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

CALCULABILITÉ

DM- à rendre avant le 16/04/2023, à 23 heure 59.

Sujet : On s'intéresse à un modèle de calcul, fondé sur des machines abstraites analogues aux machines de Turing, mais possédant une propriété de *réversibilité*. La partie II (qui est facultative) motive, par des arguments thermodynamiques, la conception de modèles de calcul réversibles.
Indications : Les questions affectées d'une étoile sont difficiles. On peut *admettre* une question et utiliser les résultats de cette question dans la suite du problème. Tous moyens d'investigation autorisés. Rédaction finale par groupes de quatre.
Barème : La partie I est notée sur 20. La partie II (facultative) apporte des points en plus, à condition d'avoir obtenu 10 points dans la partie I.

Partie I

Machines de Bennett.

On détaille ici le théorème de Bennett qui affirme que les machines de Turing "réversibles" ont la même puissance de calcul que les machines de Turing ordinaires.

Machines de Bennett Une machine de Bennett à n bandes est un 5-uplet

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

où

- Σ est un ensemble fini, que l'on appelle "l'alphabet"
- Q est un ensemble fini, que l'on appelle "l'ensemble des états"
- δ est un ensemble de quadruplets de la forme

$$q, [t_1, \ldots, t_n], [t'_1, \ldots, t'_n], q' \tag{1}$$

  où $q, q' \in Q$, $t_1, \ldots, t_n \in \Sigma \cup \{/\}$ et $t'_1, \ldots, t'_n \in \Sigma \cup \{-1, 1\}$. Lorsque $t_i \in \Sigma$, t'_i est aussi une lettre de Σ, tandis que, lorsque t_i est le symbole spécial $/$, $t'_i \in \{-1, 1\}$ i.e. t'_i est un mouvement.
- q_0 (resp. q_1) est un élément de Q, dit "état initial" (resp. "état final")

Une configuration de $\mathbb{M}$ est formée d'un état, suivi d'un n-uple de mots indexés sur $\mathbb{Z}$, suivi d'un n-uple d'entiers indiquant les positions p_i de la ième tête de lecture sur la ième bande. Chaque quadruplet (1) de δ est une *transition* de la machine ; il est interprété de la facon suivante :
si la machine est dans une configuration avec l'état q et si les symboles $t_1, \ldots, t_n$ sont visibles en positions $p_1, \ldots, p_n$, alors $\mathbb{M}$ passe dans l'état q', si t'_i est une lettre de Σ alors t_i est remplacé par t'_i sur la ième bande et p_i n'est pas changé, si $t'_i \in \{-1, 1\}$ alors t_i n'est pas changée mais la ième tête passe en position $p_i + t'_i$. Un symbole t_i est "visible" en position p_i lorsque $t_i \in \Sigma$ et la lettre en position p_i est exactement t_i ou bien lorsque $t_i = /$.
Soient

$$c = (q, w_1, \ldots, w_n, p_1, \ldots, p_n), \;\; c' = (q', w'_1, \ldots, w'_n, p'_1, \ldots, p'_n)$$

deux configurations de $\mathbb{M}$ i.e. $q, q' \in Q, w_i, w'_i \in \Sigma^{\mathbb{Z}}, p_i, p'_i \in \mathbb{Z}$. On note

$$c \vdash\!\!\!- \,_{\tau} c'$$

si la machine passe de c à c' en utilisant la transition τ et

$$c \vdash\!\!\!- \,_{\mathbb{M}} c'$$

ssi il existe $\tau \in \delta$ tel que $c \vdash\!\!\!- \,_{\tau} c'$.
1- A quelles conditions (aisément testables) sur τ, τ' est-il vrai que, pour toutes configurations c, c' :

$$c \vdash\!\!\!- \,_{\tau} c' \Leftrightarrow c' \vdash\!\!\!- \,_{\tau'} c?$$

Dans ce cas on dit que les transitions τ, τ' sont inverses l'une de l'autre.
2- A quelles conditions (aisément testables) sur τ, τ' est-il vrai qu'il existe des configurations c, d, d' telles que : $c \vdash\!\!\!- \,_{\tau} d, c \vdash\!\!\!- \,_{\tau'} d'$ et $d \neq d'$?
Dans ce cas on dit que les transitions τ, τ' ont des domaines chevauchants.
3- A quelles conditions (aisément testables) sur τ, τ' est-il vrai qu'il existe des configurations c, c', d telles que : $c \vdash\!\!\!- \,_{\tau} d, c' \vdash\!\!\!- \,_{\tau'} d$ et $c \neq c'$?
Dans ce cas on dit que les transitions τ, τ' ont des images chevauchantes.

