ENSEIRB-MATMECA- Section Informatique, 2ième année
Calculabilité, 2022/2023

# CALCULABILITÉ

DM3- Corrigé.

## Partie I

Machines de Bennett.

**Machines de Bennett** Dans les trois questions qui suivent on considère des transitions :

$$\tau = (q, \vec{s}, \vec{s'}, q'), \quad \tau' = (r, \vec{t}, \vec{t'}, r').$$

1- Une CNS pour que $\tau, \tau'$ soient inverses l'une de l'autre est que :
$q = r', \quad q' = r$ et pour tout $i \in [1, n]$

$$s_i \in \Sigma, s'_i \in \Sigma \Rightarrow (t_i = s'_i, t'_i = s_i), \quad \text{et}$$

$$s_i = /, s'_i = \varepsilon \Rightarrow (t_i = /, \quad t'_i = -\varepsilon).$$

On note maintenant $I = \{i \in [1, n] \mid s_i \in \Sigma\}, \quad J = \{j \in [1, n] \mid t_j \in \Sigma\}$.
2- Une CNS est que :

$$q = r \text{ et } \vec{s}_{|I \cap J} = \vec{t}_{|I \cap J} \text{ et } \tau \neq \tau'.$$

3- Une CNS est que :

$$q' = r' \text{ et } \vec{s'}_{|I \cap J} = \vec{t'}_{|I \cap J} \text{ et } \tau \neq \tau'.$$

**Déterminisme, réversibilité**
4- Supposons que $\mathbb{M}$ est déterministe. Si $c \vdash_{\tau} d$ et $c \vdash_{\tau'} d'$ alors $d = d'$. Donc $\vdash_{\mathbb{M}}$ est une fonction.
5- Supposons que $\mathbb{M}$ est réversible.
5.1- Par la question 4, $\vdash_{\mathbb{M}}$ est une fonction. De plus, si $c \vdash_{\tau} d$ et $c' \vdash_{\tau'} d$ alors $c = c'$. Donc $\vdash_{\mathbb{M}}$ est une fonction *injective*.
5.2 Pour chaque transition $\tau = (q, \vec{s}, \vec{s'}, q')$ de $\mathbb{M}$. posons :

$$I(\tau) := (r, \vec{t}, \vec{t'}, r')$$

où $(r, \vec{t}, \vec{t'}, r')$ vérifie la CNS de la question 1. La machine

$$\mathbb{M}' := \langle \Sigma, Q, \delta', q_0, q_1 \rangle$$

avec $\delta' := \{I(\tau) \mid \tau \in \delta\}$ vérifie que

$$\{(c, c') \mid c' \vdash_{\mathbb{M}} c\} = \vdash_{\mathbb{M}'}.$$

6- 6.1 $\delta_1$ est déterministe.
Les transitions $((p, a, /, b, +1, p), (r, a, a, b, a, p))$ ont des images chevauchantes, donc la machine n'est pas réversible.
6.2 $\delta_2$ est réversible.
7- 7.0 Dans le cas particulier de $\delta_2$ on peut compléter cet ensemble de transitions en y adjoignant les transitions :

$$(p, b, b, a, a, r), \quad (q, a, b, a, a, q), \quad (r, b, b, a, b, p), \quad (r, a, b, b, a, q), \quad (r, b, a, b, b, q).$$

7-
Introduisons une nouvelle notation, plus symétrique, pour les transitions de machines de Bennett à $n$ bandes : chaque transition est un 6-uple

$$t = (I, \vec{a}, \vec{\varepsilon}, I, \vec{b}, \vec{\eta})$$

avec $\{0\} \subseteq I \subseteq [0, n]$, $\vec{a}, \vec{b} \in (\Sigma \cup Q)^I$, $\vec{\varepsilon}, \vec{\eta} \in \{-1, +1\}^{\bar{I}}$, $\vec{\varepsilon} + \vec{\eta} = 0^{\bar{I}}$. (ici nous notons $\bar{I} := [0, n] \setminus I$). L'interprétation de $t$ dans les notations de Bennett est :

$$\tau = (q, \vec{s}, \vec{s'}, q')$$

où

$$q = a_0, s_i = a_i \text{ si } i \in I, i \geq 1 \quad s_i = / \text{ si } i \in \bar{I}, i \geq 1$$

$$q' = b_0, s'_i = b_i \text{ si } i \in I, i \geq 1 \quad s'_i = \eta_i \text{ si } i \in \bar{I}, i \geq 1.$$

