

Exercice 1 : Formalisation et Théorème de Rice

On note \mathcal{M} l'ensemble des codages binaires de machines de Turing.

Q1. Complétez : Un ensemble de machines de Turing est un ensemble de Rice s'il s'écrit $\{m \in \mathcal{M} \mid \mathcal{C}(\mathcal{L}(u(m)))\}$ où la condition \mathcal{C} porte sur le langage reconnu par m

Q2. Complétez : Tout ensemble de Rice non-trivial, c'est-à-dire différent de \emptyset et de \mathcal{M} , est indécidable.

Q3. Formalisez en termes mathématiques les ensemble suivants

1. L'ensemble des machines de Turing qui n'acceptent pas, en tant que mot, leur codage en binaire :
 $L_1 = \{m \in \mathcal{M} \mid \mathcal{L}(u(m)) \neq u(m)\}$

2. L'ensemble des machines de Turing dont l'exécution sans paramètre est infinie :
 $L_2 = \{m \in \mathcal{M} \mid \mathcal{L}(u(m)) \text{ infini}\}$

3. L'ensemble des machines de Turing qui acceptent tous les mots binaires :
 $L_3 = \{m \in \mathcal{M} \mid \mathcal{L}(u(m)) = \{0,1\}^*\}$

4. L'ensemble des machines de Turing équivalentes à la MT M_\emptyset qui reconnaît le langage vide :
 $L_4 = \{m \in \mathcal{M} \mid \mathcal{L}(u(m)) = \emptyset\}$

5. L'ensemble des MT qui rejettent le mot binaire ϵ (c'est-à-dire s'arrêtent dans l'état \otimes)
 $L_5 = \{m \in \mathcal{M} \mid \mathcal{L}(u(m))(\epsilon) \rightarrow \otimes\}$

Q4. Parmi les ensembles L_1 à L_5 certains sont des ensembles de Rice. Lesquels ? Rédigez votre réponse de la manière suivante en définissant la condition de Rice, \mathcal{C} , correspondant à l'ensemble.

Indication : ... est un ensemble de Rice car il peut s'écrire $\{m \in \mathcal{M} \mid \mathcal{C}(\mathcal{L}(u(m)))\}$ avec

$$\mathcal{C}(L) \stackrel{\text{def}}{=} \dots$$

Q5. Expliquez pourquoi les autres ensembles ne sont pas un ensemble de Rice.

Q6. Si un ensemble L n'est pas un ensemble de Rice, que peut-on en déduire ?

Exercice 2 : Pourquoi faut-il une équivalence (\Leftrightarrow) dans une réduction ?

$$\begin{array}{ccc} \omega \in \Sigma^* & \xrightarrow[\text{traduction}]{M_R} & R(\omega) = \omega' \in \Sigma'^* \\ \omega \in L & \Leftrightarrow_{(\Leftrightarrow)} & R(\omega) \in L' \end{array}$$

Q7. Supposons que le diagramme exige seulement une implication (\Rightarrow)

$$\omega \in L \Rightarrow R(\omega) \in L'.$$

Donnez un langage L' reconnaissable qui satisfait l'implication et ne donne aucune information sur L .

Q8. Supposons que le diagramme exige seulement une implication (\Leftarrow)

$$\omega \in L \Leftarrow_{(\Leftarrow)} R(\omega) \in L'$$

Donnez un langage L' reconnaissable qui satisfait l'implication et ne donne aucune information sur L .

Exercice 3 : Diagramme de réduction complémentaire

Étant donné un diagramme de réduction de $\overset{?}{L}$ à $\overset{?}{L}'$. Démontrez que le même diagramme de réduction est valable pour les langages complémentaires. Autrement dit c'est aussi un diagramme de réduction de $\overset{?}{\overline{L}}$ à $\overset{?}{\overline{L}'}$.

Q9. Complétez

$$\begin{array}{ccc} \omega \in \Sigma^* & \xrightarrow[\text{traduction}]{M_R} & R(\omega) = \omega' \in \Sigma'^* \\ \omega \in L & \xrightleftharpoons[\text{(\Leftrightarrow)}]{\quad} & R(\omega) \in L' \\ \omega \in \overline{L} & \xrightarrow[\text{(\Rightarrow)}]{\quad} & R(\omega) \in \overline{L'} \end{array}$$

Q11. Que faut-il montrer ?

Q11. Rédigez la preuve (simple) en 4 lignes

Exercice 4 : Indécidabilité en combinant Rice et Réduction

À l'aide d'un raisonnement par contradiction utilisant l'exemple \mathcal{P}_ϵ d'application du théorème de Rice (avec $\omega = \epsilon$), montrez que « l'ensemble L des machines de Turing dont l'exécution sans paramètre s'arrête » est indécidable.

Q12. Donnez la définition mathématique de L .

Q13. L correspond-t'il à un ensemble de Rice \mathcal{P}_ϵ ? si oui, donnez la condition $\mathcal{C} : \mathcal{L} \rightarrow \text{Bool}$, sinon expliquez pourquoi.

Preuve d'indécidabilité par réduction de \mathcal{P} à L .

Q14. Montrez que l'ensemble $\mathcal{P}_\epsilon \stackrel{\text{def}}{=} \{m \in \mathcal{M} \mid U(m)(\epsilon) \rightarrow \otimes\}$ est indécidable

Q15. Donnez une MT M_∞ qui ne termine jamais quel que soit le ruban.

