

26/02/2018

TURING

①

CM

## La MT universelle notée $M'$ -

Il prend en paramètres ① le codage en binaire d'une MT  $M$ . On le note  $m = [M]_2$ . (c'est la liste des transitions de  $M$ . cf TD)

② un mot  $w$  sur lequel on doit exécuter  $M$ .  $M(m, w)$  simule l'exécution de  $M(w)$ .

### Analogie-1 -

$M(m, w)$  simule  $M(w)$

$M'$  est une machine virtuelle qui exécute bytecode  $m$  sur la donnée  $w$ .

### Analogie-2 -

Si on regroupe la machine virtuelle  $M'$  et le bytecode  $m$ , on obtient  $M(m)$  qui est un exécutable.

On peut l'exécuter sur la donnée  $w$ . On obtient alors le résultat de  $M(w)$

Donc  $M(m) \equiv M$ .

### Analogie-3 -

$M(m) \equiv M$

[ code source  $\rightarrow$  version exécutable compilée de  $m$  ]

[ interpréteur ou machine virtuelle ]

### Notation -

$M(m, w) \equiv \underbrace{M(m)}_{M'}(w) \equiv M(w)$  où  $m = [M]_2$

Indécidabilité  $\Sigma = \{0, 1\}$

### Vocabulaire historique -

Définition - Un langage est récursivement enumerable si il est reconnaissable par une MT

exemple:  $\exists$  MT  $M_L$  telle que  $L(M_L) = L$

$M_L(w) \xrightarrow{*} 0 \Leftrightarrow w \in L$

Definition : Un langage est co-recursivement enumérrable si :  
 son complémentaire  $\bar{L}$  est recursivement enumérrable.  
 $\bar{L}$  reconnaissable par une MT.

Proposition (voir TD) : un langage  $L$  est décidable  
 si  $L$  est recursivement enumérrable et co-recursivement enumérrable

Consequence : un langage  $L$  est indécidable si  $L$  ou  $\bar{L}$  n'est pas reconnaissable

Par exemple, un premier langage indécidable.

On s'intéresse à l'ensemble  $M = \{m \in \{0,1\}^* \mid m = [M]_2, M \in MT\}$   
 $M$  est l'ensemble de tous les codages binaires de MT.

On considère les sous-ensembles de  $M \times \{0,1\}^*$ .

Ils sont constitués de couples  $(m, w)$  formés :  
 d'un codage de MT  $m$ .  
 d'un mot binaire  $w$ .

Proposition : Le langage  $L_U$  est indécidable.

$$L_U = \{(m, w) \in M \times \{0,1\}^* \mid m = [M]_2, M(w) \rightarrow^* \textcircled{O}\}$$

$L_U$  est l'ensemble des couples  $(m, w)$  tel que la machine  $\equiv_m$  accepte le mot  $w$ .

PREUVE :  $L_U$  indécidable signifie  $L_U$  ou  $\bar{L}_U$  n'est pas reconnaissable

On va montrer que :

①  $L_U$  est reconnaissable

②  $L_U$  n'est pas reconnaissable

1-  $L_U$  est reconnaissable si il existe une MT  $M_{L_U}$  telle que  $L(M_{L_U}) = L_U$

$$\begin{aligned} (\text{i.e.}) \quad M_{L_U}(m, w) \rightarrow^* \textcircled{O} &\iff (m, w) \in L_U \\ (m, w) \in L_U &\iff m = [M]_2, M(w) \rightarrow^* \textcircled{O} \\ &\quad \equiv_{M(w)} \end{aligned}$$

$$\iff M(m)(w) \rightarrow^* \textcircled{O}$$

$$M(m) \equiv_{M(w)} \rightarrow^* \textcircled{O}$$

(suite preuve)

② a) Donc la machine  $M_{\bar{L}_U}$  qu'on cherche est  $M$  et  $L_M = \bar{L}(M)$ , donc  $L_M$  est reconnaissable.