Avec ces notations :
- l'inverse de la transition $(I, \vec{a}, \vec{\varepsilon}, I, \vec{b}, \vec{\eta})$ est la transition $(I, \vec{b}, \vec{\eta}, I, \vec{a}, \vec{\varepsilon})$.
- deux transitions

$$t = (I, \vec{a}, \vec{\varepsilon}, I, \vec{b}, \vec{\eta}), \quad t' = (J, \vec{c}, \vec{\alpha}, J, \vec{d}, \vec{\beta})$$

sont chevauchantes ssi

$$\vec{a}_{|I \cap J} = \vec{c}_{|I \cap J} \text{ et } t \neq t' \tag{1}$$

et elles ont des images chevauchantes ssi

$$\vec{b}_{|I \cap J} = \vec{d}_{|I \cap J} \text{ et } t \neq t' \tag{2}$$

On note $\mathrm{LHS}(t) := (I, \vec{a}, \vec{\varepsilon})$, $\mathrm{RHS}(t) := (I, \vec{b}, \vec{\eta})$. Etant donnée une machine de Bennett réversible d'ensemble de transitions $\delta$ nous notons :

$$\mathcal{L}(\delta) := \{\mathrm{LHS}(t) \mid t \in \delta\}, \quad \mathcal{R}(\delta) := \{\mathrm{RHS}(t) \mid t \in \delta\}.$$

Deux triplets $(I, \vec{a}, \vec{\varepsilon})$, $(J, \vec{c}, \vec{\alpha})$ sont dits *compatibles* ssi

$$\vec{a}_{|I\cap J} \neq \vec{c}_{|I\cap J}.$$

On pose, pour tout ensemble $\mathcal{T}$ de triplets de la forme $(I, \vec{a}, \vec{\varepsilon})$

$$\mathrm{COMP}(\mathcal{T}) := \{(J, \vec{c}, \vec{\alpha}) \mid \forall (I, \vec{a}, \vec{\varepsilon}) \in \mathcal{T},\ \ ((I, \vec{a}, \vec{\varepsilon}), (J, \vec{c}, \vec{\alpha})) \text{ sont compatibles } \}.$$

Un triplet $(I, \vec{a}, \vec{\varepsilon})$ est dit total si $I = [0, n]$. On démontre alors :
**Lemme 1** :
Si $\delta$ est réversible alors le nombre de triplets totaux de COMP(LHS($\delta$)) est égal au nombre de triplets totaux de COMP(RHS($\delta$)).
On démontre ensuite le
**Lemme 2** :
La relation $\vdash_{\mathbb{M}}$ est partout définie ssi COMP(LHS($\delta$)) $= \emptyset$.
Par induction descendante sur le nombre de triplets totaux de COMP(LHS($\delta$)), on conclut que toute machine de Bennett réversible est complétable en une machine de Bennett *bijective*.

**Fonction calculée**
8- On suit les idées de l'énoncé. De plus amples détails sont donnés dans l'article [Bennett C.H., "Logical Reversibility of Computation", IBM Journal of Research and Development, 17, p. 525-532].
9- Soit $\mathbb{M}_1$ une machine de Turing à une bande, qui calcule $f$. On peut transformer $\mathbb{M}_1$ en une machine de Turing $\mathbb{M}_2$ à une bande, qui calcule $f$ et qui a un calcul infini sur chaque mot $u \notin$ Dom(f). D'après Q8 $f$ est calculée par une machine de Bennett réversible à trois bandes $\mathbb{M}_3$. La construction de $\mathbb{M}_3$ montre que $\mathbb{M}_3$ a un calcul infini ne passant pas par $q_1$, sur tout mot $u \notin$ Dom(f). D'après Q7, il existe une machine de Bennett bijective à trois bandes $\mathbb{M}_4$ qui comporte toutes les transitions de $\mathbb{M}_3$. On en conclut que :
- sur tout mot $u \notin$ Dom(f), $\mathbb{M}_4$ boucle, sans passer par l'état $q_1$,
- sur tout mot $u \in$ Dom(f), $\mathbb{M}_4$ calcule $f(u)$.
Donc $\mathbb{M}_4$ est une machine de Bennett à trois bandes, bijective, qui calcule $f$.

