ENSEIRB-MATMECA
Option second semestre, 2013/2014

# Information Quantique

DM- Avril 2014

## Partie 1

Calcul réversible.

Dans cette première partie, on détaille le théorème de Bennett qui montre 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

- $\Sigma$ est un ensemble fini, que l'on appelle "l'alphabet"
- $Q$ est un ensemble fini, que l'on appelle "l'ensemble des états"
- $\delta$ 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 $t'_1, \ldots, t'_n \in \Sigma \cup \{-1, 0, 1\}$. Lorsque $t_i \in \Sigma$, $t'_i$ est aussi une lettre de $\Sigma$, tandis que, lorsque $t_i$ est le symbole spécial $/$, $t'_i \in \{-1, 0, 1\}$ 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 $\delta$ 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 $\Sigma$ alors $t_i$ est remplacé par $t'_i$ sur la ième bande et $p_i$ n'est pas changé, si $t'_i \in \{-1, 0, 1\}$ 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

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

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 $\tau$. 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 $\tau, \tau'$ 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 $\tau, \tau'$ sont inverses l'une de l'autre.
2- A quelles conditions (aisément testables) sur $\tau, \tau'$ 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 $\tau, \tau'$ ont des domaines chevauchants.
3- A quelles conditions (aisément testables ) sur $\tau, \tau'$ 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 $\tau, \tau'$ 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- Montrer que si $\mathbb{M}$ est réversible alors $\vdash_{\mathbb{M}}$ est une fonction injective. 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- 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 $\Sigma$,$Q$) dans lui-même.
Nous dirons alors que $\mathbb{M}_t$ est réversible *totale*.

**Fonction calculée** On suppose que la machine $\mathbb{M}$ est déterministe. L'alphabet $\Sigma$ 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 $\ldots bbbbbbbbbb \ldots$ (i.e. l'application de $\mathbb{Z}$ dans $\Sigma$ qui vaut constamment $b$) et on note parfois (abusivemen) $u$ 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 $u \in$ 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 $\Sigma$
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 $q_0$.

## Partie 2

Calcul quantique

Dans cette seconde partie, on étudie les machines de Deutsch, introduites par D. Deutsch en 1985. On établit des relations entre les fonction calculables par les MD et les fonctions calculables par des MB.

**Machines de Deutsch** Une machine de Deutsch a des configurations dans un espace de Hilbert $\mathcal{H}$ que nous allons décrire :
- soit $\mathcal{B}$ l'espace de Hilbert canonique de dimension 2 et $|0\rangle, |1\rangle$ sa base canonique
- soit $\mathcal{P}$ un espace de Hilbert muni d'une base de Hilbert $(e_x)_{x\in\mathbb{Z}}$
- soit $M \geq 1$ un entier et $\mathcal{Q} = \mathcal{B}^{\otimes M}$ l'espace des états
- soit $\mathcal{F} \subseteq \bigotimes_{i\in\mathbb{Z}} \mathcal{B}$ l'ensemble des vecteurs $u = \bigotimes_{i\in\mathbb{Z}} |u_i\rangle$ tels que $\{i \in \mathbb{Z} \mid u_i \neq 0\}$ est fini ( $\mathcal{F}$ est l'ensemble des q-mots bi-infinis de support fini) et soit $\mathcal{M}$ le sous-espace vectoriel de $\bigotimes_{i\in\mathbb{Z}} \mathcal{B}$ engendré par $\mathcal{F}$.
On pose alors :

$$\mathcal{H} = \mathcal{P} \otimes \mathcal{Q} \otimes \mathcal{M}$$

C'est un espace de Hilbert. Il admet une base orthonormée formée des vecteurs

$$|e_x\rangle \otimes |n_0, n_1, \ldots, n_{M-1}\rangle \otimes |\ldots m_{-1}, m_0, m_1, \ldots\rangle$$

que l'on notera aussi

$$|x; n_0, n_1, \ldots, n_{M-1}; \ldots m_{-1}, m_0, m_1, \ldots\rangle .$$

Une machine de Deutsch (à une bande) sur cet espace de configurations est définie par trois opérateurs linéaires $U_{-1}, U_0, U_1 : \mathcal{Q} \otimes \mathcal{B} \to \mathcal{Q} \otimes \mathcal{B}$ tels que l'opérateur linéaire $U : \mathcal{H} \to \mathcal{H}$ ci-dessous est unitaire :

$$\begin{aligned} U|x\rangle \otimes |n\rangle \otimes |m\rangle &= |x-1\rangle \otimes U_{-1}|n, m_x\rangle \otimes \bigotimes_{y\neq x} |m_y\rangle \\ &+ |x\rangle \otimes U_0|n, m_x\rangle \otimes \bigotimes_{y\neq x} |m_y\rangle \\ &+ |x+1\rangle \otimes U_1|n, m_x\rangle \otimes \bigotimes_{y\neq x} |m_y\rangle \qquad (4) \end{aligned}$$

La machine déterminée par $M, U_{-1}, U_0, U_1$ est dite *rationnelle* si les opérateurs $U_j$ ont des matrices (dans la base canonique) à coefficients rationnels.