2- Le langage  $\bar{L}_U$  n'est pas reconnaissable.

$$\begin{aligned} \bar{L}_U &= (M \times \{0,1\}^*) \setminus L_U \\ &= \{(m, w) \in M \times \{0,1\}^* \mid m = [M]_2, M(w) \xrightarrow{*} \emptyset \} \end{aligned}$$

$$M(w) \xrightarrow{\text{au}} \infty$$

preuve par contradiction -

Supposons qu'il existe une MT  $M_{\bar{L}_U}$  qui reconnaît  $\bar{L}_U$  et montrons que l'on aboutit à une contradiction.

$$M_{\bar{L}_U}(m, w) \xrightarrow{*} \emptyset \iff (m, w) \in \bar{L}_U$$

$\left[ \begin{array}{l} \text{L mot} \\ \text{machine} \end{array} \right]$

On utilise  $M_{\bar{L}_U}$  pour construire la machine  $M_C$

$$M_C(w) \stackrel{\text{def}}{=} M_{\bar{L}_U}(w, w)$$

$M_C$  duplique le mot  $w$  puis lance  $M_{\bar{L}_U}$

$$\begin{aligned} \bar{L}(M_C) &= \{w \in M \mid M_C(w) \xrightarrow{*} \emptyset\} \quad \text{par définition du langage} \\ &= \{m \in M \mid M_C(m) \xrightarrow{*} \emptyset\} \quad \text{reconnu par MT.} \\ &= \{m \in M \mid M_{\bar{L}_U}(m, m) \xrightarrow{*} \emptyset\} \quad \text{,} \\ &= \{m \in M \mid (m, m) \in \bar{L}_U\} \end{aligned}$$

$$\begin{aligned} \bar{L}(M_C) &= \{m \in M \mid m = [M]_2, M(m) \xrightarrow{*} \emptyset \text{ ou } M(m) \xrightarrow{\text{au}} \infty\} \\ &\quad (\text{par déf de } \bar{L}_U) \end{aligned}$$

= [l'ensemble des codages binaires  $m$  de MT tels que la machine correspondante  $M$  n'accepte pas entant que mot, son codage binaire]

Notez que la machine  $M_C$  a un codage binaire  $m_C = [M_C]_2$

Posons nous la question  $m_C \in \bar{L}(M_C)$  par déf de  $\bar{L}(M_C)$

$$\begin{aligned} M_C(m_C) &\xrightarrow{*} \emptyset && \begin{array}{l} \xrightarrow{\text{def appartenance}} \\ \xrightarrow{\text{def de } \bar{L}(M_C)} \end{array} \\ & & m_C = [m_C]_2 & \xrightarrow{\text{def de } \bar{L}(M_C)} \\ & & & M_C(m_C) \xrightarrow{\text{au}} \infty \\ & & & M_C(m_C) \xrightarrow{*} \infty \end{aligned}$$

contradiction.



① TD TDG - MCAL TURING - Serie 3 (sujet sur internet)

Exercice 1-  $\Sigma = \{0,1\}$

q<sub>1</sub>- L ⊆ Σ\*

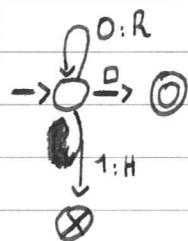
M<sub>0</sub> decide L

- ① Pour tout mot  $w \in L$ ,  $M_0(w) \rightarrow^* \emptyset$
- ② Pour tout mot  $w \notin L$ ,  $M_0(w) \rightarrow^* \emptyset$
- ③ Pour tout mots,  $M_0(w)$  termine.  $w \in \Sigma^*$