Déterminisme, réversibilité Une machine de Bennett

$$\mathbb{M} = \langle \Sigma, Q, \delta, q_0, q_1 \rangle \tag{2}$$

est dite *déterministe* ssi elle n'a pas de paire de transitions dont les domaines se chevauchent. La machine est dite *réversible* ssi elle n'a pas de

paire de transitions dont les domaines se chevauchent ou dont les images se chevauchent.
4- Montrer que si $\mathbb{M}$ est déterministe alors $\vdash_{\mathbb{M}}$ est une fonction.
5- 5.1- Montrer que si $\mathbb{M}$ est réversible alors $\vdash_{\mathbb{M}}$ est une fonction injective.
5.2 Existe-t-il, dans ce cas, une machine de Bennett $\mathbb{M}'$ telle que, la fonction inverse $\{(c, c') \mid c' \vdash_{\mathbb{M}} c\}$ est exactement $\vdash_{\mathbb{M}'}$?
6- Pour chacune des machines de Bennett suivantes, déterminer si elle est déterministe ? réversible ? :
6.1 $\Sigma = \{a, b\}$, $Q = \{p, q, r\}$ et δ_1 est l'ensemble des transitions :

$$(p, a, /, b, +1, p), \quad (p, b, a, a, b, q), \quad (q, /, a, -1, b, r), \quad (q, b, b, b, a, r),$$
$$(r, a, a, b, a, p).$$

6.2 δ_2 est l'ensemble des transitions :

$$(p, a, /, b, +1, p), \quad (p, b, a, a, b, q), \quad (q, /, a, -1, b, r), \quad (q, b, b, b, a, r),$$
$$(r, a, a, a, a, p).$$

**7- Supposons que $\mathbb{M}$ est réversible. Peut-on étendre $\mathbb{M}$ en une une machine réversible $\mathbb{M}_t = \langle \Sigma, Q, \delta_t, q_0, q_1 \rangle$ telle que $\delta \subseteq \delta_t$ et $\vdash_{\mathbb{M}_t}$ est une *bijection* de l'ensemble des configurations (pour Σ,Q) dans lui-même ?
Nous dirons alors que $\mathbb{M}_t$ est *bijective*.
Aide : on pourra commencer par traiter le cas particulier de la machine réversible vue à la question 6.

Fonction calculée On suppose que la machine $\mathbb{M}$ est déterministe. L'alphabet Σ contient un symbole particulier b ("blanc") et aussi le sous-ensemble $\{a_0, a_1\}$. Un contenu de bande est standard s'il est de la forme

$$\ldots bbbbb \cdot u \cdot bbbbbb \ldots \tag{3}$$

avec $u \in (\Sigma \setminus \{b\})^*$. On note B la suite bi-infinie $\ldots bbbbbbbbbbb \ldots$ (i.e. l'application de $\mathbb{Z}$ dans Σ qui vaut constamment b) et on note parfois (abusivement) u le mot bi-infini (3).
La machine $\mathbb{M}$ *calcule* la fonction $f : \{a_0, a_1\}^* \to \{a_0, a_1\}^*$ ssi : pour tout mot $u \in \{a_0, a_1\}^*$,
B1- partant de $(q_0, u, B, \ldots, B, 0, \ldots, 0)$ la machine atteint une configuration d'état q_1 ssi $u \in \mathrm{Dom(f)}$.
B2- la première configuration d'état q_1 atteinte est de la forme $(q_1, f(u), B, \ldots, B, 0, \ldots, 0)$.