9- Montrer que, étant donnés un entier $M$ et trois matrices $(M+1)\times(M+1)$ à coefficients rationnels $U_{-1}, U_0, U_1$, on peut décider si (4) définit une transformation unitaire de $\mathcal{H}$.
10- Etant donnée une machine de Bennett $\mathbb{M}$ sur l'ensemble d'états $\{0,1\}^M$ et l'alphabet $\{0,1\}$, on définit des transformations linéaires $U_{-1}, U_0, U_1$ par :

$$\begin{aligned} U_{-1}\,|n;b\rangle &= Z_{-1}(n,b)\,|A(n;b)\rangle \\ U_0\,|n;b\rangle &= Z_0(n,b)\,|A(n;b)\rangle \\ U_1\,|n;b\rangle &= Z_1(n,b)\,|A(n;b)\rangle \end{aligned} \tag{5}$$

où $A : \{0,1\}^{M+1} \to \{0,1\}^{M+1}$ et $Z : \{0,1\}^{M+1} \to \{0,1\}$ sont définies par :
$Z_d(n,b) = 1$ ssi la machine $\mathbb{M}$ meut sa tête dans la direction $d$, en partant de l'état n et en lisant la lettre $b$
$A(n,b) = (n',b')$ ssi la machine $\mathbb{M}$ passe dans l'état $n'$ et écrit $b'$ en partant de l'état n et en lisant la lettre $b$.
Montrer que, si $\mathbb{M}$ est réversible totale, alors (5) définit une bien une machine de Deutsch.

**Fonction calculée** Soit D la machine de Deutsch définie par $M, U_{-1}, U_0, U_1$.
On code l'alphabet $\{b, a_0, a_1, \#\}$ par les mots $\{0000, 0001, 0011, 0111\}$. Ce codage est noté $K : \{b, a_0, a_1, \#\}^* \to \{0,1\}^*$.
On dit que D *calcule* la fonction $f : \{a_0, a_1\}^* \to \{a_0, a_1\}^*$ ssi , pour tout mot $u \in \{a_0, a_1\}^*$,
D1- partant de la configuration

$$c_0 = \left|0; 0^M; \ldots 0, 0, K(u), 0, 0, \ldots\right\rangle$$

(où le premier qbit de $K(u)$ se trouve en position 0) la machine atteint au moins une configuration $c_n$ telle que

$$\Pr_{c_n}(\{\text{premier qbit de l'état vaut1}\}) = 1$$

ssi $u \in$ Dom(f).
D2- la première configuration $c_n$ ayant cette propriété vérifie que :
presque sûrement, $K(u\#f(u)\#)$ est le contenu des qbits en position 0 à $4|u\#f(u)\#| - 1$.
11- On admet que pour toute fonction calculable $f : \{a_0, a_1\}^* \to \{a_0, a_1\}^*$, il existe une machine de Bennett réversible, totale, sur l'alphabet $\{0,1\}$ qui fait passer de $(q_0, K(u), 0)$ à $(q_1, K(u\#f(u)\#), 0)$ (adaptation au cas d'une seule bande des conditions B1, B2).
En déduire que toute fonction Turing-calculable est Deutsch-calculable.
* 12- Montrer que toute fonction Deutsch-calculable (avec coefficients rationnels) est Turing-calculable.

## Partie 3

Calcul quantique, variantes.

13- On modifie la définition de la *fonction calculée* par D :
D1 est inchangée, mais D2 est remplacée par
D'2- la première configuration $c_n$ ayant cette propriété vérifie que :

$\Pr_{c_n}$ ( $\{K(u\#f(u)\#)$ est le contenu des qbits en position 0 à $4|u\#f(u)\#| - 1\}$) $> \frac{2}{3}$ .

Comparer les fonctions Turing-calculables avec les fonctions Deutsch-calculables, en ce sens.
14- On suppose maintenant que les coefficients des matrices $U_{-1}, U_0, U_1$ appartiennent à $\mathbb{Q}[\sqrt{2}]$.
Reprendre, avec ces hypothèses, les questions 9,12.
15- Un nombre réel $r$ est dit *calculable* ssi, il existe une fonction totale, calculable $f_r : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ telle que :

$$f(n) = (p, q) \Rightarrow |r - \frac{p}{q}| < \frac{1}{n}.$$

15.1 Vérifier que l'ensemble $\mathbb{R}_c$ des nombres réels calculables, muni des opérations $+, \times$ est un sous-corps de $(\mathbb{R}, +, \times)$.
15.2 Vérifier que les opérations $+, \times$ sur $\mathbb{R}_c$ sont calculables, Vérifier que les opérations $r \mapsto -r$ sur $\mathbb{R}_c$ et $r \mapsto \frac{1}{r}$ sur $\mathbb{R}_c \setminus \{0\}$ sont calculables.
15.3 La question $r = s$? (resp. $r > s$?) pour des réels calculables, donnés par des fonctions $f_r, f_s$ est-elle décidable ? semi-décidable ? co-semi-décidable ?
16- On suppose maintenant que les coefficients des matrices $U_{-1}, U_0, U_1$ appartiennent à $\mathbb{R}_c$.
16.1 Avec ces hypothèses, et la définition D1,D2 reprendre les questions 9,12.
16.2 Avec ces hypothèses, et la définition D1,D'2 reprendre les questions 9,12.