MR reconnaît le langage L

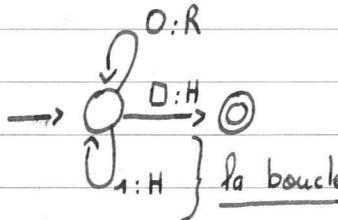
- ① Pour tout mots  $w \in L$ ,  $MR(w) \rightarrow^* \emptyset$
- ② Pour tout mots  $w \notin L$ , soit  $M_n(w) \rightarrow^* \emptyset$  ou  $MR(w) \rightarrow \infty$

q<sub>2</sub>- M<sub>2</sub> qui decide  $\{0^m \mid m \in \mathbb{N}\}$

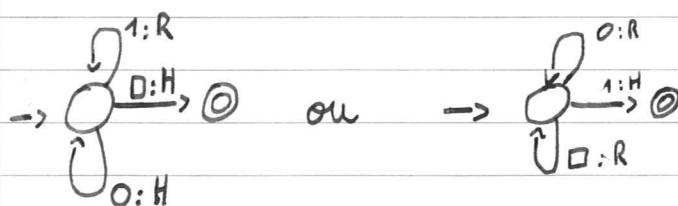


q<sub>3</sub>- M<sub>3</sub> qui decide pas mais qui reconnaît  $\{0^m \mid m \in \mathbb{N}\}$

↳ au moins un mot sur lequel elle boucle.



q<sub>4</sub>- M<sub>4</sub> qui ne decide pas mais qui reconnaît  $\{0^m \mid m \in \mathbb{N}\}$



q5 -  $M_1$  décide  $L$ , montrez que  $\bar{L}$  est décidable.

$\hookrightarrow M_1$  termine  $\forall$  mots  $w \in \Sigma^*$

$$M_1(w) \rightarrow \textcircled{O} \Leftrightarrow w \in L$$

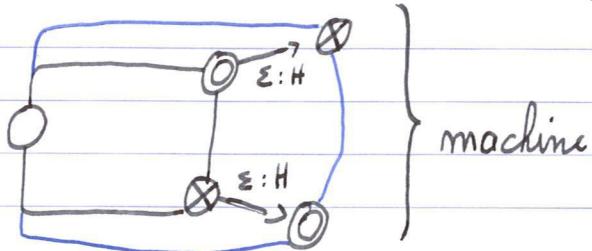
$$M_1(w) \rightarrow \textcircled{X} \Leftrightarrow w \notin L$$

$\exists$  une MT  $M_2$  qui décide  $\bar{L}$

$M_2$  termine  $\forall w \in L$

$$M_2(w) \rightarrow \textcircled{O} \Leftrightarrow w \in \bar{L} \Leftrightarrow w \notin L$$

$$M_2(w) \rightarrow \textcircled{X} \Leftrightarrow w \notin \bar{L} \Leftrightarrow w \in L$$



q6 - langage  $L$ :

$M_1$  reconnaît  $L$  mais ne décide pas  $\bar{L}$  donc il existe au moins un mot de  $\bar{L}$  sur laquelle elle boucle.

$M_2$  reconnaît  $\bar{L}$  mais ne décide pas  $\bar{L}$  donc il existe au moins un mot de  $L$  sur laquelle elle boucle.

Montrez que  $L$  est décidable.

l'idée :

$$M(w) = \left\{ \begin{array}{ll} B_1 & \boxed{\square | w |} \\ & M_1 \rightarrow \textcircled{O} \\ & \rightarrow \textcircled{X} \\ & \rightarrow \textcircled{O} \\ B_2 & \boxed{\square | w |} \\ & M_2 \rightarrow \textcircled{O} \text{ si } w \notin L \end{array} \right\}$$

Dès qu'une des machines  $M_1$  ou  $M_2$  s'arrête on peut répondre

- Si  $M_1$  s'est arrêté, on rend le résultat de  $M_1$

- Si  $M_2$  s'est arrêté la première, on rend le résultat inverse.  $\textcircled{O}$  si  $\textcircled{X}$  et inversement.