Démontrons que L est indécidable par réduction de l'ensemble \mathcal{P}_ϵ à L

On considère la transformation R définie par $R(m)(...) \stackrel{\text{def}}{=} [\text{if } U(m)(...) \text{ then } \rightarrow \otimes \text{ else } M_\infty]$

$$\xrightarrow[\text{(\Rightarrow)}]{\quad} \dots \dots \dots$$

Q16. Complétez le diagramme de réduction $\xrightarrow[\text{traduction}]{M_R}$
 $m \in \mathcal{P}_\epsilon \quad \dots \dots \quad \in L$

Q17. Si le diagramme de réduction est correct, que peut-on en conclure ?

- Q18. Que reste-t'il à montrer pour avoir le droit d'appliquer la réduction ?
- Q19. Rédiger la preuve de (\Rightarrow) en commençant par expliciter ce qu'on doit montrer.
- Q20. Rédiger la preuve de (\Leftarrow) en commençant par expliciter ce qu'on doit montrer.

Exercice 5 : Indécidabilité de l'équivalence de machines de Turing

Le théorème de Rice permet de montrer qu'il n'existe pas de MT (*i.e.* de programme) capable de dire si deux MTS (ou programmes) fournis en paramètre sont équivalents (*c'est-à-dire* qu'ils retournent le même résultat sur toutes les entrées possibles).

- Q21. Complétez (répondez sur votre copie). Deux MT M_1 et M_2 sont équivalentes si et seulement si

- Q22. Étant donnée une MT M' , montrez, à l'aide du théorème de Rice, que l'ensemble $\mathcal{P} \stackrel{\text{def}}{=} \{m \mid U(m) \equiv M'\}$ des machines de Turing équivalentes à M' est indécidable.

Exercice 6 :

Soit \bar{L} un langage indécidable. Appliquez les définitions du cours afin de montrer que L est indécidable.

^{cm} Rappel: Diagramme de réduction de $E^?L$ à $E^?L'$

$$w \in \Sigma^* \xrightarrow[\text{introduction}]{M_0} R(w) \in \Sigma'^*$$

$$w \in E^?L \stackrel{(\#)}{\iff} R(w) \in E^?L'$$

L reconnaissable $\Leftarrow L'$ reconnaissable

\overline{L} reconnaissable $\Leftarrow \overline{L}'$ reconnaissable

L décidable $\Leftarrow L'$ décidable

L non-reconnaissable $\Rightarrow L'$ non-reconnaissable

L indécidable $\Rightarrow L'$ indécidable

Théorème de Rice et MT équivalentes

Définition: 2 MT équivalentes, notées M_1 et M_2 , $M_1 \equiv M_2$
 si $\mathcal{L}(M_1) = \mathcal{L}(M_2)$
 i.e., elles reconnaissent le même langage

Proposition: Considérons un ensemble de Rice

$$P_c = \{m \in M \mid C(\mathcal{L}(U(m)))\}$$

si m_1 et m_2 sont deux codages binaires de $[M_1]_2$ et $[M_2]_2$ équivalentes.

$$\text{i.e. } [M_1 \equiv M_2], [U(m_1) = U(m_2)] \text{ (hypothèse)}$$

alors $m_1 \in P_c \stackrel{?}{\iff} m_2 \in P_c$

Preuve en appliquant les définitions.

Considérons un ensemble de Rice P_c et montrons qu'il est indécidable par réduction de $E^?L_{EF}$ à $E^?P_c$
 indécidable \Rightarrow indécidable

Rappel on a déjà montré que L_{EF} est indécidable

$$L_{EF} = \{(m, w) \mid U(m)(w) \not\rightarrow \infty\}$$

L_{EF} est indécidable car $\overline{L_{EF}}$ est non-reconnaissable

On considère P_c non-trivial $P_c \neq M, P_c \neq \emptyset$ donc

$\exists m_1 \in P_c$ (sinon P_c serait \emptyset)

$\exists m_2 \notin P_c$ (sinon P_c serait M)

- On note $M_\phi = \rightarrow \otimes$ la MT qui reconnaît le langage $\{\}$
 et on note $m_\phi = [M_\phi]_2$ son codage binaire

- La preuve distingue 2 cas :
 - (cas 1) $m_\phi \notin P_C$
 - (cas 2) $m_\phi \in P_C$

Diagramme de reduction de $E^?$ Lef à $E^?P_C$

$$(m, w) \in {}^?L_{ef} \iff_{(\neq)} R(m, w) \in {}^?P_C$$

Pour avoir une réduction, il faut :

- 1) Définir la traduction R
 - 2) Montrez qu'on peut la réaliser par un MT MR (qui termine toujours)
 - 3) montrez l'équivalence (\neq)

On en conclut que $\mathcal{E}P_c$ est indécidable car $\mathcal{E}^?L_{\text{EF}}$ est indécidable.

$$\boxed{\begin{array}{l} M_R(m, w) \\ R(m, w) \in M \end{array}} \quad (w_1) \quad \stackrel{\text{def}}{=} \quad \left[\begin{array}{l} \text{if } M(m)(w) \rightarrow \infty \text{ then } U(m_1)(w_1) \\ \text{else } U(m_1)(w_1) \end{array} \right]_2$$

- ③ Preuve de l'équivalence (en 2 temps \Rightarrow puis \Leftarrow)
 Montrons que $(m, w) \in L_{GF} \Rightarrow R(m, w) \in P_C$

on fait l'hypothèse (hyp) que $(m, w) \in L_{EF}$ et on doit montrer que $R(m, w) \in \mathbb{A} \cdot P_C$

Technique de preuve | si $\mathcal{L}(R(m, w)) = \mathcal{L}(\ ?_m \ ?)$
 alors $R(m, w) \in P_C \Leftrightarrow ?_m \ ? \in P_C$

On cherche à déterminer $L(R(m, w))$?