On veut montrer le théorème suivant ([Bennett 1973]) : Soit $\mathbb{M}$ une machine de Bennett déterministe sur une bande, calculant une fonction f.
Alors on peut construire une machine de Bennett *réversible* $\mathbb{M}'$, sur un alphabet $\Sigma' \supseteq \Sigma$, à trois bandes, telle que : pour tout contenu de bande standard w sur l'alphabet Σ
TB1- $\mathbb{M}$ atteint q_1 à partir de $(q_0, w, 0)$ ssi $\mathbb{M}'$ atteint q_1 à partir de $(q_0, w, B, B, 0, 0, 0)$
TB2- la première configuration d'état q_1 atteinte par $\mathbb{M}$ est de la forme (q_1, W, p_1) ssi la première configuration d'état q_1 atteinte par $\mathbb{M}'$ est de la forme $(q_1, w, B, W, p'_1, p'_2, p'_3)$.
*8- Démontrer le théorème de Bennett.
Indications : $\mathbb{M}'$ procède en trois étapes :
étape 1 :$\mathbb{M}'$ simule sur la bande 1 le fonctionnement de $\mathbb{M}$ en mémorisant sur la bande 2 l'histoire de ce calcul (suite des adresses de la tête de lecture et transitions) ; jusqu'à ce que q_1 soit atteint ou alors indéfiniment.
étape 2 : $\mathbb{M}'$ recopie la bande 1 sur la bande 3.
étape 3 : $\mathbb{M}'$, en suivant l'histoire (écrite sur la bande 2), à l'envers, simule, sur la bande 1, l'inverse du calcul de $\mathbb{M}$, tout en effaçant l'histoire, jusqu'à atteindre l'état q_0.
9- Montrer que toute fonction partielle calculable $f : \{a_0, a_1\}^* \to \{a_0, a_1\}^*$ est calculable par une machine de Bennett à trois bandes, *bijective*.

Partie II

Nous présentons une modélisation simple d'un calculateur physique [1].
On considère deux ensembles finis $\mathcal{E}, \mathcal{E}'$ et quatre applications $\pi_0, \pi_1 : \mathcal{E} \to \mathcal{E}'$ et $\tau : \mathcal{E} \to \mathcal{E}$, $\tau' : \mathcal{E}' \to \mathcal{E}'$. L'ensemble $\mathcal{E}$ (resp. $\mathcal{E}'$) modélise l'"ensemble des états microscopiques"(resp. des "états macroscopiques"). L'application π_i modélise la relation entre un état microscopique (objectif, mais non directement observable) et un état macroscopique (directement observable), à l'instant $i \in \{0, 1\}$ (ce que l'on appelle une une "observable"). L'application π_0 est supposée surjective : $\mathcal{E}'$ modélise l'ensemble des résultats d'observations *possibles* à l'instant 0. L'application τ (resp. τ') modélise la loi d'évolution de l'instant 0 à l'instant 1, du point de vue microscopique (resp. macroscopique). On note $\Pr : \mathcal{P}(\mathcal{E}) \to [0, 1]$ la mesure de probabilité uniforme sur $\mathcal{E}$:

$$\forall P \subseteq \mathcal{E}, \ \Pr(P) := \frac{\#(P)}{\#(\mathcal{E})}.$$

Nous faisons les hypothèses suivantes :
(H0) $\pi_1 \circ \tau = \tau' \circ \pi_0$.

1. les raisonnements pourraient néanmoins être étendus à des modélisations plus sophistiquées

(H1) τ est une bijection.
(H2) τ' est une application.
(voir le diagramme 1). On définit pour tout état macroscopique $e' \in \mathcal{E}'$,

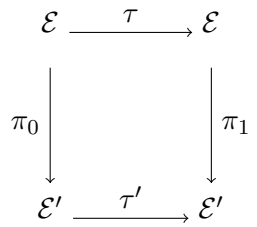

FIGURE 1 – Micro-états versus macro-états.

