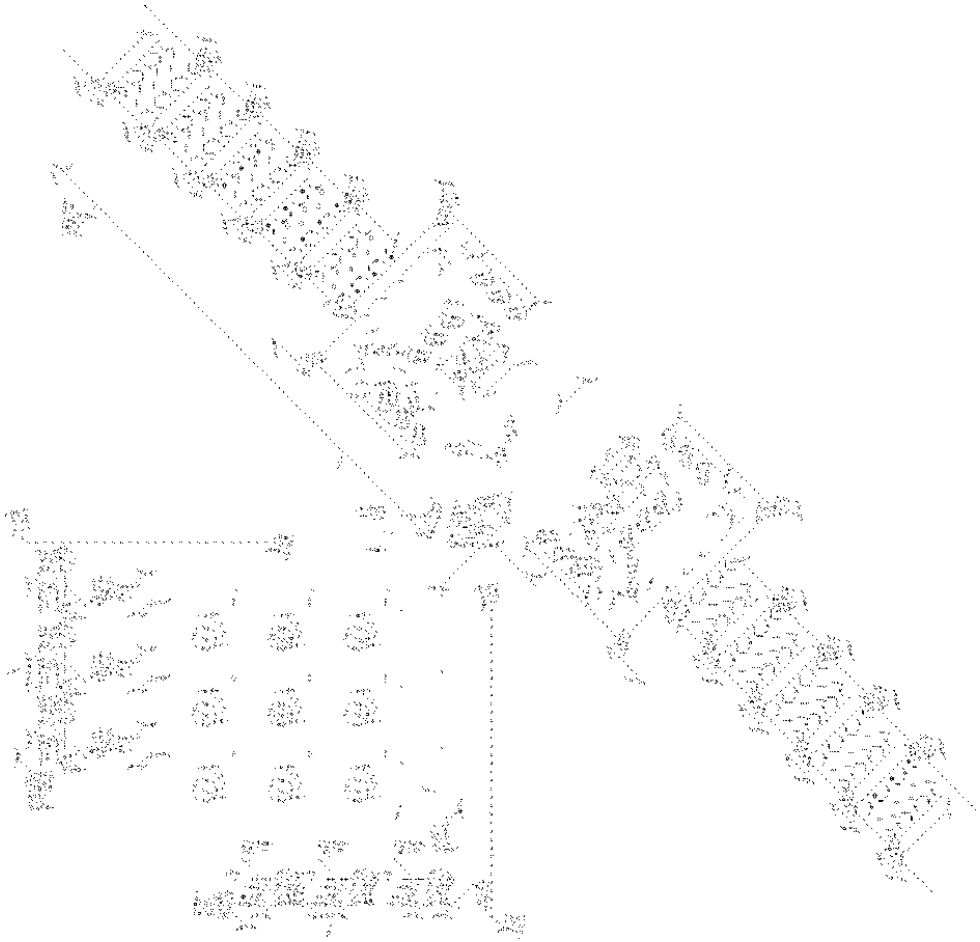
LIFE a été inventé par le mathematicien John Conway en 1970.

Peut-on prédire l'évolution de la population à partir de la configuration initiale ?

La plupart des caractéristiques d'une population de départ dans *LIFE* donnent lieu à des problèmes indécidables...

...car on peut simuler une MT avec *LIFE*.

Universalité de *LIFE*



Hiérarchie

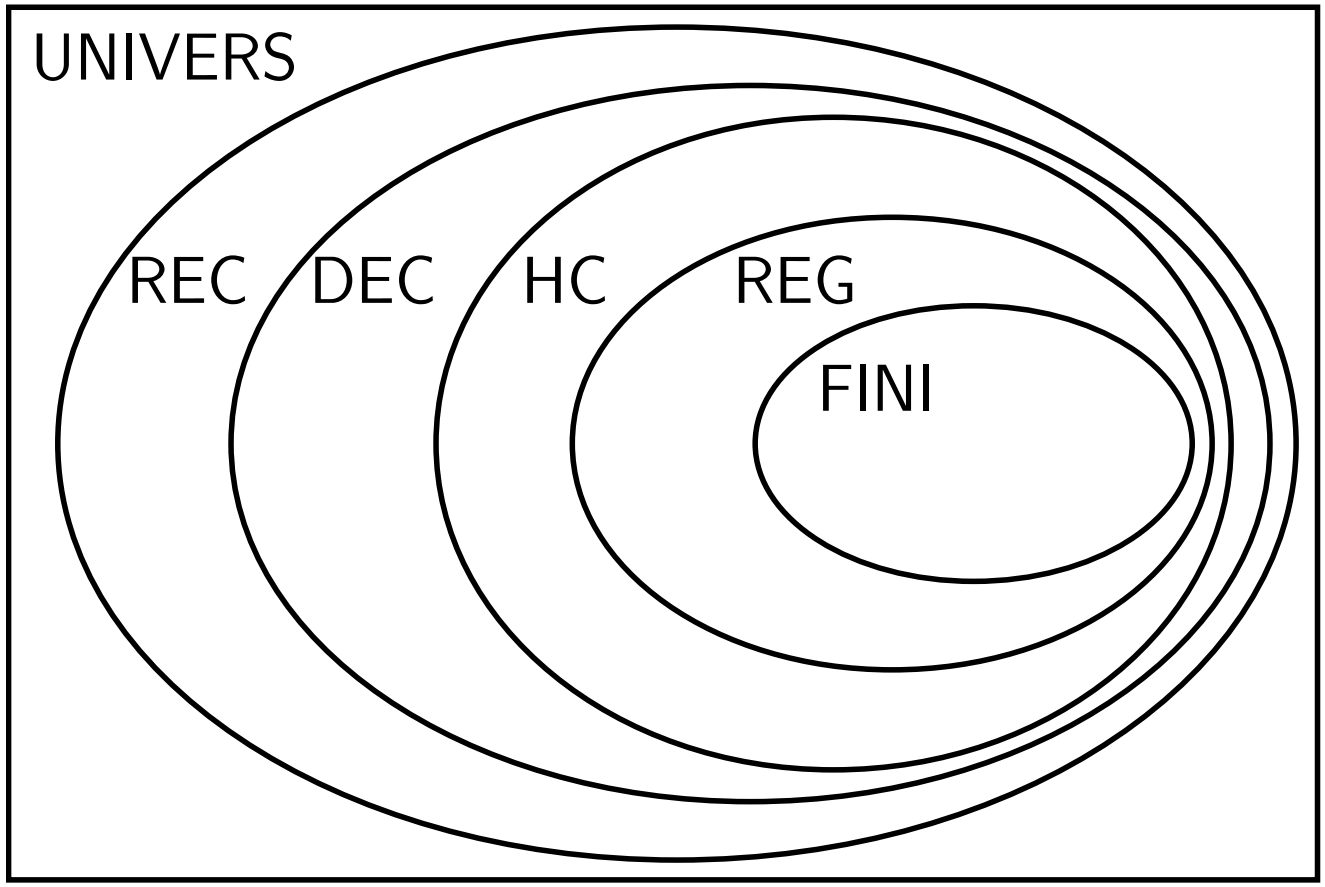



Figure 7.1.