D'après l'hypothèse $(m, w) \in L_{\text{cc}}$ donc $U(m)(w) \rightarrow \infty$

Que dire de l'exécution de $R(m)(w) = \frac{\text{perdu temps}}{fini à exécuter} ; M(m_1)(w_1)$

si m_1 accepte w_1 alors $R(m)(w)$ aussi.

Si m n'accepte pas w , alors $R(m)(w)$ non plus.

se

$$\text{cm} \quad \text{Donc } L(R(m)(w)) = L(U(m_1))$$

Par conséquent, puisque les MT reconnaissent le même langage,
 $\underbrace{R(m, w) \in P_c}_{\text{CQFD}} \Leftrightarrow \underbrace{m_1 \in P_c}_{\text{notre hypothèse car } P_c \text{ non-trivial}}$

Deuxième partie de l'équivalence

On doit montrer que $R(m, w) \in P_c \stackrel{?}{\Rightarrow} (m, w) \in L_{EF}$

On doit montrer la contreposée (qui est équivalente) $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$
 i.e. $(m, w) \notin L_{EF} \stackrel{?}{\Rightarrow} R(m, w) \notin P_c$

On fait l'hypothèse (HYP) que $(m, w) \notin L_{EF}$
 et on doit montrer que $R(m, w) \notin P_c$

Pour hyp $(m, w) \notin L_{EF}$ i.e. $U(m)(w) \rightarrow \infty$

Regardons l'exécution de $R(m, w)$ sur un mot w_1 ,

$$\boxed{R(m, w)}(w_1) = U(m, w)$$

et donc $R(m, w)(w_1) \rightarrow \infty$ quand quel que soit w_1

mais alors $L(R(m, w)) : \{\} = L(U(m_\phi))$ où $m_\phi = \boxed{\rightarrow \otimes}_2$

et puisque $R(m, w)$ et m_ϕ reconnaissent le même langage.

$$\underbrace{R(m, w) \notin P_c}_{\text{CQFD}} \Leftrightarrow \underbrace{m_\phi \in P_c}_{\text{}}$$

Dans le cas 1 de la preuve on a supposé
 $m_\phi \in P_c$

$$\underline{\text{cas 1}} \quad \exists m_1 \in P_c \\ m_\phi \notin P_c$$

$$\underline{\text{cas 2}} \quad \exists m_2 \notin P_c \\ m_\phi \in P_c$$

$$\frac{m_2 \in P_c}{m_\phi \notin P_c}$$

TD Théorème de Rice & Preuve par déduction (2 TD)

q4 - L_3 est un ensemble de Rice car il peut s'écrire $\{m \in M \mid C(L(U(m)))\}$ avec $C(L) \stackrel{\text{def}}{=} L = \{0,1\}^*$

L_4 est un ensemble de Rice car il peut s'écrire $\{m \in M \mid C(L(U(m)))\}$ avec $C(L) \stackrel{\text{def}}{=} L = \emptyset$

q5 - L_1 n'est pas un ensemble de Rice car $m \notin L(U(m))$ n'est pas une bonne condition
 $w \in L(M)$ si $M(w) \rightarrow \emptyset$; $w \notin L(M) \Leftrightarrow M(w) \sim \emptyset$ ou $M(w) \rightarrow \infty$

$$\begin{aligned} P_E &= \{m \in M \mid E \notin L(U(m))\} \\ &= \{m \in M \mid U(m)(E) \not\rightarrow \emptyset\} \\ &= \{m \in M \mid U(m)(E) \rightarrow \emptyset \vee U(m)(E) \rightarrow \infty\} \\ &= L_2 \cup L_3 \Rightarrow \text{ce ne sont pas des ensembles de Rice.} \end{aligned}$$

q6 - Un ensemble de Rice est décidable, mais tout les ~~déterminés~~ ensembles décidables
ne sont pas des ensembles de Rice.

Si un ensemble n'est pas de Rice, on ne peut donc rien dire.

Exercice 2.

q7 - Σ^*

q8 - \emptyset

Exercice 3.

q9 - $w \in \Sigma^* \xrightarrow[\text{réduction}]{M_R} R(w) = w' \in \Sigma^{*\prime}$
 $w \in L \Leftrightarrow R(w) \in L'$
 $w \in \overline{\Sigma^*} \xrightarrow[\text{définition}]{M_R} R(w) \in \overline{\Sigma^{*\prime}}$

q10 - $w \in \overline{L} \Leftrightarrow R(w) \in \overline{L'}$

q11 - On sait que $w \in L \Leftrightarrow R(w) \in L'$
on 1) $w \notin L \Leftrightarrow w \in \overline{L}$ et 2) $R(w) \notin L' \Leftrightarrow R(w) \in \overline{L'}$
 $w \in L \Leftrightarrow R(w) \in L$
 $\Leftrightarrow w \notin L \Leftrightarrow R(w) \notin L$
 $\Leftrightarrow w \in \overline{L} \Leftrightarrow R(w) \in \overline{L'}$

Exercice 4-

q₁₂ - $\{m \in M \mid U(m)(\varepsilon) \rightarrow ?\}$

q₁₃ - Von can le predicat c serait trivial

q₁₄ - $P_C \stackrel{\text{def}}{=} \{m \in M \mid U(m)(\varepsilon) \rightarrow \emptyset\}$

q₁₅ - $\rightarrow Q$

$\Sigma \setminus \Sigma : R$

avec $\Sigma = \Sigma \cup \{\Box\}$

q₁₆ -

05/03/2018

TURING

1 1^{er} Théorème de Rice & Applications

Définition : Un sous-ensemble de M est appelé un ensemble de Rice si il s'écrit

$$\{m \in M \mid C(\underbrace{\mathcal{L}(\mathcal{L}(U(m)))}_{\text{langage reconnu}})\}$$

par m .