Exercice 2 - q7.  $\mathbb{N} \rightarrow \mathbb{B}$  mon denombreable

$\mathbb{N} \rightarrow \mathbb{B}$  l'ensemble fonction entier prédictat entier booleen

$$\mathbb{N} \rightarrow \mathbb{B} = \{ P \mid P(n) = b, n \in \mathbb{N}, b \in \mathbb{B} \}$$

prédictat définit  $[0 \dots \mathbb{N}]$

vois y sujet  
pour comprendre.

q8 - 4 éléments  $\mathbb{N} \rightarrow \mathbb{B}$

$$P_0 \quad 1 \rightarrow \text{F} \quad | \quad 1 \rightarrow (1=0)$$

$$P_1 \quad 1 \rightarrow \text{V} \quad | \quad 1 \rightarrow i \bmod 2 = 0 \text{ (pair)}$$

②

	0 0	1 1	2 2	3 3	4 4	...
q <sub>9</sub>	N					
P <sub>1</sub>	F	F	F	F	F	...
P <sub>2</sub>	V	V	V	V	V	...
P <sub>3</sub>	V	F	F	F	F	...
P <sub>4</sub>	V	F	V	F	V	...
	...	...	...	...	...	
						P <sub>c</sub>

en gris, enumeration des entiers.

q<sub>10</sub> - l'absurde

contradiction

Supposons en bijection avec N

bijection entre N et N → B

à l'associer P<sub>f</sub>Tous contenant ligne l valeur booleennes des predicats P<sub>f</sub>

numéro

diagonale.  $P(i) \stackrel{\text{def}}{=} P_f(i)$  doit apparaître dans laT contenant tout les predicats<sup>1</sup>tableau à une certaine ligne l, donc  $P = P_f$ .

$$\text{Cons : } f(i) = F_f(i) + 1$$

évaluons P au point l

$$P(0) = V \quad P(1) = F \quad P(2) = V \quad P(3) = V$$

↳ négation de la diagonale.

$$P(l) = P_f(l) \text{ puisque } P = P_f.$$

†

→ contradiction.

$$P(l) = \neg P_f(l) \text{ par définition.}$$

Exercice 3 -

$$\begin{aligned} C_2(m, (l, c)) \\ \{C_2(0, (0, 0))\} \end{aligned}$$

$$\begin{cases} C_2(m, (l, c)) \xrightarrow{l \geq 1} C_2(m+1, (l-1, c+1)) \\ C_2(m, (0, c)) \longrightarrow C_2(m+1, (c+1, 0)) \end{cases}$$

q<sub>13</sub> -  $m \leftrightarrow (i, j, k) \leftrightarrow ((i, j), k)$

$$\begin{matrix} & \uparrow \\ C_2 & \xrightarrow{(m, l)} (m, l) \end{matrix} \leftrightarrow m$$

q<sub>14</sub> -  $C_2(m, (i, j)), \quad \rightarrow C_3(m, (i, j, k))$

$$C_2(m, (m, l))$$

① CM DS de MCAL MT ce vendredi en salle 319, 321.

→ MT à 1 ou 2 bandes.

→ try catch.

→ busy beaver.

### Exemple d'ensemble non-dénombrable (ie $\not\cong \mathbb{N}$ )

① l'ensemble des fonctions  $\mathbb{N} \rightarrow \mathbb{N} \rightsquigarrow \mathbb{R}$  ensemble des réels de  $[0, 1[$

② l'ensemble des prédicts  $\mathbb{N} \rightarrow \text{bool} \rightsquigarrow \mathcal{P}(\mathbb{N})$  ensemble des parties  $\mathbb{N}$

↳ sous-ensemble

Montrons que  $f = \{f : \mathbb{N} \rightarrow \mathbb{N}\}$

Preuve par contradiction.

Supposons que  $f$  soit dénombrable (ie  $f \cong \mathbb{N}$ ) autrement dit, on peut attribuer un numéro à chaque fonction. Alors on peut ranger les fonctions dans un tableau : à la ligne  $l$ , on range la fonction  $f_l$ .

