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

Information Quantique

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

Partie I

Automates finis réversibles.

Automates à groupe 1- Choisissons $\mathcal{A}_1 :=< \{a\}, \{0,1\}, \{0\}, \{0\}, \tau_1 >$ où τ_1 est définie par le tableau :

τ_1	a
0	1
1	0

On vérifie que, pour tout $i \in Q$ et tout $u \in \{a\}^*$:

$$\tau^*(i,u) \equiv i + |u| \pmod 2$$

Donc

$$\mathrm{L}(\mathcal{A}_1) = \{a^n \mid n \text{ est pair}\}.$$

Choisissons $\mathcal{A}_2 :=< \{a,b\}, \{0,1,2\}, \{0\}, \{1\}, \tau_2 >$ où τ_2 est définie par le tableau :

τ_2	a	b
0	1	2
1	2	0
2	0	1

On vérifie que, pour tout $i \in Q$ et tout $u \in \{a,b\}^*$, :

$$\tau^*(i,u) \equiv i + |u|_a - |u|_b \pmod 3$$

Donc

$$\mathrm{L}(\mathcal{A}_2) = \{w \in \{a,b\}^* \mid |w|_a - |w|_b \equiv 1 \pmod 3\}.$$

2- Supposons que L est un langage à groupe, reconnu par un automate fini "à groupe" $\mathcal{A} =< X, Q, I, T, \tau >$. L'application $\mu_{\mathcal{A}} : X^* \to \mathcal{S}_Q$ est un homomorphisme du monoide X^* dans le groupe des permutations de Q. Comme ce groupe a pour cardinal $|Q|!$, on sait que tout élément de ce groupe vérifie $g^{|Q|!} = 1$. Posons $k := |Q|!$. Pour tout $w \in X^*$:

$$\mu_{\mathcal{A}}(w^k) = (\mu_{\mathcal{A}}(w))^k = \mathrm{Id}_Q.$$

Soient maintenant deux mots quelconques $u, v \in X^*$. On a :

$$\mu_{\mathcal{A}}(uw^k v) = \mu_{\mathcal{A}}(u) \circ \mu_{\mathcal{A}}(w)^k \circ \mu_{\mathcal{A}}(v) = \mu_{\mathcal{A}}(u) \circ \mu_{\mathcal{A}}(v).$$

Comme, pour tout mot m, le fait d' être accepté (ou non) par $\mathcal{A}$ ne dépend que de $\mu_{\mathcal{A}}(m)$, l'égalité ci-dessus entraîne que :

$$\forall u, v \in X^*, \;\; uw^k v \in L \Leftrightarrow uv \in L.$$

N.B. Nous avons prouvé un lemme plus fort que celui demandé par l'énoncé, car le nombre k donné par notre solution est *indépendant* du mot w.
3- Considérons le langage $L := (ab)^*$.
Posons $w := a$. Pour tout entier $k > 0$: $aa^k b \notin L$ mais $ab \in L$.
Ce langage L ne vérifie donc pas le lemme d'itération de la question 2, donc il n'est pas "à groupe".

Automates réversibles 4- Choisissons $\mathcal{A}_3 :=< \{a, b\}, \{0, 1, 2\}, \{0\}, \{0\}, \tau_3 >$ où τ_3 est définie par le tableau :

τ_3	a	b
0	1	−
1	−	0

(le trait "-" indique une absence de transition). On vérifie que $\mathrm{L}(\mathcal{A}_3) = (ab)^*$.
5- Supposons que M est un groupe et $m \cdot m = m$. En multipliant les 2 membres par m^{-1} on obtient que $m = 1_M$, qed.
6- Soient $R \in I(Q)$. Supposons que $R \circ R = R$. Soit $x \in \mathrm{Dom(R)}$. Alors il existe $y, z \in Q$ tel que $(x, y) \in R$ et $(x, z) \in R \circ R$. Comme R est une application, $(y, z) \in R$,
Comme $R = R \circ R$, $y = z$ et $(y, y) \in R$.
On a donc $(x, y), (y, y) \in R$. Mais comme R est injective, $x = y$.
Finalement R est l' identité restreinte au sous-ensemble $D = \mathrm{Dom(R)}$.
Réciproquement, on vérifie que toute restriction de l' identité à un sous-ensemble de Q est un idempotent.
7- Soient e, f sont des idempotents du monoïde $\langle I(Q), \circ, \mathrm{Id}_Q \rangle$. D'après la question 6, il existe des parties $D, D' \subseteq Q$ telles que : $e = \mathrm{I}_{|D}$ et $f = \mathrm{I}_{|D'}$.
Donc $e \circ f = \mathrm{I}_{|D \cap D'} = f \circ e$.
8 - Montrons le " lemme de relèvement des idempotents" : si $\varphi : M_1 \to M_2$ est un homomorphisme surjectif de monoïdes et M_1 est fini, alors $\forall e_2 \in M_2, (e_2 = e_2 \cdot e_2 \Rightarrow \exists e_1 \in M_1, e_1 = e_1 \cdot e_1$ et $e_2 = \varphi(e_1))$.
On vérifie que, pour tout monoide fini M et tout $m \in M$, il existe un entier