où la condition C est un prédictat non-trivial sur les langages

$$C: \mathcal{L} \rightarrow \text{Bool}.$$

C est non-trivial si C n'est pas vrai tout le temps.

$$\textcircled{1} C \neq V \wedge L$$

$$\textcircled{2} C \neq F \wedge L$$

$$\textcircled{3} \{m \in M \mid F\} = \{\} = \mathcal{L}$$

$$\textcircled{4} P_C = \{m \in M \mid V\} = \mathcal{L}$$

Des exemples de condition de rice

$$C: \mathcal{L} \rightarrow \text{Bool}$$

$$C(L) \stackrel{\text{def}}{=} (L = \{\})$$

$$C(L) \stackrel{\text{def}}{=} 101 \in L$$

$$C(L) \stackrel{\text{def}}{=} |L| \in \mathbb{N}$$

$$C(L) \stackrel{\text{def}}{=} L = ? \mathcal{L}(M_{\text{foo}})$$

le langage est-il vide

le mot 101 appartient au langage

le langage est-il finit

est-ce le langage de la machine M_{foo}

Remarque : si m est le codage binaire de M qui représente

$$\underbrace{\mathcal{L}(U(m))}_M = \mathcal{L}(M)$$

Si C est une condition non-triviale sur les langages alors l'appartenance à l'ensemble

$$\{m \in M \mid C(\mathcal{L}(U(m)))\}$$

est indécidable.

Autrement dit, toute condition non-triviale sur le langage reconnu par une MT est indécidable.

Applications

$$P_{101} = \{m \in M \mid U(m)(101) \rightarrow \textcircled{3}\}$$

$$101 \in \mathcal{L}(U(m))$$

$$C_{101}(\mathcal{L}(U(m)))$$

$$P = \{ m \in M \mid \forall w \in \Sigma^*, L(m)(w) \not\rightarrow \textcircled{0} \}$$

$$\forall w \in \Sigma^* \quad w \notin L(U(m))$$

$$L(U(m)) = \{\} \quad \text{...}$$

$$C \neq L(L(U(m)))$$

Principe de réduction

Un diagramme de réduction permet de réduire la question difficile de l'appartenance à un langage L' plus simple

* : à un langage
 $L \subseteq \Sigma^*$ la question
 de l'appartenance

On utilise une traduction

$$\begin{array}{ccc} w \in \Sigma^* & \xrightarrow[\text{réduction}]{M_R} & R(w) = w' \in \Sigma'^* \\ w \in L & \longleftrightarrow & R(w) \in L' \end{array}$$

Pour avoir une réduction, il faut respecter 2 conditions.

1) La traduction R doit être réalisable par une MT M_R
 i.e. la machine M_R termine $\forall w \in \Sigma^*$

2) il faut démontrer l'équivalence

Proposition: Le diagramme précédent permet de conclure

- (i) L reconnaissable $\iff L'$ est reconnaissable
- (ii) L non reconnaissable $\Rightarrow L'$ non-reconnaissable
- (iii)
- (iv)
- (v)

preuve (i) pour démontrer (\Leftarrow),

On suppose L' reconnaissable

i.e. $\exists M'$ telle que $M'(w') \rightarrow \textcircled{0} \iff w \in L'$

On doit montrer L est reconnaissable

i.e. $\exists M$ telle que $M(w) \rightarrow \textcircled{0} \iff w \in L$

Il existe c'est $M \stackrel{\text{def}}{=} [M_R; M']$

en effet, $M(w) \rightarrow \textcircled{0} \iff w \in L$

$$\underbrace{w \xrightarrow{M_R} R(w) \xrightarrow{M'} \textcircled{0}}_{M'(R(w)) \rightarrow \textcircled{0}} \quad \begin{matrix} \uparrow (\#) \\ R(w) \in L' \end{matrix}$$

$$\stackrel{\text{def}}{=} R(w) \in L(M')$$

05/03/2018

TURING

2 CM

(ii) Appliquons le principe de réduction pour montrer que l'ensemble $\overline{L_{\text{TF}}}$ n'est pas reconnaissable

$$\overline{L_{\text{TF}}} = \{ m \in M \mid \forall w \in \Sigma^*, U(m)(w) \not\rightarrow \infty \}$$

$$\begin{aligned} \overline{L_{\text{TF}}} &= M \setminus L_{\text{TF}} \\ &= \{ m \in M \mid \exists w \in \Sigma^*, U(m)(w) \rightarrow \infty \} \end{aligned}$$

On montre $\overline{L_{\text{TF}}}$ non-reconnaissable par une réduction de $E \overline{L_{\text{EF}}} \rightsquigarrow E? \overline{L_{\text{TF}}}$
non-reconnaissable.

Diagramme de réduction

Rappel

$$\begin{aligned} \overline{L_{\text{EF}}} &= M \times \Sigma^* \setminus L_{\text{EF}} \\ &= \{ (m, w) \mid U(m)(w) \rightarrow \infty \} \\ (m, w) \in M \times \Sigma^* &\xrightarrow{M_R} R(m, w) = m \in M \end{aligned}$$

$$(m, w) \in \overline{L_{\text{EF}}} \iff R(m, w) = m \in \overline{L_{\text{TF}}}$$

$\exists w'$ tel que
 $U(m')(w') \rightarrow \infty$

1) pour la traduction M_R : notons $w = s_1 \dots s_m$

$$m' = M_R(m, w) = [M_{\text{eff}}, O^{0/s_1:R} O \dots O^{0/s_m:R}, M]_2, m$$

$$U(m')(w') \quad \left. \begin{array}{c} B_1 \quad \overbrace{s_1 s_2 \dots s_m}^w \\ B_2 \quad \dots \quad m \quad \dots \end{array} \right\} \rightarrow \infty$$