Une fonction  $f : \mathbb{N} \rightarrow \mathbb{N}$  elle peut être définie par un tableau :  $n \quad 0 \quad 1 \quad 2 \quad 3 \quad \dots \quad \mathbb{N}$   
 $f(n) \quad f(0) \quad \dots \quad \dots \quad \dots$

On construit le tableau de contrepôts :

$\mathbb{N}$	0	1	2	3	4	5	$\dots$
mul = $f_0$	0	0	0	0	0	0	$\dots$
ident = $f_1$	0	1	2	3	4	5	$\dots$
incr = $f_2$	0	1	2	3	4	5	$\dots$
double = $f_3$	0	2	4	6	8	10	$\dots$
$f_4$	$\dots$	$\dots$	$\dots$	$\dots$	$f_4(4)$	$\dots$	$\dots$

Si  $f : \mathbb{N} \rightarrow \mathbb{N}$  est dénombrable alors toute fonction  $\mathbb{N} \rightarrow \mathbb{N}$  apparaît à une certaine ligne du tableau.  
Considérons la fonction  $g$  suivante :

$$g(n) = f_n(n) + 1 : \mathbb{N}$$

$g$  est bien une fonction de  $\mathbb{N}$  dans  $\mathbb{N}$ .  
quelques valeurs de  $g$ :

$$g(0) = f_0(0) + 1 = 1$$

$$g(1) = 2$$

$$g(2) = f_2(2) + 1 = 3$$

→  $g$  doit donc apparaître à une certaine ligne, disons  $l$ , du tableau.  
donc  $g = f_l$

On aboutit à une contradiction.

$$\text{puisque } g = f_l \text{ alors } g(l) = f_l(l)$$

$$\text{par définition de } g \text{ on a } g(l) = f_l(l) + 1 \quad x \rightarrow \text{contradiction}$$

### CONCLUSION:

En supposant  $f$  dénombrable, on aboutit à une contradiction  
Donc  $f : \mathbb{N} \rightarrow \mathbb{N} \simeq \mathbb{N}$ . Donc il y a une infinité de fonction  
 $\mathbb{N} \rightarrow \mathbb{N}$  bien plus grande que l'infini de  $\mathbb{N}$ .

Bilan: On a vu que l'ensemble des MTs étaient dénombrables  
l'ensemble  $\mathbb{N} \rightarrow \mathbb{N}$  est non-dénombrable.

Donc il y a infinité plus de fonctions  $\mathbb{N} \rightarrow \mathbb{N}$  que de MT.

Donc il y a une infinité de fonctions non-calculables.

Aujourd'hui, l'objectif est de réduire l'étude des fonctions calculables.  
« existe-t'il une MT capable de calculer  $f(wd) = w_n \forall wd \in \Sigma^*$  »  
» à l'étude des relations décidables.

« exercice t'il une MT MR qui répond V si  $R(wd, w_n) = V$  ? »  
qui répond E si  $R(wd, w_n) = F$  »

Lemon

②

cm

Ensemble décidable

→ l'univers de tout les éléments

Un ensemble  $E \subseteq U$  peut être défini par un prédictor  $E_E^? : U \rightarrow \text{Bool}$  appelé test d'appartenance

$$E_E^?(u) = V \Leftrightarrow u \in E$$

$$E_E^?(u) = F \Leftrightarrow u \notin E$$

Un ensemble  $E$  est décidable si

- i)  $E \subseteq U$  et  $U$  enumerable
- ii) la fonction  $E_E^?$  est calculable

ie il existe une MTM qui réalise la fonction  $E_E^? : U \rightarrow \text{Bool}$

ie M termine pour toute entrée  $u \in U$

$$\cdot M(u) = V \Leftrightarrow M(u) \rightarrow^* \textcircled{O} \Leftrightarrow E_E^?(u) = V \Leftrightarrow u \in E$$

$$\cdot M(u) = F \Leftrightarrow M(u) \rightarrow^* \textcircled{X} \Leftrightarrow E_E^?(u) = F \Leftrightarrow u \notin E$$

Un ensemble est enumerable

- ① si  $U$  est denombrable (i.e.  $U \cong \mathbb{N}$ ) , en particulier il existe une

- ② fonction surjective

$$\text{get} : \mathbb{N} \rightarrow U$$

$$i \mapsto u_i$$

- ③ La fonction get doit être calculable.

