ENSEIRB-MATMECA- Section Informatique, 2ième année
Option second semestre, 2014/2015

Information Quantique

DM- à rendre avant le 7 Avril 2015, à midi

Indications : Chaque partie dépend des parties précédentes.
Les questions affectées d'une étoile sont difficiles.
On peut *admettre* une question (voire même toute une partie) et utiliser les résultats de cette question (ou partie) dans la suite du problème.

Partie I

Automates finis réversibles.

Dans cette première partie, on définit des notions de *réversibilité* sur les automates finis et on étudie leur influence sur le pouvoir d'expression des automates finis.

Automates à groupe Un automate fini est un 5-uplet $\mathcal{A} =< X, Q, I, T, \tau >$ où

- X est un ensemble fini, l'alphabet d'entrée
- Q est un ensemble fini, l'ensemble des états
- $I \subseteq Q$ est l'ensemble des états initiaux
- $T \subseteq Q$ est l'ensemble des états terminaux
- $\tau \subseteq Q \times X \times Q$ est l'ensemble des transitions.

Pour toute lettre $x \in X$ on note $\mu_{\mathcal{A}}(x) := \{(q, q') \in Q \times Q \mid (q, x, q') \in \tau\}$. On étend $\mu_{\mathcal{A}}$ en un homorphisme de $\langle X^*, \cdot, \varepsilon\rangle$ dans le monoïde des relations binaires sur Q muni de la loi de composition :

$$R \circ R' := \{(p, r) \in Q \times Q \mid \exists q \in Q, (p, q) \in R \text{ et } (q, r) \in R'\}.$$

Le langage reconnu par $\mathcal{A}$ est :

$$\mathrm{L}(\mathcal{A}) := \{w \in X^* \mid \mu_{\mathcal{A}}(w) \cap I \times T \neq \emptyset\}$$

Autrement dit : un mot w est reconnu par $\mathcal{A}$ ssi il admet au moins un calcul partant d'un état initial et arrivant dans un état final.

L'automate fini $\mathcal{A}$ est dit *déterministe* ssi l'ensemble I ne possède qu'un élément et, pour toute lettre $x \in X$ la relation $\mu_{\mathcal{A}}(x)$ est une *fonction*. L'automate fini $\mathcal{A}$ est dit *à groupe* ssi l'ensemble I ne possède qu'un élément et,

pour toute lettre $x \in X$, $\mu_{\mathcal{A}}(x)$ est une *bijection* de Q dans Q.

1- Montrer que les langages suivants sont des langages à groupe :

$$\{a^n \mid n \text{ est pair}\}, \quad \{w \in \{a,b\}^* \mid |w|_a - |w|_b \equiv 1 \pmod 3\}$$

2- Montrer que, si L est un langage à groupe, alors il vérifie le " lemme d'itération" suivant :

$$\forall w \in X^*, \exists k \in \mathbb{N} \setminus \{0\}, \forall u, v \in X^*, \quad uw^k v \in L \Leftrightarrow uv \in L.$$

3- Montrer que le langage $(ab)^*$ n'est pas "à groupe".

Automates réversibles Un automate fini $< X, Q, I, T, \tau >$ est dit *réversible* ssi l'ensemble I ne possède qu'un élément et, pour toute lettre $x \in X$, $\mu_{\mathcal{A}}(x)$ est une injection partielle de Q dans Q i.e. :

$$\forall x \in X, \forall q, q', r \in Q, [(q,r) \in \mu_{\mathcal{A}}(x) \text{ et } (q',r) \in \mu_{\mathcal{A}}(x)] \Rightarrow q = q'.$$

4- Construire un automate réversible qui reconnaît $(ab)^*$.

Soit $\langle M, \cdot, 1_M \rangle$ un monoïde. On dit que $m \in M$ est *idempotent* ssi $m \cdot m = m$.
5- Vérifier que si M est un groupe, il n'a qu'un idempotent (l'élément neutre).
6- Soit Q un ensemble. Notons $I(Q)$ l'ensemble des injections partielles de Q dans Q. On vérifie que $\langle I(Q), \circ, \mathrm{Id}_Q \rangle$ est un monoïde.
Quels sont les idempotents de ce monoïde ?
7- Montrer que si e, f sont des idempotents du monoïde $\langle I(Q), \circ, \mathrm{Id}_Q \rangle$, alors $e \circ f = f \circ e$.