Pour obtenir le mot m décrivant M on fait précéder la séquence des transitions de l'état initial suivi du symbole \$. on obtient alors le mot¹

suivi du symbole \$, on obtient alors le mot

$(Q;1) \$ (Q;1) 0 1 R (Q;1) (Q;1) 1 0 H (A;10)$

Codage binaire de Σ_U

$L \mapsto$	<table border="1"><tr><td>1</td><td>1</td><td>0</td><td>0</td></tr></table>	1	1	0	0	$0 \mapsto$	<table border="1"><tr><td>0</td><td>0</td><td>0</td><td>0</td></tr></table>	0	0	0	0
1	1	0	0								
0	0	0	0								
$H \mapsto$	<table border="1"><tr><td>0</td><td>1</td><td>1</td><td>0</td></tr></table>	0	1	1	0	$1 \mapsto$	<table border="1"><tr><td>1</td><td>1</td><td>1</td><td>1</td></tr></table>	1	1	1	1
0	1	1	0								
1	1	1	1								
$R \mapsto$	<table border="1"><tr><td>0</td><td>0</td><td>1</td><td>1</td></tr></table>	0	0	1	1	$(\mapsto$	<table border="1"><tr><td>1</td><td>0</td><td>0</td><td>0</td></tr></table>	1	0	0	0
0	0	1	1								
1	0	0	0								
$Q \mapsto$	<table border="1"><tr><td>1</td><td>1</td><td>1</td><td>0</td></tr></table>	1	1	1	0	$: \mapsto$	<table border="1"><tr><td>0</td><td>1</td><td>0</td><td>0</td></tr></table>	0	1	0	0
1	1	1	0								
0	1	0	0								
$A \mapsto$	<table border="1"><tr><td>0</td><td>1</td><td>1</td><td>1</td></tr></table>	0	1	1	1	$) \mapsto$	<table border="1"><tr><td>0</td><td>0</td><td>1</td><td>0</td></tr></table>	0	0	1	0
0	1	1	1								
0	0	1	0								
$E \mapsto$	<table border="1"><tr><td>1</td><td>1</td><td>0</td><td>1</td></tr></table>	1	1	0	1	$\$ \mapsto$	<table border="1"><tr><td>0</td><td>0</td><td>0</td><td>1</td></tr></table>	0	0	0	1
1	1	0	1								
0	0	0	1								

Finalement,

$$m = [M]_2 = \begin{array}{ccccccccc} & \boxed{1\ 0\ 0\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 0} & \cdot & \boxed{0\ 1\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 1} & \cdot & \boxed{0\ 0\ 1\ 0} & \cdot & \boxed{\dots\ 0\ 0\ 0\ 1} \\ & \boxed{0\ 0\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 1} & \cdot & \boxed{0\ 0\ 1\ 1} & & & & & & \underbrace{\hspace{1cm}}_{\$} \\ & \boxed{1\ 0\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 0} & \cdot & \boxed{0\ 1\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 1} & \cdot & \boxed{0\ 0\ 1\ 0} & & \\ & \boxed{1\ 0\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 0} & \cdot & \boxed{0\ 1\ 0\ 0} & \cdot & \boxed{1\ 1\ 1\ 1} & \cdot & \boxed{0\ 0\ 1\ 0} & & \\ & \boxed{1\ 1\ 1\ 1} & \cdot & \boxed{0\ 0\ 0\ 0} & \cdot & \boxed{0\ 1\ 1\ 0} & & & & & & \\ & \boxed{1000} & \cdot & \boxed{0111} & \cdot & \boxed{0100} & \cdot & \boxed{1111} & \cdot & \boxed{0000} & \cdot & \boxed{0010} \\ & (& A & : & & & & 1 & \leftarrow & 0 &) \end{array}$$

Définition 1 (*codage binaire des machine de Turing*) On note $\mathcal{M} = \{m \in \{0, 1\}^* \mid m = [M]_2, M \in \text{MT}\}$ l'ensemble des mots binaires qui correspondent à des MT sur l'alphabet $\{0, 1\}$.

Remarque : Si on lance l'exécution de U sur un couple (m, ω) où $m \notin \mathcal{M}$, c'est-à-dire lorsque m ne correspond pas à codage valide de MT alors le comportement de U est imprévisible. Néanmoins il est possible d'étendre la MT U pour qu'une première phase vérifie si le mot m correspond bien à un codage de MT.

Exercice 4 : Fonctionnement de la machine de Turing universelle

On définit la MT U comme une machine à deux bandes. L'exécution de $U(m)(\omega)$ doit simuler l'exécution de M sur le mot ω .

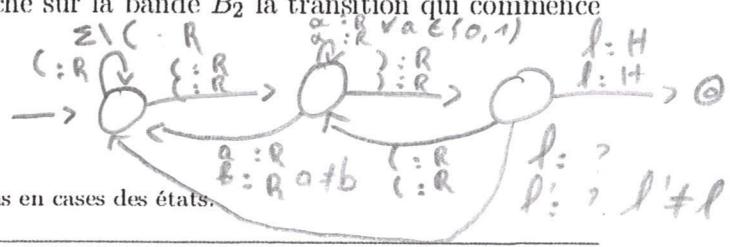
- La bande B_2 contient le mot m correspondant à la représentation binaire de M , cf. § Exercice 3;
 - La bande B_1 contiendra la configuration courante de M ie. $(\omega_L, \mathbf{q}, \ell, \omega_R)$ où ω_L est la partie du ruban de M située à gauche de T_M (la tête de M), ℓ est le symbole courant sur lequel pointe T_M , et ω_R est la partie du ruban située à droite de T_M . On représente la configuration $(\omega_L, \mathbf{q}, \ell, \omega_R)$ de la manière suivante sur la bande B_1 où l'état $\mathbf{q} = (t : n)$ avec $t \in \{\text{A, E, Q}\}$ est le statut de l'état, $n \in \mathbb{N}$ son numéro d'état et $[n]_2$ la représentation binaire de n .

$$B_1 = \overline{\omega_L \mid (\mid t \mid : \mid [n]_2 \mid) \mid \ell \mid \omega_R \mid}^\infty$$

\uparrow
 T_M

Par souci de lisibilité on désignera désormais par $((q_n))$ un état $((t : [n]_2))$

Q1. Donnez une MT à 2 bandes M_{match} qui recherche sur la bande B_2 la transition qui commence par le motif $(q)\ell$ de la configuration courante de B_1 .