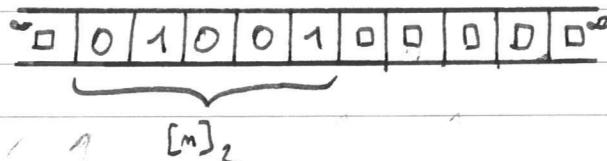
$$\exists M_{\text{get}} \text{ qui termine pour tout } u \in \mathbb{N}, \text{ et } M_{\text{get}}(u) = u \in U$$

Exercice :  $\Sigma = \{0, 1\}$ , montrons que  $\Sigma^*$  est enumerable.

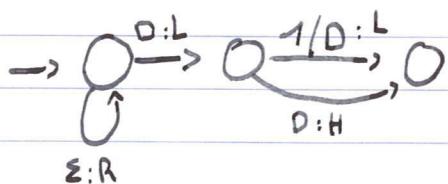
①  $\Sigma^*$  est-il denombrable ?  $\Sigma = \{0, 1\} \subseteq \mathbb{N}$  donc  $\Sigma^* \subseteq \mathbb{N}^*$  et  $\mathbb{N}^*$  est denombrable donc  $\Sigma^*$  aussi.

② Donnons une machine  $M_{\text{get}} : \mathbb{N} \rightarrow \Sigma^*$  qui réalise une fonction surjective.

Autrement dit, on doit pouvoir produire tout les mots binaires de  $\Sigma^*$  comme un résultat de  $M_{\text{get}}$  pour un certain entier.



Réaliser la fonction :  $[N]_2 \rightarrow \Sigma$

$$\begin{array}{l} w_1 \rightarrow w \\ 0 \rightarrow E \\ [16]_2 = 0001 \rightarrow 0000 \end{array}$$


Proposition : (équivalence entre calculabilité et décidabilité)

Une fonction  $f : \Sigma^* \rightarrow \Sigma^*$  est calculable

$\Leftrightarrow$

les relations  $R_f : \Sigma^* \times \Sigma^* \rightarrow \text{Bool}$  est décidable

Preuve : Montrons  $f$  calculable  $\Rightarrow R_f$  décidable.

On suppose

$\exists M_f$  qui termine pour toute entrée  $w_d \in \Sigma^*$

$$M_f(w_d) = V(w_n) \text{ si } f(w_d) = w_n$$

On doit construire une MT  $M_{R_f}$  qui décide  $R_f$

La relation  $R_f$  associée à  $f$  est définie ainsi :

$$R_f(w_d, w_n) = V \Leftrightarrow f(w_d) = w_n$$

$$R_f(w_d, w') = E \Leftrightarrow f(w_d) \neq w'$$

On doit construire - à partir de  $M_f$  - une MT  $M_{R_f}$  qui :

- termine pour toute entrée de  $\Sigma^* \times \Sigma^*$

- Dans l'état  $\oplus$  si  $R_f(w_d, w_n) = V$  (ie  $f(w_d) = w_n$ )

- Dans l'état  $\ominus$  si  $R_f(w_d, w_n) = E$  (ie  $f(w_d) \neq w_n$ )

$$M_{R_f}(w_d, w_n) = \begin{array}{|c|c|c|} \hline B_1 & \overset{\infty D}{\overbrace{\square}} & w_d & \overset{\infty \square}{\overbrace{\square}} & \rightarrow & \overset{\infty \square}{\overbrace{\square}} & w_R & \overset{\infty \square}{\overbrace{\square}} \\ \hline \end{array} \xrightarrow{\uparrow M_{eq}}$$

$$B_2 = \begin{array}{|c|c|c|} \hline \overset{\infty \square}{\overbrace{\square}} & w_n & \overset{\infty \square}{\overbrace{\square}} \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline \overset{\infty \square}{\overbrace{\square}} & w'_R & \overset{\infty \square}{\overbrace{\square}} \\ \hline \end{array}$$

$$M_{R_f}(w_d, w'_R) = [B_1 := w_d ; B_2 := w'_R ; M_f(B_1) ; M_{eq}(B_1, B_2)]$$