$0 \leq k \leq |M|$ tel que : $x^k = x^{2k}$.
Soit e_2 un idempotent de M_2. Comme φ est surjective, il existe $m_1 \in M_1$ tel que $\varphi(m_1) = e_2$. Soit $k > 0$ un entier tel que $m_1^k = m_1^{2k}$. On a :

$$\varphi(m_1^k) = \varphi(m_1)^k = m_2^k = m_2$$

(puisque m_2 est idempotent). Posons $e_1 := m_1^k$. On a bien $\varphi(e_1) = e_2$ et $e_1^2 = e_1$.
Supposons maintenant que L est un langage reconnu par un automate fini réversible $\mathcal{A} =< X, Q, I, T, \tau >$. Considérons le monoide $M_{\mathcal{A}}$ ("le monoide transition" de $\mathcal{A}$) défini par :

$$D_{\mathcal{A}} := \{\mu_{\mathcal{A}}(w) \mid w \in X^*\}, \quad M_{\mathcal{A}} := \langle D_{\mathcal{A}}, \circ, \mathrm{Id_Q}\rangle.$$

Il s'agit d'un sous-monoide de $\langle I(Q), \circ, \mathrm{Id}_Q\rangle$, donc dans ce monoide, les idempotents commutent.
Définissons une application $\varphi : D_{\mathcal{A}} \to X^*/\equiv_L$ par :

$$\varphi(\mu_{\mathcal{A}}(w)) := [w]_{\equiv_L}.$$

Cette définition est bien posée car, si $\mu_{\mathcal{A}}(w) = \mu_{\mathcal{A}}(w')$ on a aussi $w \equiv_L w'$. De plus

$$\begin{aligned} \varphi(\mu_{\mathcal{A}}(w) \cdot \mu_{\mathcal{A}}(w')) &= \varphi(\mu_{\mathcal{A}}(w \cdot w')) \\ &= [w \cdot w']_{\equiv_L} \\ &= [w]_{\equiv_L} \cdot [w']_{\equiv_L} \\ &= \varphi(\mu_{\mathcal{A}}(w)) \cdot \varphi(\mu_{\mathcal{A}}(w')) \end{aligned}$$

et

$$\varphi(\mu_{\mathcal{A}}(\varepsilon)) = [\varepsilon]_{\equiv_L}$$

ce qui montre que φ est un homomorphisme de monoides. Il est surjectif : tout élément de $X^*/\equiv_L$ est de la forme $[w]_{\equiv_L}$ qui est aussi de la forme $\varphi(\mu_{\mathcal{A}}(w))$.
Par le lemme de relèvement des idempotents, si e, f sont des idempotents de $X^*/\equiv_L$ ils sont de la forme $e = \varphi(e'), f = \varphi(f')$ pour des idempotents e', f' de $M_{\mathcal{A}}$. Par la question 7, $e'f' = f'e'$ et, en appliquant φ à cette égalité, $ef = fe$. On a prouvé que, dans $X^*/\equiv_L$, les idempotents commutent.
9- Notons $L = a^*b^*$. On a alors

$$a \equiv_L a^2, \quad b \equiv_L b^2, \text{ mais } ab \not\equiv_L ba$$

puisque, par exemple $a(ab)b \in L$ mais $a(ba)b \notin L$. Le monoide syntaxique $X^*/\equiv_L$ ne vérifie donc pas la condition nécessaire trouvée à la question 8. Donc L n'est pas réversible.

Partie II

Automates finis avec multiplicités.

Séries formelles reconnaissables 1.a- Soit $k \in K$. Posons :
$\mathcal{A} =< X, \{q_0\}, (k), (1), \tau >$ où τ est définie par le tableau :

τ	$x \in X$
q_0	q_0

La série constante : $w \mapsto k$ est bien égale à

$$w \mapsto k \cdot \mu_{\mathcal{A}}(w) \cdot 1$$

puisque $\mu_{\mathcal{A}}(w) = \mathrm{Id}_Q$.
1.b- Posons : $\mathcal{A}_1 =< \{a, b\}, \{q_0, q_1\}, (1, 0), (0, 1)^t, \tau_1 >$ où τ_1 est définie par le tableau :

τ_1	a	b
q_0	$q_0 + q_1$	q_0
q_1	q_1	q_1

On vérifie que

$$\mathrm{S}(\mathcal{A}_1) = \sum_{w \in \{a,b\}^*} |w|_a w$$

Cherchons un a.f. avec mutiplicités dans $\mathbb{R}$ qui reconnaisse

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

On remarque que, pour tout entier n :

$$\cos(n\theta) = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

L'automate pourra être construit en choisissant :

$$I = \begin{pmatrix} 1 & 0 \end{pmatrix}, \ \ \mu(a) = \mu(b) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \ \ T = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

On définit donc $\mathcal{A}_2 =< \{a, b\}, \{q_0, q_1\}, (1, 0), (1, 0)^t, \tau_2 >$ où τ_2 est définie par le tableau :

τ_2	a	b
q_0	$\cos(\theta)q_0 - \sin(\theta)q_1$	$\cos(\theta)q_0 - \sin(\theta)q_1$
q_1	$\sin(\theta)q_0 + \cos(\theta)q_1$	$\sin(\theta)q_0 + \cos(\theta)q_1$