1. Pour rester lisible, on ne fait pas apparaître les séparations en cases des états

$$\begin{aligned}
 \mathcal{L}(M_C) &= \{\omega \mid \dots \dots \dots \} \text{ par définition du langage reconnu par une MT} \\
 &= \{\omega \mid M_{\overline{EF}}(\omega, \omega) = \text{Acc}\} \text{ par définition de } M_C \\
 &= \{\omega \mid \dots \dots \in \overline{L_{EF}}\} \text{ par définition du langage reconnu par une MT} \\
 &\quad \text{donc } \omega \text{ n'est pas un mot quelconque de } \{0, 1\}^* \text{ mais un élément de } M \\
 &= \{m \in M \mid (m, m) \in \dots \dots \} \\
 &= \{m \in M \mid U(m)(m) \dots \dots \} \text{ par définition de } \overline{L_{EF}} \\
 \mathcal{L}(M_C) &= \{m \in M \mid m = \dots \dots, M(m) \rightarrow \infty\} \text{ par définition de la} \\
 &\quad \dots \dots \dots
 \end{aligned}$$

Noir page précédente

$\mathcal{L}(M_C)$ est donc l'ensemble des mots binaires de M qui correspondent à des MT qui ne s'arrêtent pas lorsqu'on les exécute sur leur binaire.

Exhibons la contradiction : Considérons maintenant m_c le codage binaire de la MT M_C que l'on vient de construire. On peut alors se demander si m_c appartient à $\mathcal{L}(M_C)$?

$$\begin{aligned}
 m_c \in \mathcal{L}(M_C) &\iff m_c \in \{m \in M \mid m = [M]_2, M(m) \rightarrow \infty\} \text{ par définition de } \mathcal{L}(M_C) \\
 &\iff \dots \dots \rightarrow \infty \text{ puisque } m_c = [M_c]_2
 \end{aligned}$$

Ainsi, (†) $m_c \in \mathcal{L}(M_C) \iff M_C(m_c) \rightarrow \infty$

Par ailleurs, par définition du langage par une MT, on a aussi l'équivalence :

$$(‡) m_c \in \mathcal{L}(M_C) \iff M_C(m_c) = \text{Acc} \iff M_C(m_c) \rightarrow^* \text{ } \textcircled{O}$$

Les équivalences (†) et (‡) donnent la CONTRADICTION cherchée puisque l'exécution $M_C(m_c)$ est censée terminer (dans l'état \textcircled{O}) d'après (‡), et ne pas terminer d'après (†).

Conclusion : En supposant qu'il existait une MT qui reconnaît $\overline{L_{EF}}$ nous aboutissons à une contradiction ; donc $\overline{L_{EF}}$ n'est pas reconnaissable, ce qui termine la preuve de (ii). Le langage L_{EF} est donc indécidable.

□

Exercice 3 : Représentation binaire d'une machine de Turing

Considérons une MT $M = (\Sigma, \mathcal{Q}, q_i, \delta, \mathcal{A}cc, \mathcal{E}rr)$ avec $\Sigma = \{0, 1\}$.

Pour coder cette représentation de M sur le ruban on va considérer un alphabet à 12 symboles $\Sigma_U = \Sigma \cup \{\Lambda, E, Q, (, :,), L, H, R, \$\}$ contenant les symboles de Σ et enrichi de nouveaux symboles :

$\Lambda, E, Q, (, :,)$ afin de représenter les états quelconques par Q, accepteur par Λ , erreur par E.

Exemples :

- l'état $\textcircled{5}$ sera représenté par $(\Lambda : 101)$ ce qui donne $\overbrace{\infty \square | (\boxed{\Lambda} : 1 \ 0 \ 1)}^{\infty} \square \infty$ sur le ruban
- l'état \textcircled{X} sera représenté par $(E : 0)$
- l'état $\textcircled{2}$ sera représenté par $(Q : 01)$.

-- L, H, R afin de représenter les déplacements $d \in \{L, H, R\}$ de la tête lors des transitions.

Exemple : La transition $\textcircled{1} \xrightarrow{\ell/e:d} \textcircled{2}$ avec $\ell, e \in \Sigma$ sera représentée sur le ruban par

$(\boxed{Q} : 1) | \ell \ e \ d | (\boxed{\Lambda} : \boxed{01} \ \boxed{10})$

-- Les transitions sont inscrites les unes derrière les autres. La séparation entre transitions est indiquée par la succession des cases $\boxed{} \boxed{}$.