On rappelle que la congruence syntaxique d'un langage $L \subseteq X^*$ est définie par, pour tous $w, w' \in X^*$, $w \equiv_L w'$ ssi :

$$\forall u, v \in X^*, u \cdot w \cdot v \in L \Leftrightarrow u \cdot w' \cdot v \in L$$

Le monoïde syntaxique du langage L est le quotient $X^*/\equiv_L$.
8 *- Montrer que, si L est un langage réversible, alors, dans le monoïde $X^*/\equiv_L$, les idempotents commutent.
Aide : Montrer que si $\varphi : M_1 \to M_2$ est un homomorphisme surjectif de monoïdes et M_1 est fini, alors $\forall e_2 \in M_2, (e_2 = e_2 \cdot e_2 \Rightarrow \exists e_1 \in M_1, e_1 = e_1 \cdot e_1 \text{ et } e_2 = \varphi(e_1))$.
9- Montrer que a^*b^* n'est pas réversible.

Partie II

Automates finis avec multiplicités.

Dans cette seconde partie, on définit les notions de série formelle et de langage à seuil. On associe à tout automate fini " avec multiplicités" dans un corps K, une série et (lorsque K est ordonné) une famille de langages. Dans tout ce qui suit K est un corps commutatif (le plus souvent $K = \mathbb{Q}$ ou $K = \mathbb{R}$ ou $K = \mathbb{C}$).

Séries formelles générales Une *série formelle*, sur l'ensemble d'indéterminées (non-commutatives) X, à coefficients dans K est une application $S : X^* \to K$. On la note aussi :

$$S = \sum_{w \in X^*} S(w) \cdot w.$$

On dénote par $K\langle\langle\ X\ \rangle\rangle$ l'ensemble des séries formelles à coefficients dans K sur l'ensemble d'indéterminées X. On définit sur les séries formelles les opérations suivantes : pour tous $S, T \in K\langle\langle\ X\ \rangle\rangle, k \in K$,
le *produit externe* $k \cdot S$:

$$\forall w \in X^*, (k \cdot S)(w) := k \cdot S(w)$$

la *somme* $S + T$:

$$\forall w \in X^*, (S + T)(w) := S(w) + T(w)$$

le *produit de Hadamard* $S \odot T$:

$$\forall w \in X^*, (S \odot T)(w) := S(w) \cdot T(w)$$

le *produit de convolution* $S \cdot T$:

$$\forall w \in X^*, S \cdot T(w) = \sum_{u \cdot v = w} S(u) \cdot T(v).$$

Séries formelles reconnaissables Un automate fini avec multiplicités dans K (K-automate, en abrégé) est un 5-uplet $\mathcal{A} =< X, Q, I, T, \tau >$ où

- X est un ensemble fini, l'alphabet d'entrée
- $Q = \{q_0, \ldots, q_{d-1}\}$ est un ensemble fini, l'ensemble des états
- $I \in K^{1 \times d}$ est le vecteur-ligne initial
- $T \in K^{d \times 1}$ est le vecteur-colonne terminal
- $\tau \subseteq Q \times X \times K \times Q$ est l'ensemble des transitions

Pour toutre lettre $x \in X$, on note $\mu_{\mathcal{A}}(x) \in K^{d\times d}$ la matrice dont le coefficient en ligne i, colonne j est :

$$\mu_{\mathcal{A}}(x)_{i,j} := \sum_{(q_i,x,k,q_j)\in\tau} k$$

On étend $\mu_{\mathcal{A}}$ en un homorphisme de $\langle X^*, \cdot, \varepsilon\rangle$ dans le monoïde des matrices carrées $d \times d$ à coefficients dans K. La série reconnue par $\mathcal{A}$ est :

$$\mathrm{S}(\mathcal{A}) : w \mapsto I \cdot \mu_{\mathcal{A}}(w) \cdot T$$

Une série $S \in K\langle\langle\ X\ \rangle\rangle$ est dite K-reconnaissable ssi il existe un K-automate fini $\mathcal{A}$ tel que $S = \mathrm{S}(\mathcal{A})$.
1.a- Montrer que pour tout $k \in K$, la série constante : $w \mapsto k$ est K-reconnaissable.
1.b- Donner des automates avec multiplicités dans $\mathbb{R}$ qui reconnaissent les séries sur $X = \{a, b\}$:

$$S_1 = \sum_{w\in\{a,b\}^*} |w|_a w, \quad S_2 = \sum_{w\in\{a,b\}^*} cos(|w|\theta)w$$