On vérifie que

$$\mathrm{S}(\mathcal{A}_2) = \sum_{w\in\{a,b\}^*} cos(|w|\theta)w$$

2- Supposons que, pour tout $w \in X^*$:

$$S_1 = I_1 \cdot \mu_1(w) \cdot T_1, \;\; S_2 = I_1 \cdot \mu_2(w) \cdot T_1.$$

où $I_j \in K^{1\times d_j}, \mu_j : X^* \to K^{d_j\times d_j}, T_j \in K^{d_j\times 1}$.
2.a Posons $I = k \cdot I_1$

$$(k \cdot S_1)(w) = I \cdot \mu_1(w) \cdot T_1.$$

2.b Posons $I = (I_1, I_2) \in K^{1\times d_1+d_1}$, $\mu(x) = \begin{pmatrix} \mu_1(x) & 0_{d_1\times d_2} \\ 0_{d_2\times d_1} & \mu_2(x) \end{pmatrix} T = \begin{pmatrix} T_1 \\ T_2 \end{pmatrix}$
Alors :

$$(S_1 + S_2)(w) = I \cdot \mu(w) \cdot T$$

autrement dit,la somme directe des représentations linéaires de S_1, S_2 représente $S_1 + S_1$.
2.c Posons $I = I_1 \otimes I_2 \in K^{1\times d_1\cdot d_2}$, $\mu(x) = \mu_1(x) \otimes \mu_2(x) \in K^{d_1\cdot d_2\times d_1\cdot d_2}$, $T = T_1 \otimes T_2 \in K^{d_1\cdot d_2\times 1}$. Alors :

$$(S_1 \odot S_2)(w) = I \cdot \mu(w) \cdot T$$

autrement dit, le produit tensoriel des représentations linéaires de S_1, S_2 représente $S_1 \odot S_2$.
2.d On construit une représentation linéaire de dimension $d_1 + d_2$:

$$I = \begin{pmatrix} I_1 & I_1T_1I_2 \end{pmatrix}, \;\; T = \begin{pmatrix} 0_{d_1,1} \\ T_2 \end{pmatrix}$$

et $\mu(x) \in K^{(d_1+d_1)\times(d_1+d_2)}$ est définie par :

$$\mu(x) = \begin{pmatrix} \mu_1(x) & \mu_1(x)T_1I_2 \\ 0_{d_2,d_1} & \mu_2(x) \end{pmatrix}$$

On montre, par récurrence sur la longueur de w que :

$$\mu(w) = \begin{pmatrix} \mu_1(w) & \sum_{uv=w,u\neq\varepsilon} \mu_1(u)T_1I_2\mu_2(v) \\ 0_{d_2,d_1} & \mu_2(w) \end{pmatrix}$$

On en conclut que :

$$\begin{aligned}\begin{pmatrix} I_1 & I_1T_1I_2 \end{pmatrix} \cdot \mu(w) \cdot \begin{pmatrix} 0_{d_1,1} \\ T_2 \end{pmatrix} &= \begin{pmatrix} I_1\mu_1(w) & (\sum_{uv=w,u\neq\varepsilon} S_1(u)I_2\mu_2(v)) + I_1T_1I_2\mu_2(w) \end{pmatrix} \cdot \begin{pmatrix} 0_{1,d_1} \\ T_2 \end{pmatrix} \\ &= \sum_{uv=w,u\neq\varepsilon} S_1(u)S_2(v) + I_1T_1S_2(w) \\ &= (S_1 \cdot S_2)(w).\end{aligned}$$

3- On a vu à la question 1.b que $S_1 = \sum_{w\in\{a,b\}^*} |w|_a w$ est reconnue par l'automate $\mathcal{A}_1$. Comme tous les coefficients des transitions de $\mathcal{A}_1$ sont dans $\mathbb{Q}$, S_1 est $\mathbb{Q}$-reconnaissable.
En échangeant $\mu(a)$ et $\mu(b)$ dans $\mathcal{A}_1$, on obtient un automate $\mathcal{A}_1'$ qui reconnaît $S_1' = \sum_{w\in\{a,b\}^*} |w|_b w$. Comme l'ensemble des séries $\mathbb{Q}$-reconnaissables est clos par combinaisons $\mathbb{Q}$-linéaires, $S_1 - S_1' = \sum_{w\in\{a,b\}^*}(|w|_a - |w|_b)w$ est $\mathbb{Q}$-reconnaissable.
4- Soit $\theta \in \mathbb{R}$. En nous inspirant de la question 1.b on définit l' automate : $\mathcal{A}_4 =< \{a,b\}, \{q_0,q_1\}, (1,0), (1,0)^t, \tau_4 >$ où τ_4 est définie par le tableau :

τ_4	a	b
q_0	$\cos(\theta)q_0 - \sin(\theta)q_1$	$\cos(\theta)q_0 + \sin(\theta)q_1$
q_1	$\sin(\theta)q_0 + \cos(\theta)q_1$	$-\sin(\theta)q_0 + \cos(\theta)q_1$

et l'on a

$$\mathrm{S}(\mathcal{A}_4) = \sum_{w\in\{a,b\}^*} \cos((|w|_a - |w|_b)\theta)w.$$

Comme l'ensemble des séries $\mathbb{Q}$-reconnaissables est clos par produit de Hadamard, $\sum_{w\in\{a,b\}^*} \cos^2((|w|_a - |w|_b)\theta)w$ est $\mathbb{Q}$-reconnaissable.