## Partie II

1- L'entropie de Shannon d'une mesure de probabilité $p : \mathcal{P}(\Omega) \to [0, 1]$ est définie par :

$$S(p) := \sum_{x\in\Omega} -p(\{x\}) \cdot \log(p(\{x\})).$$

On a donc :

$$S(\mathrm{Pr}_{i,e'}) := \sum_{e\in\mathcal{E}} -\mathrm{Pr}_{i,e'}(\{e\}) \cdot \log(\mathrm{Pr}_{i,e'}(\{e\})).$$

Mais pour tout $e \notin \pi^{-1}(e')$, $\mathrm{Pr}_{i,e'}(\{e\}) \cdot \log(\mathrm{Pr}_{i,e'}(\{e\})) = 0$. La formule ci-dessus se simplifie donc en :

$$S(\mathrm{Pr}_{i,e'}) := \sum_{e\in\pi^{-1}(e')} -\mathrm{Pr}_{i,e'}(\{e\}) \cdot \log(\mathrm{Pr}_{i,e'}(\{e\})),$$

ce qui est bien la définition (1) de l'énoncé.
2- Comme $\mathrm{Pr}_{i,e'}(e) = \frac{1}{\#\pi_i^{-1}(e')}$ on obtient

$$\begin{aligned} S(\mathrm{Pr}_{i,e'}) &= \sum_{e\in\pi^{-1}(e')} -\frac{1}{\#\pi_i^{-1}(e')} \cdot \log(\#\pi_i^{-1}(e')), \\ &= \log(\#\pi_i^{-1}(e')), \end{aligned}$$

puisque tous les nombres sommés sont égaux entre eux et qu'il y en a $\#\pi_i^{-1}(e')$.
3.1 Montrons que

$$\tau(\pi_0^{-1}(e')) \subseteq \pi_1^{-1}(\tau'(e')). \tag{3}$$

Soit $e \in \pi_0^{-1}(e')$.
On déduit successivement :

$$\begin{aligned} \pi_0(e) &= e' \\ \tau'(\pi_0(e)) &= \tau'(e') \\ \pi_1(\tau(e)) &= \tau'(e) \quad \text{par H0 appliquée au membre gauche} \\ \tau(e) &\in \pi_1^{-1}(\tau'(e)). \end{aligned}$$

De l'inclusion (3) entre ensembles on tire une inégalité (dans le même sens) entre les cardinaux de ces ensembles, puis entre les logarithnmes de ces cardinaux :

$$\log(\#\tau(\pi_0^{-1}(e'))) \leq \log(\#\pi_1^{-1}(\tau'(e'))). \tag{4}$$

ce qui, vue la question 2, se réécrit en

$$S_0(e') \leq S_1(\tau'(e')). \tag{5}$$

3.2 Il y a égalité dans l'inégalité (5) ssi il y a égalité dans l'inégalité (4) i.e.

$$\#\tau(\pi_0^{-1}(e')) = \#\pi_1^{-1}(\tau'(e'))$$

ce qui, vue l'inégalité ensembliste (3), est équivalent à l'égalité

$$\tau(\pi_0^{-1}(e')) = \pi_1^{-1}(\tau'(e')).$$

3.3 Montrons que la CNS obtenue à la question 3.2. est équivalente à la condition annoncée.

$$\begin{aligned}
\tau'^{-1}(\tau'(e')) = \{e'\} &\Leftrightarrow \pi_0^{-1}(\tau'^{-1}(\tau'(e'))) = \pi_0^{-1}(\{e'\}) \text{ car } \pi_0 \text{ est surjective} \\
&\Leftrightarrow \tau^{-1}(\pi_1^{-1}(\tau'(e'))) = \pi_0^{-1}(\{e'\}) \text{ par H0} \\
&\Leftrightarrow \pi_1^{-1}(\tau'(e')) = \tau(\pi_0^{-1}(\{e'\})) \text{ car } \tau \circ \tau^{-1} = \mathrm{Id}_{\mathcal{E}}.
\end{aligned}$$

4- Montrons l'équivalence demandée.