Exemple : La MT $\xrightarrow{\quad} \textcircled{1} \xrightarrow{0/1:R} \textcircled{2} \xrightarrow{1/0:H} \textcircled{1}$ sera représentée par la séquence de transitions $(Q:1) 0 \ 1 \ R (Q:1) \dots (Q:1) 1 \ 0 \ H (\Lambda:0 \ 1 \ 0 \ 0)$

MCAL/MT - Indécidabilité - Complétez les preuves (0.5 TD)

Exercice 1 : Indécidabilité : premier exemple, preuve directe

Proposition 1 (Le langage universel n'est pas décidable) *Le langage universel L_U est l'ensemble défini par*

$$L_U = \{(m, \omega) \in \mathcal{M} \times \{0, 1\}^* \mid m = [M]_2, M(\omega) = \mathbb{V}\}$$

C'est l'ensemble des couples (m, ω) tels que la ~~machine~~ m accepte le ~~mot~~ ... ω .

- (i) L_U est ~~recursivement~~ ~~enumérable~~..... , ie. reconnaissable par une MT
- (ii) L_U n'est pas ~~cpt~~ -récursivement énumérable, ie. $\overline{L_U}$ n'est pas reconnaissable par une MT
- (iii) L_U n'est pas décidable.

Preuve :

- (i) On doit montrer qu'il existe une MT qui reconnaît L_U : la MT cherchée c'est U . En effet,

$$\mathcal{L}(U) \stackrel{\text{def}}{=} \{(m, \omega) \mid U(m, \omega) = \mathbb{V}\} \text{ par définition du langage reconnu par une MT.}$$

$$\text{or } U(m, \omega) = U(m)(\omega) = M(\omega) \text{ avec } m = [M]_2 \text{ par définition de la } U$$

$$\text{donc } \mathcal{L}(U) = \{(m, \omega) \mid M(\omega) = \mathbb{V}, m = [M]_2\} \stackrel{\text{def}}{=} L_U \text{ d'après la définition de } L_U.$$

Conclusion : $\mathcal{L}(U) = L_U$ ce qui signifie que la machine ~~universelle~~ U reconnaît le langage ~~universel~~ ... L_U .

- (ii) On va montrer par ~~contradiction~~ qu'il n'existe pas de MT qui ~~reconnaît~~ ... $\overline{L_U}$.

Que représente $\overline{L_U} \stackrel{\text{def}}{=} (\mathcal{M} \times \{0, 1\}^*) \setminus L_U$? Les éléments de $\overline{L_U}$ sont les couples (m, ω) que la machine universelle U n'accepte pas.

$$\overline{L_U} = \{(m, \omega) \in \mathcal{M} \times \{0, 1\}^* \mid U(m)(\omega) \neq \mathbb{V}\}$$

Preuve de (ii) par contradiction : SUPPOSONS qu'il une MT $M_{\overline{L_U}}$ qui recon-

naisse $\overline{L_U}$. On peut l'utiliser pour construire une MT $M_C(\omega) \stackrel{\text{def}}{=} M_{\overline{L_U}}(\omega, \omega)$ qui duplique le mot binaire ω pour en faire un couple et exécute $M_{\overline{L_U}}$ sur ce couple.

$$\begin{aligned} \mathcal{L}(M_C) &= \{\omega \mid M_C(\omega) = \mathbb{V}\} \quad \text{par définition du langage par une MT} \\ &= \{\omega \mid M_{\overline{L_U}}(\omega, \omega) = \mathbb{V}\} \quad \text{par définition de } M_C \\ &= \{\omega \mid (\omega, \omega) \in \overline{L_U}\} \quad \text{par définition du langage reconnu par} \\ &\quad \text{donc } \omega \text{ n'est pas un mot quelconque de } \{0, 1\}^* \text{ mais un élément de } \mathcal{M} \\ &= \{m \in \dots \mid (m, m) \in \overline{L_U}\} \\ &= \{m \in \dots \mid U(m)(m) \neq \mathbb{V}\} \quad \text{par définition de } \overline{L_U} \\ \mathcal{L}(M_C) &= \{m \in \dots \mid m = [M]_2, M(m) \neq \mathbb{V}\} \quad \text{par définition de la universelle} \end{aligned}$$

$\mathcal{L}(M_C)$ est donc l'ensemble des mots binaires de \mathcal{M} qui correspondent à *des MT qui n'accepte pas, en tant que, leur binaire, ie. $M(m) \rightarrow^* \mathbb{X} \vee M(m) \rightarrow^\infty$* .

Exhibons la contradiction : Considérons maintenant m_c le codage binaire de la MT M_C que l'on vient de

On peut alors se demander si m_c appartient à $\mathcal{L}(M_C)$?

$$\begin{aligned} m_c \in \mathcal{L}(M_C) &\iff m_c \in \{m \in \mathcal{M} \mid m = [M]_2, M(m) \neq \mathbb{V}\} \text{ par définition de } \mathcal{L}(M_C) \\ &\iff M_C(m_c) \neq \mathbb{V} \text{ puisque } m_c = [M_c]_2 \end{aligned}$$

Ainsi,

$$(\dagger) \quad m_c \in \mathcal{L}(M_C) \iff M_C(m_c) \neq \mathbb{V}$$

Par ailleurs,

$$(\ddagger) \quad m_c \in \mathcal{L}(M_C) \iff M_C(m_c) = \mathbb{V} \quad \text{par définition du langage par une MT}$$

Les équivalences (\dagger) et (\ddagger) donnent la CONTRADICTION cherchée.

Conclusion : En supposant qu'il existait une MT qui reconnaît $\overline{L_U}$ nous aboutissons à une contradiction. Donc $\overline{L_U}$ est indécidable, ce qui termine la preuve de (ii).

- (iii) D'après la proposition ?? un langage L est décidable si et seulement si L et \overline{L} sont reconnus par une MT. $\overline{L_U}$ n'étant pas reconnaissable par une MT, cf. (ii). L_U n'est pas décidable.