Langages à seuil 5- Soit $L \subseteq X^*$ un langage reconnaissable. Il est reconnu par un a.f. déterministe $\mathcal{A} =< X, Q, I, T, \tau >$ où $I, T \subseteq Q$ et $\tau \subseteq Q \times X \times Q$. Supposons que $Q = \{0, 1, \ldots, n-1\}$.
On définit un automate $\mathcal{A}_{\mathbb{Q}} =< X, Q, I_{\mathbb{Q}}, T_{\mathbb{Q}}, \tau_{\mathbb{Q}} >$ avec multiplicités dans $\mathbb{Q}$ en posant :
$I_{\mathbb{Q}}$ (resp. $T_{\mathbb{Q}}$) est le vecteur-ligne (resp. colonne) tel que :

$I_{\mathbb{Q},1,j} = 1$ si $j \in I$, $I_{\mathbb{Q},1,j} = 0$ si $j \notin I$, $T_{\mathbb{Q},j,1} = 1$ si $j \in T$, $T_{\mathbb{Q},j,1} = 0$ si $j \notin T$.

(en quelque sorte on " traduit" le booléen 0 (resp. 1) par le nombre rationnel 0 (resp. 1)). On définit :

$$\tau_{\mathbb{Q}} := \{(q,x,1,q') \in Q \times X \times \mathbb{Q} \times Q \mid (q,x,q') \in \tau\})$$

On vérifie que, pour tout $w \in X^*$:

$$\mathrm{S}(\mathcal{A}_{\mathbb{Q}})(w) = 1 \text{ si } w \in \mathrm{L}(\mathcal{A}), \;\; \mathrm{S}(\mathcal{A}_{\mathbb{Q}})(w) = 0 \text{ si } w \notin \mathrm{L}(\mathcal{A}).$$

Donc

$$L = \{w \in X^*, \mathrm{S}(\mathcal{A}_{\mathbb{Q}})(w) > \frac{1}{2}\}.$$

Par ailleurs, comme les coefficients de $\mathrm{S}(\mathcal{A}_{\mathbb{Q}})$ sont dans $\{0,1\} \subseteq \mathbb{Q}$,

$$\forall w \in X^*, |\mathrm{S}(\mathcal{A}_{\mathbb{Q}})(w) - \frac{1}{2}| \geq \frac{1}{2}.$$

Le seuil $\frac{1}{2}$ est donc isolé.
6- Notons

$$S_3 = \sum_{w \in \{a,b\}^*} (|w|_a - |w|_b)w,$$

choisissons $\theta = \frac{\pi}{\sqrt{2}}$ et notons

$$S_4 = \sum_{w \in \{a,b\}^*} \cos^2((|w|_a - |w|_b)\theta)w.$$

On a :

$$\{w \in \{a,b\}^* \mid |w|_a > |w|_b\} = \{w \in \{a,b\}^* \mid S_3(w) > 0\}$$

$$\{w \in \{a,b\}^* \mid |w|_a \neq |w|_b\} = \{w \in \{a,b\}^* \mid -S_4(w) > -1\}.$$

Or, par les questions 2.a,3,4 S_3 et $-S_4$ sont des séries $\mathbb{R}$-rationnelles.
7- Supposons que S, reconnue par $\mathcal{A}$ à d états, vérifie (2).
Notons $V_{\mathcal{A}} = \mathrm{vect}(\{I \cdot \mu_{\mathcal{A}}(w) \mid w \in X^*\})$. Ce sous-espace de $\mathbb{R}^d$ est de dimension finie (en fait $\leq d$). Donc il existe une partie de $\{I \cdot \mu_{\mathcal{A}}(w) \mid w \in X^*\}$, de cardinal $\leq d$, qui est une base de $V_{\mathcal{A}}$: fixons une telle base

$$\mathcal{B}_{\mathcal{A}} = \{I \cdot \mu_{\mathcal{A}}(w_j) \mid j \in J\}.$$

Notons $\vec{u}_j = I \cdot \mu_{\mathcal{A}}(w_j)$ (pour tout $j \in J$).
L'espace vectoriel $V_{\mathcal{A}}$ admet une norme $\| * \|_1$ définie par :

$$\| \sum_{j \in J} \lambda_j \vec{u}_j \|_1 = \sum_{j \in J} |\lambda_j|.$$

Comme $V_{\mathcal{A}}$ est de dimension finie, les normes $\| * \|_1$ et $\| * \|_2$ sont équivalentes sur $V_{\mathcal{A}}$. Donc il existe une constante $K \in \mathbb{R}$ telle que :

$$\forall \vec{u} \in V_{\mathcal{A}}, \|\vec{u}\|_1 \leq K \cdot \|\vec{u}\|_2$$

Posons :

$$C' = K \cdot C$$

Soit $\vec{u} \in \text{vect}(\{I \cdot \mu_{\mathcal{A}}(w) \mid w \in X^*\})$: il est de la forme

$$\vec{u} = \sum_{j \in J} \lambda_j \vec{u}_j.$$

Pour tout $w \in X^*$:

$$\begin{array}{rcll}
\|\vec{u} \cdot \mu_{\mathcal{A}}(w)\|_2 = & \|\sum_{j\in J} \lambda_j \cdot \vec{u}_j \cdot \mu_{\mathcal{A}}(w)\|_2 & \\
= & \|\sum_{j\in J} \lambda_j \cdot I \cdot \mu_{\mathcal{A}}(w_j w)\|_2 & \\
\leq & (\sum_{j\in J} |\lambda_j|) \cdot \|I \cdot \mu_{\mathcal{A}}(w_j w)\|_2 & \\
\leq & (\sum_{j\in J} |\lambda_j|) \cdot C & \text{par (2)} \\
= & \|\vec{u}\|_1 \cdot C & \\
\leq & K \cdot \|\vec{u}\|_2 \cdot C & \text{par définition de } K \\
= & C' \cdot \|\vec{u}\|_2. &
\end{array}$$