pour un nombre $\theta \in \mathbb{R}$ quelconque.
2- Montrer que si $S, T \in K\langle\langle\ X\ \rangle\rangle$ sont K-reconnaissables et $k \in K$ alors :
2.a- $k \cdot S$ est K-reconnaissable
2.b- $S + T$ est K-reconnaissable.
2.c- $S \odot T$ est K-reconnaissable.
2.d- $S \cdot T$ est K-reconnaissable.
3- Montrer que $\sum_{w\in\{a,b\}^*}(|w|_a - |w|_b)w$ est $\mathbb{Q}$-reconnaissable.
4- Montrer que, pour tout $\theta \in \mathbb{R}$, $\sum_{w\in\{a,b\}^*} \cos^2((|w|_a - |w|_b)\theta)w$ est $\mathbb{R}$-reconnaissable.

Langages à seuil Soit $S \in \mathbb{R}\langle\langle\ X\ \rangle\rangle$. Pour tout nombre $\lambda \in \mathbb{R}$, on définit le langage :

$$L := \{w \in X^*, S(w) > \lambda\}. \tag{1}$$

On dit que L est le langage défini par la série S et le *seuil* λ.
Une série $\mathbb{R}$-reconnaissable S est dite *bornée* ssi il existe un $\mathbb{R}$-automate $\mathcal{A} =< X, Q, I, T, \tau >$ et un nombre $C \in \mathbb{R}$ tels que :

$$S = \mathrm{S}(\mathcal{A}) \quad \text{et} \quad \forall w \in X^*, \|I \cdot \mu_{\mathcal{A}}(w)\| \leq C. \tag{2}$$

Le seuil λ est dit *isolé* (pour la série S) ssi, il existe un nombre réel $\delta > 0$ tel que :

$$\forall w \in X^*, |S(w) - \lambda| \geq \delta. \tag{3}$$

5- Montrer que tout langage rationnel est aussi un langage à seuil défini par une série $\mathbb{Q}$-reconnaissable, avec un seuil isolé.
6- Montrer que les langages suivants sont des langages à seuil définis par des séries $\mathbb{R}$-reconnaissables :

$$\{w \in \{a,b\}^* \mid |w|_a > |w|_b\}, \quad \{w \in \{a,b\}^* \mid |w|_a \neq |w|_b\}.$$

Aide : on pourra s'inspirer des questions 3,4 (de la même partie)
7- Montrer que, si S est $\mathbb{R}$-reconnaissable bornée (i.e. vérifie (2)) alors, il existe $C' \in \mathbb{R}$ tel que, pour tout vecteur $\vec{u} \in \text{vect}(\{I \cdot \mu_{\mathcal{A}}(w) \mid w \in X^*\})$:

$$\|\vec{u} \cdot \mu_{\mathcal{A}}(w)\| \leq C'\|\vec{u}\| \tag{4}$$

8- Soit $W \subseteq X^*$ un ensemble infini de mots. Montrer que :

$$\forall \varepsilon > 0, \exists w, w' \in W, w \neq w' \text{ et } \|I \cdot \mu_{\mathcal{A}}(w) - I \cdot \mu_{\mathcal{A}}(w')\| < \varepsilon \tag{5}$$

9 *- Supposons que le langage L soit défini par (1), avec S, λ vérifiant (2) et (3) et qu'il existe un ensemble infini $W = \{w_i \mid i \in \mathbb{N}\}$ de mots tels que $i \neq j \Rightarrow w_i^{-1}L \neq w_j^{-1}L$.
Montrer que ces hypothèses sont contradictoires.
10- En déduire que, si L est défini par une série rationnelle bornée et un seuil isolé λ, alors L est rationnel.
11- Supposons que S soit définie par un $\mathbb{Q}$-automate $\mathcal{A}$, que le seuil λ soit rationnel et que l'on connaisse des nombres rationnels C, δ vérifiant (2)(3). Peut-on alors *calculer* un automate fini reconnaissant L ?
12- Donner un exemple de série reconnaissable non-bornée et de seuil isolé définissant un langage à seuil L non-rationnel.
13- Donner un exemple de série reconnaissable bornée et de seuil non-isolé, définissant un langage à seuil L non-rationnel.

Partie III

Automates finis quantiques à une mesure.

Dans cette troisième partie, on se concentre sur le cas de $\mathbb{C}$-automates finis qui sont *quantiques* i.e. où les matrices $\mu_{\mathcal{A}}(x)$ sont *unitaires*.

