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 .... m accepte le .... ω.

(i) L_U *est* .... *, ie. reconnaissable par une* MT

(ii) L_U *n'est pas* .... ***-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,
$\mathscr{L}(U) \overset{def}{=} \{\, (m, \omega) \mid \ \ldots (m, \omega) = \mathbb{V} \,\}$ par définition du langage reconnu par une MT.

or $U(m, \omega) = U(m)(\omega) = M(\omega)$ avec $m = [M]_2$ par définition de la U
donc $\mathscr{L}(U) = \{\, (m, \omega) \mid M(\omega) = \ldots,\ m = \ \ldots\ldots \,\} \overset{def}{=} L_U$ d'après la définition de L_U.

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

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

Que représente $\overline{L_U} \overset{def}{=} (\mathcal{M} \times \{0,1\}^*) \setminus L_U$? 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 reconnaisse $\overline{L_U}$. On peut l'utiliser pour construire une MT $M_C(\omega) \overset{def}{=} M_{\overline{L_U}}(\omega, \omega)$ qui duplique le mot binaire ω pour en faire un couple et exécute $M_{\overline{L_U}}$ sur ce couple.

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

$\mathscr{L}(M_C)$ 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.* $M(m) \to^* \bigotimes \ \vee \ M(m) \to^\infty$.

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 $\mathscr{L}(M_C)$?

$$\begin{array}{rcl} m_c \in \mathscr{L}(M_C) & \Longleftrightarrow & m_c \in \{\, m \in \mathcal{M} \mid m = [M]_2,\ M(m) \neq \mathbb{V} \,\} \textit{ par définition de } \mathscr{L}(M_C) \\ & \Longleftrightarrow & M_c(m_c) \neq \mathbb{V} \quad \textit{puisque} \quad m_c = [M_c]_2 \end{array}$$

Ainsi,

(†) $m_c \in \mathscr{L}(M_C) \Longleftrightarrow M_C(m_c) \neq \mathbb{V}$

Par ailleurs,

(‡) $m_c \in \mathscr{L}(M_C) \Longleftrightarrow M_C(m_c) = \mathbb{V}$ *par définition du langage* .... *par une* MT

Les équivalences (†) et (‡) 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 propostion **??** un langage L est décidable si et seulement si L et $\overline{L}$ sont reconnu 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*

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

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

(i) L_{EF} *est **récursivement énumérable**, ie. reconnaissable ....*

(ii) L_{EF} *n'est **pas co-récursivement énumérable**, ie. .... n'est pas reconnaissable.*

Preuve :

(i) Montrons L_{EF} reconnaissable : Montrons qu'il existe une MT M_{EF} qui reconnaît L_{EF}, *ie.* $\mathscr{L}(M_{EF}) =$ ...., *ie.* $M_{EF}(m,\omega) =$ .... $\Longleftrightarrow (m,\omega) \in L_{EF}$, *ie.* $M_{EF}(m,\omega) =$ .... $\Longleftrightarrow$ $U(m)(\omega) \not\to$ .....

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 ◎. Puisque les couples de L_{EF} sont précisement les couples pour lesquels l'exécution de U .... , on a la garantie que la MT M_{EF} ci-dessous .... dans l'état ◎ pour les couples de ....

$$M_{EF}(m,\omega) \overset{\textit{def}}{=} [\ U(m)(\omega)\ \ ;\ \to ◎\ ]$$

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

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

$$\overline{L_{EF}} \overset{\textit{def}}{=} (\mathcal{M} \times \{0,1\}^*) \setminus L_{EF} = \{\, (m,\omega) \in \mathcal{M} \times \{0,1\}^* \mid U(m)(\omega) .... \,\}$$

Preuve de (ii) par contradiction : SUPPOSONS qu' . . . . une MT $M_{\overline{EF}}$ qui . . . .

$\overline{L_{EF}}$. On peut l'utiliser pour . . . . une MT $M_C(\omega) \stackrel{def}{=} M_{\overline{EF}}(\omega,\omega)$ qui . . . .

le mot binaire ω pour en faire un couple et . . . . $M_{\overline{EF}}$ sur ce couple.

$$
\begin{array}{rcll}
\mathscr{L}(M_C) & = & \{\omega \mid \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\} & \textit{par définition du langage reconnu par une MT} \\
 & = & \{\omega \mid M_{\overline{EF}}(\omega,\omega) = \mathbb{V}\} & \textit{par définition de } M_C \\
 & = & \{\omega \mid \ldots\ldots\ldots \in \overline{L_{EF}}\} & \textit{par définition du langage reconnu par une MT} \\
 & & & \textit{donc } \omega \textit{ n'est pas un mot quelconque de } \{0,1\}^* \textit{ mais un élément de } \mathcal{M} \\
 & = & \{m \in \mathcal{M} \mid (m,m) \in \ldots\ldots\ldots\} & \\
 & = & \{m \in \mathcal{M} \mid U(m)(m) \ldots\ldots\ldots\} & \textit{par définition de } \overline{L_{EF}} \\
\mathscr{L}(M_C) & = & \{m \in \mathcal{M} \mid m = \ldots\ldots\ldots,\ M(m) \to \infty\} & \textit{par définition de la } \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}
$$

$\mathscr{L}(M_C)$ est donc l'ensemble des mots binaires de $\mathcal{M}$ qui correspondent à *des* MT *qui ne s'arrête 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 $\mathscr{L}(M_C)$?**

$$
\begin{array}{rcll}
m_c \in \mathscr{L}(M_C) & \Longleftrightarrow & m_c \in \{m \in \mathcal{M} \mid m = [M]_2,\ M(m) \to \infty\} & \textit{par définition de } \mathscr{L}(M_C) \\
 & \Longleftrightarrow & \ldots\ldots\ldots\ldots\ldots \to \infty & \textit{puisque } m_c = [M_c]_2
\end{array}
$$

Ainsi, (†) $m_c \in \mathscr{L}(M_C) \Longleftrightarrow M_C(m_c) \to \infty$

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

$$(\ddagger) \quad m_c \in \mathscr{L}(M_C) \Longleftrightarrow M_C(m_c) = \mathbb{V} \Longleftrightarrow M_C(m_c) \to^* \circledcirc$$

Les équivalences (†) et (‡) donnent la CONTRADICTION cherchée puisque l'exécution $M_C(m_c)$ est censée terminer (dans l'état $\circledcirc$) 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 $\overline{L_{EF}}$ est indécidable, ce qui termine la preuve de (ii).

□