8- Soit $W \subseteq X^*$ un ensemble infini de mots. Soit $w_0, w_1, \ldots, w_n, \ldots$ une numérotation des mots de W (i.e. $n \mapsto w_n$ est une injection de $\mathbb{N}$ dans W). Comme la boule fermée de rayon C, $B(0, C)$, est un sous-espace compact de $\mathbb{R}^d$, il existe une sous-suite $(I\mu_{\mathcal{A}}(w_{\varphi(n)}))_{n\geq 0}$ qui converge dans $B(0, C)$. Donc

$$\forall \varepsilon > 0, \exists n < m \text{ tels que } \|I \cdot \mu_{\mathcal{A}}(w_n) - I \cdot \mu_{\mathcal{A}}(w_m)\| < \varepsilon.$$

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 $i \neq j \Rightarrow w_i^{-1}L \neq w_j^{-1}L$.
Posons

$$\varepsilon = \frac{\delta}{C' \cdot \|T\|}.$$

Par la question 8, il existe des entiers $i \neq j$ tels que

$$\|I \cdot \mu_{\mathcal{A}}(w_i) - I \cdot \mu_{\mathcal{A}}(w_j)\| < \varepsilon.$$

Mais $w_i^{-1}L \neq w_j^{-1}L$. Choisissons un mot $w' \in X^*$ tel que :

$$w_i w' \in L \Leftrightarrow w_j w' \notin L.$$

On a donc :

$$\begin{aligned}
|S(w_iw') - S(w_jw')| = & \quad |I \cdot \mu_{\mathcal{A}}(w_iw') \cdot T - I \cdot \mu_{\mathcal{A}}(w_jw') \cdot T| \\
\leq & \quad \|I \cdot \mu_{\mathcal{A}}(w_iw') - I \cdot \mu_{\mathcal{A}}(w_jw')\| \cdot \|T\| \\
= & \quad \|(I \cdot \mu_{\mathcal{A}}(w_i) - I \cdot \mu_{\mathcal{A}}(w_j)) \cdot \mu_{\mathcal{A}}(w')\| \cdot \|T\| \\
\leq & \quad C' \cdot \|I \cdot \mu_{\mathcal{A}}(w_i) - I \cdot \mu_{\mathcal{A}}(w_j)\| \cdot \|T\| \qquad (\text{ par la qu.7}) \\
\leq & \quad C' \cdot \varepsilon \cdot \|T\| \qquad (\text{ par le choix des entiers } i, j \\
= & \quad \delta.
\end{aligned}$$

Or les deux nombres $S(w_iw'), S(w_jw')$ sont de part et d'autre de λ, donc

$$|S(w_iw') - S(w_jw')| \geq 2\delta$$

ce qui contredit l'inégalité juste au-dessus.
10- Soit L un langage défini par une série rationnelle bornée et un seuil isolé λ. Par la question 9, il n'existe pas d'ensemble infini $W = \{w_i \mid i \in \mathbb{N}\}$ de mots tels que $i \neq j \Rightarrow w_i^{-1}L \neq w_j^{-1}L$. Donc L n'a qu'un nombre fini de résiduels. Donc 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).
Etape 1 : On calcule une base de $V_{\mathcal{A}}$: il suffit de calculer, selon l'ordre croissant des longueurs des mots w, les vecteurs $I \cdot \mu_{\mathcal{A}}(w)$. Notons $V_{\mathcal{A},n}$ le sous-espace engendré par les mots w de longueur $\leq n$. Pour chaque longueur n :
- si $V_{\mathcal{A},n} = V_{\mathcal{A},n+1}$ alors $V_{\mathcal{A},n} = V_{\mathcal{A}}$
- sinon $\dim(V_{\mathcal{A},n}) < \dim(V_{\mathcal{A},n+1})$

Ce calcul s' arrête donc après au plus d étapes et fournit une base $\mathcal{B}$ de $V_{\mathcal{A}}$.
Etape 2 : On transforme la base $\mathcal{B}$ en une base $\mathcal{B}'$ de $V_{\mathcal{A}}$ qui est orthogonale. (Méthode classique en algèbre linéaire).
Etape 3 : Soit $\mathcal{B}' = (\vec{e}'_1, \ldots, \vec{e}'_{d'})$.
Posons

$$K := \frac{d'}{\min\{\|\vec{e}'_i\|_2 \mid 1 \leq i \leq d'\}}$$

On vérifie que :

$$\forall \vec{u} \in V_{\mathcal{A}}, \quad \|\vec{u}\|_1 \leq K \cdot \|\vec{u}\|_2$$

Etape 4 : Posons (comme à la question 9)

$$C' := K \cdot C, \quad \varepsilon := \frac{\delta}{C' \cdot \|T\|}$$

On définit la relation binaire R_ε sur X^* par :

$$R_\varepsilon(u,v) \Leftrightarrow \|I \cdot (\mu_{\mathcal{A}}(u) - \mu_{\mathcal{A}}(v))\| \leq \varepsilon.$$