Séries Une série $S : X^* \to \mathbb{R}$ est dite "quantique à une mesure" (abbrévié par l'acronyme anglo-saxon MOQ) ssi elle est de la forme suivante :

$$S(w) = \|I \cdot \mu(w) \cdot P\|^2$$

où d est un entier naturel, $\mu : X^* \to \mathsf{U}(d)$ un homomorphisme de monoïdes, $I \in \mathbb{C}^{1\times d}$ est un vecteur-ligne de norme 1 (pour la norme ℓ_2) et $P : \mathbb{C}^d \to \mathbb{C}^d$ est une projection orthogonale sur un sous-espace de $\mathbb{C}^d$.
On remarquera :
- que $w \mapsto I \cdot \mu(w) \cdot T$ est une série $\mathbb{C}$-reconnaissable, pour tout vecteur $T \in \mathbb{C}^{d\times 1}$
- que $S(w)$ peut être vue comme la probabilité que le résultat du calcul quantique suivant donne une valeur fixe $\nu : \mathbb{C}^d$ muni de la norme ℓ_2 est un espace de Hilbert qui est l'espace des états ; on part de l'état I, puis on applique la suite des transformations unitaires $\mu(w[0]), \mu(w[1], \dots \mu(w[n-1])$ correspondant aux lettres de w ; puis on mesure une observable ; P est la projection orthogonale sur le sous-espace propre de ν.

1- Montrer que, si S est une série MOQ, alors elle vérifie la propriété suivante :

$$\forall w \in X^*, \forall \varepsilon > 0, \exists k \in \mathbb{N} \setminus \{0\}, \forall u, v \in X^*, \ \ |S(uw^k v) - S(uv)| < \varepsilon.$$

Aide : on utilisera la norme des matrices, le fait que cette norme vaut 1 pour toute matrice unitaire et le fait que, pour toutes matrices U, V, $\|U \cdot V\| \leq \|U\| \cdot \|V\|$.

Langages à seuil Un langage L est dans la classe MOQ ssi il est de la forme (1) où S est une série MOQ. Il est dans la classe MOQ-is, si il est de la forme (1) pour une série MOQ S et un seuil λ isolé pour S.
2- Montrer que tout langage à groupe est aussi un langage MOQ-is.
3- Montrer que le langage $\{w \in \{a, b\}^*, |w|_a \neq |w|_b\}$ est un langage MOQ.
4- Montrer que, si L est un langage MOQ-is, alors il vérifie le
"lemme d'itération" suivant :

$$\forall w, u, v \in X^*, \exists k \in \mathbb{N} \setminus \{0\}, \quad uw^k v \in L \Leftrightarrow uv \in L.$$

5- Montrer que le langage $(ab)^*$, qui est réversible (partie I), n'est pas MOQ-is.
6 *- Montrer que tout langage MOQ-is est rationnel.
7- Le seuil λ utilisé pour résoudre la question 3 peut-il être choisi isolé ?

Partie IV

Automates finis quantiques multi-mesures.

Dans cette quatrième partie, on considère le cas de $\mathbb{C}$-automates finis qui sont *quantiques* (i.e. où les matrices $\mu_{\mathcal{A}}(x)$ sont *unitaires*) dont chaque pas de calcul est formé d'une transition unitaire *suivie d'une mesure*.

Séries Une série $S : X^* \to \mathbb{R}$ est dite "quantique multi-mesure" (abrévié par l'acronyme anglo-saxon MMQ) ssi elle est de la forme suivante :

$$S(w) = \|I \cdot \mu(w) \cdot U \cdot P\|^2$$

où $\mu : X^* \to \mathbb{C}^{d\times d}$ est un homomorphisme de monoïdes, d un entier naturel,$I \in \mathbb{C}^{1\times d}$ est un vecteur de norme 1 (pour la norme ℓ_2),$U, P \in \mathbb{C}^{d\times d}$ sont (respectivement) une matrice unitaire et une projection orthogonale et, pour toute lettre $x \in X$

$$\mu(x) = U(x) \cdot P(x) \tag{6}$$

où $U(x)$ est une matrice unitaire et $P(x)$ est une projection orthogonale.

Langages à seuil Un langage L est dans la classe MMQ ssi il est de la forme (1) où S est une série MMQ. Il est dans la classe MMQ-is, si il est de la forme (1) pour une série MMQ S et un seuil λ isolé pour S.
1 *- Montrer que tout langage réversible (voir partie I) est aussi un langage MMQ-is.
2- Montrer que tout langage MOQ-is est MMQ-is, mais qu'il existe un langage MMQ-is qui n'est pas MOQ-is.
3 *- Montrer que tout langage MMQ-is est rationnel.