l'*entropie* de e', pour l'observable π_i comme :

$$S_i(e') := \sum_{e \in \pi_i^{-1}(e')} -\mathrm{Pr}_{i,e'}(\{e\}) \cdot \log(\mathrm{Pr}_{i,e'}(\{e\})) \tag{4}$$

[2] où $\mathrm{Pr}_{i,e'}$ est la probabilité conditionnelle par rapport à $\pi_i^{-1}(e')$, autrement dit :

$$\mathrm{Pr}_{i,e'}(\{e\}) = \frac{1}{\#(\pi_i^{-1}(e'))} \text{ si } e \in \pi_i^{-1}(e'), \;\; \mathrm{Pr}_{i,e'}(\{e\}) = 0 \text{ si } e \notin \pi_i^{-1}(e').$$

1- Vérifier que $S_i(e')$ est l'entropie de Shannon de la mesure de probabilité $\mathrm{Pr}_{i,e'}$.
2- Exprimer le plus simplement possible $S_i(e')$ à partir de $\#(\pi_i^{-1}(e'))$.
3- 3.1 Montrer que, pour tout $e' \in \mathcal{E}'$

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

3.2 Montrer qu'il y a égalité dans (5) si et seulement si

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

*3.3 En déduire qu'il y a égalité dans (5) si et seulement si

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

2. on convient que pour $x \neq 0$, $\log(x)$ est le logarithme de base 2 de x et que $0 \cdot log(0) = 0$

4- Montrer que τ' est une bijection si et seulement si :

$$\forall e' \in \mathcal{E}', \quad S_1(\tau'(e')) = S_0(e').$$

i.e. la loi d'évolution macroscopique est *bijective* ssi elle *conserve l'entropie*.
5- On considère le cas où $\mathcal{E}' = \mathbb{B}^8$ et où, à l'instant 0 , toutes les images réciproques $\pi_0^{-1}(e')$ ont le même cardinal c.
5.1 Calculer l'augmentation d'entropie produite par la loi d'évolution macroscopique $\tau : \mathbb{B}^8 \to \mathbb{B}^8$, $\tau(\vec{b}) := 0^8$ (le vecteur qui a toutes ses composantes nulles).
5.2 Même question pour les applications τ_1, τ_2, τ_3 suivantes :

$$\tau_1(\vec{b}) := 0^7 1 \quad \text{si la majorité des bits vaut 1,} \quad \tau_1(\vec{b}) := 0^7 0 \quad \text{sinon ,}$$
$$\tau_2(0^8) := 0^8 \quad \tau_2(\vec{b}) := 0^7 1 \quad \text{si } \vec{b} \neq 0^8,$$

(on distinguera différents cas suivant l'état de départ $e' \in \mathbb{B}^8$).

$$\tau_3(\vec{b}) := (b_0 \oplus b_1, b_1 \oplus b_2, \ldots, b_6 \oplus b_7, b_8).$$

6- On supose encore que toutes les images réciproques $\pi_0^{-1}(e')$ ont le même cardinal c (mais l'espace $\mathcal{E}'$ est maintenant quelconque).
6.1 Donner une formule la plus simple possible qui exprime le nombre :

$$\max(\{S_1(\tau'(e')) - S_0(e') \mid e' \in \mathcal{E}'\})$$

à partir de l'application τ'.
6.2 Retrouver le résultat de la question 4 dans ce contexte.

L'analogie avec la thermodynamique statistique fait penser que l'expression $k \cdot T \cdot [S_1(\tau'(e')) - S_0(e')]$ (où k est la constante de Boltzman et T est la température ambiante) exprime la quantité de chaleur que doit produire toute machine, dont l'ensemble des états microscopiques serait $\mathcal{E}$ et dont l'état macroscopique passerait de e' à $\tau'(e')$. [3]
En se restreignant à des machines logiques dont la fonction de transition τ' est *bijective*, on réduit à néant ce phénomène de production de chaleur (voir I.Q.4 et I.Q.6.2).

3. C'est ce que pensent et argumentent divers physiciens, notamment R. Landauer et C.H. Bennett alors travaillant chez IBM, dans divers articles des années 1960 à 1980.