On a vu à la question 9 que

$$R_\varepsilon(u,v) \Rightarrow u^{-1}L = v^{-1}L.$$

Etape 5 : Il existe un entier N tel que : pour tout mot $w \in X^*$ si $|w| \leq N$ alors il existe des préfixes $w_1 \prec w_2 \preceq w$ tels que

$$R_\varepsilon(w_1, w_2).$$

(Nous dirons dans ce cas que N est suffisant pour ε). En effet la boule $B(0,C)$ de $V_{\mathcal{A}}$ (muni de la norme ℓ_2) admet un recouvrement fini

$$\bigcup_{i=1}^{N} B(\vec{v}_i, \frac{\varepsilon}{2})$$

pour des points $\vec{v}_i \in \mathbb{R}^d$. Donc, si $|w| \leq N$, il existe un indice $i \in [1,N]$ et deux mots distincts w_1, w_2 de l'ensemble des préfixes de w, tels que $I \cdot \mu_{\mathcal{A}}(w_1) \in B(\vec{v}_i, \frac{\varepsilon}{2})$, $I \cdot \mu_{\mathcal{A}}(w_2) \in B(\vec{v}_i, \frac{\varepsilon}{2})$ et donc $R_\varepsilon(w_1, w_2)$.
Etape 6 :Comme R_ε peut être calculée, on peut déterminer un entier N qui est suffisant pour ε.
Etape 7 : Considérons l' automate fini $\mathcal{A}'$ suivant sur X :
- l'ensemble des états est $Q' := X^{\leq N}$ (l'ensemble des mots de longueur $\leq N$)
- l'état initial est ε (le mot vide)
- l'ensemble de transitions est

$$\tau' := \{(w,x,wx) \mid wx \in Q'\} \cup \{(w,x,w') \mid w' \prec w, w \in Q', R_\varepsilon(w',w)\}.$$

- l' ensemble des états finaux est $Q' \cap L$.
On vérifie que :
- tout mot w a un calcul dans cet automate fini, partant de l'état initial
- tout état u atteint en lisant w vérifie que $w^{-1}L = u^{-1}L$. (qed).
12- Reprenons le langage $L_3 = \{w \in \{a,b\}^* \mid |w|_a > |w|_b\}$ de la question 6. La série S_3 n'a que des coefficients entiers, donc le seuil 0 est *isolé*. Le langage L_3 a une infinité de résiduels, donc n'est pas rationnel.
13- Reprenons le langage $L_4 = \{w \in \{a,b\}^* \mid |w|_a \neq |w|_b\}$ de la question 6. La série $-S_4$ est définie par la représentation linéaire :

$$I = (-1,0,0,0), \mu(a) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \otimes \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},$$

$$\mu(b) = \mu(a)^{-1}, T = (1, 0, 0, 0)^t.$$

Comme les matrices $\mu(a), \mu(b)$ sont des produits tensoriels de matrices orthogonales, elles sont aussi orthogonales, et pour tout $w \in X^*, \mu(w)$ est orthogonale, donc $\|\mu(w)\| = 1$. La représentation linéaire (I, μ, T) vérifie l'inégalité :

$$\|I \cdot \mu(w)\| \leq \|I\| \cdot \|\mu(w)\| = 1,$$

donc elle est *bornée*. Le langage L_4 a une infinité de résiduels, donc n'est pas rationnel.
(Le seuil (-1) n'est donc pas isolé, d'après la question 9 ; on peut aussi le vérifier directement).

Partie III

Automates finis quantiques à une mesure.

Séries 1- Soit S est une série MOQ définie par

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

où d, μ, I, P vérifient les conditions de l'énoncé. Soit $w \in X^*$ et $\varepsilon > 0$.
Comme toutes les matrices $\mu(w)$ (pour $w \in X^*$) sont unitaires, l'ensemble $\{\mu(w^n) \mid n \in \mathbb{N}\}$ est une partie de la boule unité de $\mathbb{C}^{d \times d}$ qui est compacte. Donc cet ensemble possède un point d'accumulation. Supposons que $P \neq 0$ et posons

$$\varepsilon_1 := \frac{\varepsilon}{2 \cdot \|I\|^2 \cdot \|P\|}$$

Il existe $n_1 < n_2$ tels que

$$\|\mu(w^{n_2}) - \mu(w^{n_1})\| < \varepsilon_1.$$

Choisissons $k := n_2 - n_1$. Comme $\mu(w^{n_1})$ est unitaire,

$$\|\mu(w^{n_2}) - \mu(w^{n_1})\| = \|\mu(w^{n_1}) \cdot (\mu(w^k) - \mu(\mathrm{Id}))\| = \|(\mu(w^k) - \mu(\mathrm{Id}))\|.$$

Donc

$$\|\mu(w^k) - \mu(\mathrm{Id})\| < \varepsilon_1.$$

Il en résulte que, pour tous mots $u, v \in X^*$:

$$\begin{aligned} |\|I \cdot \mu(uw^k v)P\| - \|I \cdot \mu(uv) \cdot P\|| &\leq \|(I \cdot \mu(uw^k v) \cdot P) - (I \cdot \mu(uv) \cdot P)\| \\ &= \|I \cdot (\mu(uw^k v) - \mu(uv)) \cdot P\| \\ &\leq \|I\| \cdot \|\mu(w^k) - \mu(Id)\| \cdot \|P\| \\ &< \|I\| \cdot \varepsilon_1 \\ &= \frac{\varepsilon}{2 \cdot \|I\| \cdot \|P\|} \end{aligned}$$

En tenant compte du fait que $\|I \cdot \mu(uw^k v) \cdot P\| + \|I \cdot \mu(uv) \cdot P\| \leq 2\|I\| \cdot \|P\|$ on obtient alors :

$$\begin{aligned} |\|I \cdot \mu(uw^k v)P\|^2 - \|I \cdot \mu(uv) \cdot P\|^2| &\leq \|I \cdot \mu(uw^k v) \cdot P\| - \|I \cdot \mu(uv) \cdot P\| \cdot 2\|I\| \cdot \|P\|) \\ &< \frac{\varepsilon}{2 \cdot \|I\| \cdot \|P\|} \cdot 2\|I\| \cdot \|P\|) \\ &= \varepsilon. \end{aligned}$$