$$\begin{aligned}
\forall e' \in \mathcal{E}', S_1(\tau'(e')) = S_0(e') &\Leftrightarrow \forall e' \in \mathcal{E}', \tau'^{-1}(\tau'(e')) = e' \text{ par Q3.3} \\
&\Leftrightarrow \tau' \text{ est une bijection de } \mathcal{E}' \text{ sur son image} \\
&\Leftrightarrow \tau' \text{ est une bijection de } \mathcal{E}' \text{ dans } \mathcal{E}' \text{ car } \mathcal{E}' \text{ est fini.}
\end{aligned}$$

5- Par la Q3.1 on sait que la variation d'entropie

$$\Delta S(e') := S_1(\tau'(e')) - S_0(e')$$

est égale à

$$\log(\#\pi_1^{-1}(\tau'(e'))) - \log(\#\pi_0^{-1}(e)).$$

Remarquons que

$$\begin{aligned}
\#\pi_1^{-1}(\tau'(e')) &= \#\tau^{-1}(\pi_1^{-1}(\tau'(e'))) \text{ car } \tau \text{ est bijective} \\
&= \#\pi_0^{-1}(\tau'^{-1}(\tau'(e'))) \text{ par H0}
\end{aligned}$$

Donc

$$\begin{aligned}
\Delta S(e') &= \log \#(\pi_0^{-1}(\tau'^{-1}(\tau'(e')))) - \log(\#\pi_0^{-1}(e')) \\
&= \log\left(\frac{\#\pi_0^{-1}(\tau'^{-1}(\tau'(e')))}{\#\pi_0^{-1}(e')}\right)
\end{aligned}$$

et comme toutes les images réciproques $\pi_0^{-1}(e')$ ont le même cardinal

$$\Delta S(e') = \log(\#\tau'^{-1}(\tau'(e'))). \tag{6}$$

Nous utiliserons cette formule dans chacun des cas particuliers qui suivent.
5.1 $\Delta S(\overrightarrow{b}) = \log(2^8) = 8 \cdot \log(2)$.
5.2 pour $\tau = \tau_1$ :
si $\tau_1(\overrightarrow{b}) = 0^8$ alors

$$\Delta S(\overrightarrow{b}) = \log(\sum_{k=0}^{3} \binom{8}{k}) = \log(93) \approx 6\log(2)$$

si $\tau_1(\overrightarrow{b}) = 0^7 1$ alors

$$\Delta S(\overrightarrow{b}) = \log(\sum_{k=0}^{4} \binom{8}{k}) = \log(163) \approx 7\log(2)$$

(approximations par défaut).
pour $\tau = \tau_2$ :
si $\overrightarrow{b} = 0^8$ alors

$$\Delta S(\overrightarrow{b}) = 0.$$

si $\overrightarrow{b} \neq 0^8$ alors

$$\Delta S(\overrightarrow{b}) = \log(2^8 - 1) = \log(255) \approx 8 \cdot \log(2).$$

pour $\tau = \tau_3$ :

$$\Delta S(\overrightarrow{b}) = \log(2).$$

6.1 En utilisant la formule (6) établie ci-dessus (début de Q5), et en tenant compte de la croissance de la fonction log, nous obtenons :

$$\max(\{S_1(\tau'(e')) - S_0(e') \mid e' \in \mathcal{E}'\}) = \log(\max_{e' \in \mathcal{E}'} \#\tau'^{-1}(\tau'(e')))$$

6.2 On a la suite d'équivalences

$$\begin{aligned}
\forall e' \in \mathcal{E}', \Delta S(e') = 0 \quad &\Leftrightarrow \quad \log(\max_{e' \in \mathcal{E}'} \#\tau'^{-1}(\tau'(e'))) = 0 \\
&\Leftrightarrow \quad \max_{e' \in \mathcal{E}'} \#\tau'^{-1}(\tau'(e')) = 1 \\
&\Leftrightarrow \quad \tau' \text{ est une bijection de } \mathcal{E}' \text{ sur son image} \\
&\Leftrightarrow \quad \tau' \text{ est une bijection de } \mathcal{E}' \text{ dans } \mathcal{E}' \text{ car } \mathcal{E}' \text{ est fini.}
\end{aligned}$$

Donc on retrouve le fait que $\tau'$ est bijective ssi elle conserve l'entropie (point par point).