□

Exercice 2 : Indécidabilité : second exemple, preuve directe

Proposition 2 (Le langage des exécutions finies n'est pas décidable) *Le langage des exécutions finies L_{EF} est l'ensemble défini par*

$$L_{EF} = \{(m, \omega) \in \mathcal{M} \times \{0, 1\}^* \mid U(m)(\omega) \not\rightarrow \infty\}$$

C'est l'ensemble des couples (m, ω) tels que l'exécution de la machine m termine quand on accepte le mot ... ω .

(i) L_{EF} est récursivement énumérable, ie. reconnaissable par une MT

(ii) L_{EF} n'est pas co-récursevement énumérable, ie. $\overline{L_{EF}}$ n'est pas reconnaissable.

Preuve :

- (i) **Montrons L_{EF} reconnaissable :** Montrons qu'il existe une MT M_{EF} qui reconnaît L_{EF} , ie. $\mathcal{L}(M_{EF}) = L_{EF}$, ie. $M_{EF}(m, \omega) = \mathbb{V} \iff (m, \omega) \in L_{EF}$, ie. $M_{EF}(m, \omega) = \mathbb{V} \iff U(m)(\omega) \not\rightarrow \infty$.

La MT M_{EF} doit s'arrêter dans un état accepteur pour tout couple (m, ω) de L_{EF} , c'est-à-dire pour les couples qui correspondent à des finies. M_{EF} consiste à exécuter $U(m)(\omega)$ – le résultat nous importe peu – puis à passer dans l'état accepteur \bigcirc . Puisque les couples de L_{EF} sont précisément les couples pour lesquels l'exécution de U termine...., on a la garantie que la MT M_{EF} ci-dessous termine..... dans l'état \bigcirc pour les couples de L_{EF} .

$$M_{EF}(m, \omega) \stackrel{\text{def}}{=} [U(m)(\omega) ; \rightarrow \bigcirc]$$

- (ii) **Montrons $\overline{L_{EF}}$ non-reconnaissable :** On va montrer par contradiction qu'il existe pas de MT qui reconnaît $\overline{L_{EF}}$.

Que représente $\overline{L_{EF}} \stackrel{\text{def}}{=} (\mathcal{M} \times \{0, 1\}^*) \setminus L_{EF}$? Les éléments de $\overline{L_{EF}}$ sont les couples (m, ω) sur lesquels que la machine universelle U ne termine.... pas.

$$\overline{L_{EF}} \stackrel{\text{def}}{=} (\mathcal{M} \times \{0, 1\}^*) \setminus L_{EF} = \{(m, \omega) \in \mathcal{M} \times \{0, 1\}^* \mid U(m)(\omega) \rightarrow \infty\}$$

Preuve de (ii) par contradiction : SUPPOSONS qu'il existe une MT $M_{\overline{EF}}$ qui reconnaît $\overline{L_{EF}}$. On peut l'utiliser pour construire une MT $M_C(\omega) \stackrel{\text{def}}{=} M_{\overline{EF}}(\omega, \omega)$ qui copie le mot binaire ω pour en faire un couple et exécute $M_{\overline{EF}}$ sur ce couple.

$$\begin{aligned}\mathcal{L}(M_C) &= \{\omega \mid M_C(\omega) = \bigvee (\text{Acc})\} \text{ par définition du langage reconnu par une MT} \\ &= \{\omega \mid M_{\overline{EF}}(\omega, \omega) = V\} \text{ par définition de } M_C \\ &= \{\omega \mid (\omega, \omega) \in \overline{L_{EF}}\} \text{ par définition du langage reconnu par une MT} \\ &\quad \text{donc } \omega \text{ n'est pas un mot quelconque de } \{0, 1\}^* \text{ mais un élément de } \mathcal{M} \\ &= \{m \in \mathcal{M} \mid (m, m) \in \overline{L_{EF}}\} \\ &= \{m \in \mathcal{M} \mid U(m)(m) \rightarrow \infty\} \text{ par définition de } \overline{L_{EF}} \\ \mathcal{L}(M_C) &= \{m \in \mathcal{M} \mid m = [M]_2, M(m) \rightarrow \infty\} \text{ par définition de la MT universelle}\end{aligned}$$

$\mathcal{L}(M_C)$ est donc l'ensemble des mots binaires de \mathcal{M} qui correspondent à des MT qui ne s'arrêtent pas lorsqu'on les exécute sur leur description binaire.

Exhibons la contradiction : Considérons maintenant m_c le codage binaire de la MT M_C que l'on vient de construire. **On peut alors se demander si m_c appartient à $\mathcal{L}(M_C)$?**

$$\begin{aligned}m_c \in \mathcal{L}(M_C) &\iff m_c \in \{m \in \mathcal{M} \mid m = [M]_2, M(m) \rightarrow \infty\} \text{ par définition de } \mathcal{L}(M_C) \\ &\iff M_C(m_c) \rightarrow \infty \text{ puisque } m_c = [M_c]_2\end{aligned}$$

Ainsi, (\dagger) $m_c \in \mathcal{L}(M_C) \iff M_C(m_c) \rightarrow \infty$

Par ailleurs, par définition du langage reconnu par une MT, on a aussi l'équivalence :

$$(\ddagger) \quad m_c \in \mathcal{L}(M_C) \iff M_C(m_c) = V \iff M_C(m_c) \rightarrow^* \textcircled{O}$$

Les équivalences (\dagger) et (\ddagger) donnent la CONTRADICTION cherchée puisque l'exécution $M_C(m_c)$ est censée terminer (dans l'état \textcircled{O}) d'après (\ddagger), et ne pas terminer d'après (\dagger).

Conclusion : En supposant qu'il existait une MT qui reconnaît $\overline{L_{EF}}$ nous aboutissons à une contradiction. Donc $\overline{L_{EF}}$ est indécidable, ce qui termine la preuve de (ii).

□