Dans le cas où $P = 0$:

$$|\|I \cdot \mu(uw^k v) \cdot P\|^2 - \|I \cdot \mu(uv) \cdot P\|^2| = 0 < \varepsilon.$$

(qed)

Langages à seuil 2- Soit $\mathcal{A}_0 =< X, Q, I_0, T_0, \tau_0 >$ un automate à groupe et $L = \mathrm{L}(\mathcal{A}_0)$.
On suppose que $Q = \{0, 1, \ldots, n-1\}$ et que l'unique état initial est 0. Pour chaque lettre $x \in X$, on définit $\mu(x)$ comme la matrice de la permutation $\mu_{\mathcal{A}}(x)$, $I := (1, 0, \ldots, 0)$ et $T = (t_0, \ldots, t_j, \ldots, t_{n-1})$ avec

$$t_j = 1 \text{ si } j \in T_0, \;\; t_j = 0 \text{ si } j \notin T_0$$

et enfin le projecteur $P \in \mathbb{C}^{n \times n}$ est défini par

$$P := T \cdot T^{\dagger}.$$

On vérifie que, pour tout mot $w \in X^*$: si $(0, j) \in \mu_{\mathcal{A}}(w)$ et $j \in T_0$

$$I \cdot \mu(w) \cdot P = (0, \ldots, 1, \ldots, 0)$$

(vecteur avec toutes les colonnes nulles sauf la j-ieme, qui vaut 1)
et si $(0, j) \in \mu_{\mathcal{A}}(w)$ et $j \notin T_0$

$$I \cdot \mu(w) \cdot P = (0, \ldots, 0, \ldots, 0)$$

(vecteur nul).
Donc

$$\|I \cdot \mu(w) \cdot P\|^2 = 1 \text{ si } w \in L, \;\; \|I \cdot \mu(w) \cdot P\|^2 = 0 \text{ si } w \notin L$$

et finalement

$$L = \{w \in X^* \mid \|I \cdot \mu(w) \cdot P\|^2 > \frac{1}{2}\}.$$

De plus, comme l' application $w \mapsto \|I \cdot \mu(w) \cdot P\|^2$ ne prend ses valeurs que dans $\{0, 1\}$, le seuil $\frac{1}{2}$ est *isolé*.
3- Choisissons un nombre $\theta \in \mathbb{R}$ tel que $\frac{\theta}{\pi} \notin \mathbb{Q}$,

$$I := (1, 0), \;\; \mu(a) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos\theta) \end{pmatrix}, \;\; \mu(b) := \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos\theta) \end{pmatrix}, \;\; P := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \;\; \lambda := 0.$$

Pour tout $w \in \{a, b\}^*$, $I \cdot \mu(w) = (\cos((|w|_a - |w|_b)\theta), -\sin((|w|_a - |w|_b)\theta))$
d' où

$$\|I \cdot \mu(w) \cdot P\|^2 = \sin^2((|w|_a - |w|_b)\theta)).$$

et

$$\|I \cdot \mu(w) \cdot P\|^2 > 0 \Leftrightarrow |w|_a \neq |w|_b.$$

4- Soit L est un langage MOQ-is défini par μ, I, P. Notons, pour tout mot $w \in X^*$, $S(w) := \|I \cdot \mu(w) \cdot P\|^2$. Soient $w, u, v \in X^*$. Posons $\varepsilon := \delta$ (où δ est un nombre réel réalisant la condition d'"isolement" (3)).
D'après la question 1, il existe un entier $k > 0$ tel que :

$$|S(uw^k v) - S(uv)| < \varepsilon = \delta$$

Mais si $S(uw^k v), S(uv)$ étaient l'un au-dessus, l'autre au-dessous du seuil λ alors on aurait

$$|S(uw^k v) - S(uv)| \geq 2\delta$$

ce qui contredirait l'inégalité précédente.
Donc

$$|S(uw^k v)| > \lambda \Leftrightarrow |S(uv)| > \lambda$$

i.e.

$$uw^k v \in L \Leftrightarrow uv \in L.$$

5- Prenons $L := (ab)^*, u := a, v := b, w := ba$. Pour tout entier $k \neq 0$:

$$uv \in L \text{ et } uw^k v \notin L$$

donc L ne vérifie pas le lemme d'itération de la question 4. Donc $(ab)^*$ n'est pas un langage MOQ-is.
6*- On adapte la preuve de la partie II question 10 comme suit.
On note $S'(w) := \|I \cdot \mu(w) \cdot P\|$. L' hypothèse (2) de la partie II est vérifiée par la série S', avec $C := \|I\|$.
Posons $C' := 1$. Par le raisonnement de la question II-7 on prouve que, pour tout $w \in X^*$ et $\vec{u} \in \text{vect}(\{I \cdot \mu_{\mathcal{A}}(w') \mid w' \in X^*\})$:

$$\|\vec{u} \cdot \mu(w)\| \leq C' \cdot \|\vec{u}\|.$$

Supposons que le langage L soit défini par (1). On a vu que S' vérifiant (2) et on suppose que (S, λ) vérifie (3).
Supposons maintenant qu'il existe un ensemble infini $W = \{w_i \mid i \in \mathbb{N}\}$ de mots tels que $i \neq j \Rightarrow w_i^{-1}L \neq w_j^{-1}L$.
Posons

$$\varepsilon = \frac{\delta}{2\|I\|}.$$

Par l'argument de compacité de la question II-8, il existerait des entiers $i \neq j$ tels que

$$\|I \cdot \mu(w_i) - I \cdot \mu(w_j)\| < \varepsilon.$$

Donc

$$\begin{aligned} |S(w_iw') - S(w_jw')| = & \quad |\|I \cdot \mu(w_iw')P\|^2 - \|I \cdot \mu(w_jw') \cdot P\|^2| \\ \leq & \quad \|I \cdot (\mu(w_i) - \mu(w_j))\mu(w')\| \cdot 2\|I\| \\ \leq & \quad \varepsilon \cdot 2\|I\| \\ = & \quad \delta. \end{aligned}$$

Or les deux nombres $S(w_iw'), S(w_jw')$ sont de part et d'autre de λ, donc

$$|S(w_iw') - S(w_jw')| \geq 2\delta$$

ce qui contredit l'inégalité juste au-dessus.
7- Le seuil λ utilisé pour résoudre la question 3 ne peut pas être choisi isolé, puisque le langage $\{w \in \{a, b\}^* \mid |w|_a \neq |w|_b\}$ n'est pas rationnel.

Partie IV

Automates finis quantiques multi-mesures.

1*- Soit $\mathcal{A} =< X, Q, I_0, T_0, \tau_0 >$ un automate réversible et L le langage qu'il reconnait (on peut supposer que $Q = [0, |Q| - 1]$ et $I = \{0\}$). Nous

construisons tout d'abord un nouvel a.f. à groupe $\mathcal{B} =< X, Q', I', T', \tau' >$ comme suit.

$$Q' := Q \times \{0\} \cup Q \times \{1\}$$

Pour chaque lettre $x \in X$, $\mu_{\mathcal{B}}(x)$ est une permutation de Q' vérifiant les conditions :

$$\text{si } (p,q) \in \mu_{\mathcal{A}}(x) \text{ alors } ((p,0),(q,0)) \in \mu_{\mathcal{B}}(x)$$

$$\text{si } \forall q \in Q, (p,q) \notin \mu_{\mathcal{A}}(x) \text{ alors } ((p,0),(p,1)) \in \mu_{\mathcal{B}}(x).$$

Une telle bijection existe car,

$$\{((p,0),(q,0)) \mid (p,q) \in \mu_{\mathcal{A}}(x)\} \cup \{((p,0),(p,1)) \mid \forall q \in Q, (p,q) \notin \mu_{\mathcal{A}}(x)\}$$

est une injection partielle de Q' dans Q'.

$$I' := \{(p,0) \mid p \in I_0\}, \quad T' := \{(p,0) \mid p \in T_0\}.$$

le langage L est alors l'ensemble des mots $w \in X^*$ tels que

il existe un calcul de $\mathcal{B}$ lisant w, n' utilisant que des états de $Q \times \{0\}$,

partant de I' et se terminant dans T'.

On construit maintenant un quintuplet I, μ, U, P, λ permettant de reconnaitre L comme un langage à seuil.
Le vecteur I vaut $(1, 0, \ldots, 0)$ (1 dans la colonne 0 et 0 dans les autres colonnes).
Pour toute lettre $x \in X$, $U(x)$ est la matrice, de dimension $|Q'| \times |Q'|$, de la permutation $\mu_{\mathcal{B}}(x)$, $P(x)$ (resp. P) est la matrice (en ligne) de la projection orthogonale sur le sous-espace vect$(Q \times \{0\})$ (resp. vect$(T \times \{0\})$), U est la matrice identité. On pose $\mu(x) = U(x)P(x)$. Alors, pour tout $w \in X^*$:

$$I \cdot \mu(w) = (c_k)_{0 \leq k \leq |Q'|-1}$$

avec
$c_k = 1$ ssi $[k \leq |Q'| - 1$ et $((0,0),(k,0)) \in \mu_{\mathcal{B}}(w)$ et tous les états du calcul de $\mathcal{B}$ lisant w et partant de $(0,0)$ sont dans $Q \times \{0\}]$.

$$I \cdot \mu(w) \cdot U \cdot P = (d_k)_{0 \leq k \leq |Q'|-1}$$

avec
$d_k = 1$ ssi $[k \leq |Q'| - 1$ et $((0,0),(k,0)) \in \mu_{\mathcal{B}}(w)$ et tous les états du calcul

de $\mathcal{B}$ lisant w et partant de $(0,0)$ sont dans $Q \times \{0\}$ et $k \in T_0$].
Finalement :

$$w \in L \Leftrightarrow \|I \cdot \mu(w) \cdot U \cdot P\|^2 > \frac{1}{2}$$

et comme tous les nombres $\|I \cdot \mu(w) \cdot U \cdot P\|^2$ valent 0 ou 1, ce seuil $\frac{1}{2}$ est isolé.
2- Tout langage MOQ-is est MMQ-is : il suffit de remarquer que l' on peut choisir $P(x) = P = U =$ I dans la définition d'une série MOQ. Donc toute série MOQ est aussi MMQ.
Le langage $(ab)^*$ est réversible, donc MMQ-is (question 1).
Par contre il n'est pas MOQ-is (question III-5).
3*- Tout langage MMQ-is est rationnel : il suffit de reprendre les arguments utilisés dans la question II-10.