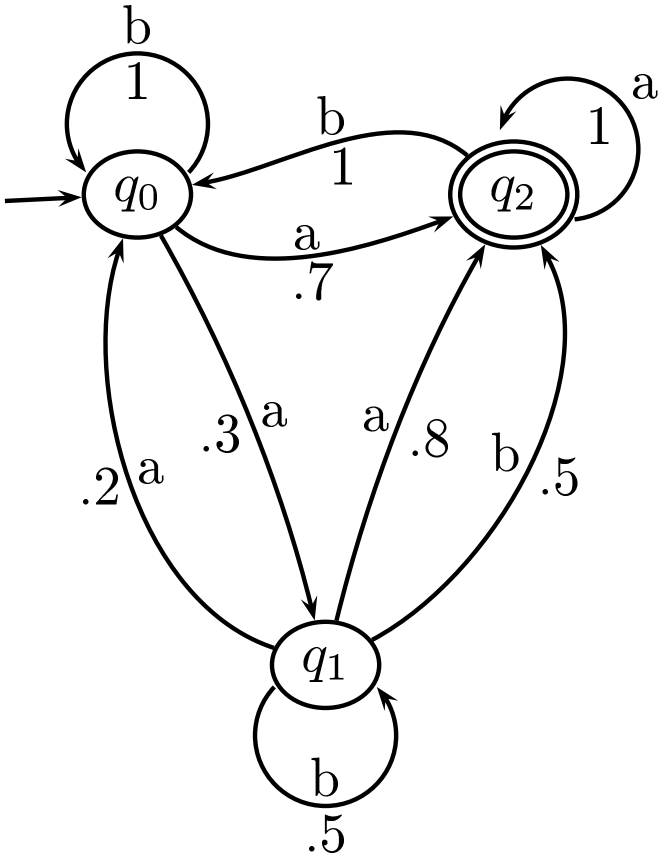
Indécidabilité sur les automates quantiques

Emmanuel Jeandel
Stagiaire de DEA à l'ÉNS Lyon
Sous la direction de P. Koiran et N. Portier

Première Journée de l'action spécifique Nouveaux modèles de calcul

Automates Probabilistes



$$q_0 \quad \to_a \quad .7q_2 + .3q_1$$

$$\to_b \quad .7q_0 + .15q_1 + .15q_2$$

$$ACC(ab) = .15$$

$$\mathcal{X}_a = \begin{pmatrix} 0 & .2 & 0 \\ .3 & 0 & 0 \\ .7 & .8 & 1 \end{pmatrix} \quad \mathcal{X}_b = \begin{pmatrix} 1 & 0 & 1 \\ 0 & .5 & 0 \\ 0 & .5 & 0 \end{pmatrix}$$

$$\mathbf{s} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T \quad \pi = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}^T$$

$$ACC(\omega) = \pi^T \mathcal{X}_\omega \mathbf{s}$$

- Une configuration est un ensemble d'états avec certaines probabilités : $\sum_i \alpha_i q_i$, avec $\sum_i \alpha_i = 1$
- On est dans l'état q_i avec probabilité α_i
- Un opérateur $\mathcal{X}_a$ est une matrice dont toutes les colonnes somment à 1 (matrice stochastique).
- Le résultat est obtenu en regardant les probabilités sur certains états

- Une configuration est une *superposition* d'états : $\sum_i \alpha_i q_i$, avec $\sum_i |\alpha_i|^2 = 1$, $\alpha \in \mathbb{C}$
- On est simultanément dans tous les états ; l'amplitude de l'état q_i est α_i
- Un opérateur $\mathcal{X}_a$ est une matrice qui conserve les distances, donc une matrice unitaire.
- Le résultat est obtenu en effectuant une *mesure*, c'est à dire une projection orthogonale sur certains états.

Définition

Un automate quantique MO est la donnée d'un ensemble d'états q_i qui forment la base d'un espace euclidien (ou hermitien) H et

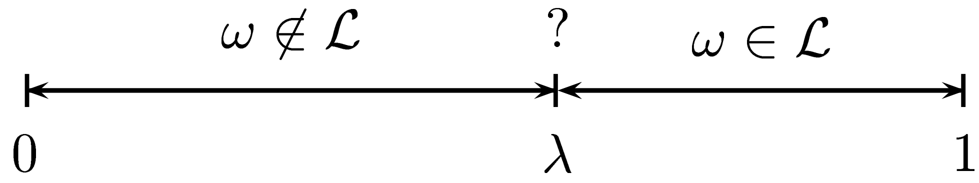
- D'un vecteur de H de norme 1 appelé configuration initiale, et noté $\vec{s}$.
- D'états d'acceptation, $\mathcal{P}$ étant l'opérateur de projection orthogonale sur l'espace engendré par ces états.
- D'un alphabet Σ et de matrices unitaires $\mathcal{X}_i$ pour chaque lettre i de l'alphabet

La probabilité qu'un mot ω soit accepté est :

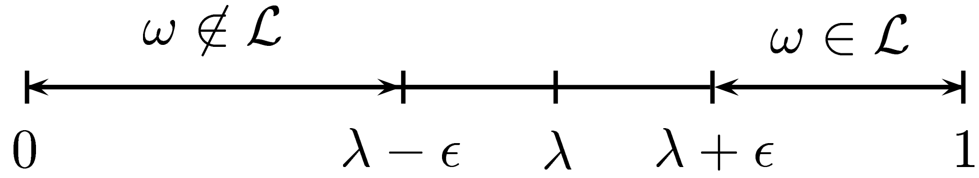
$$ACC(\omega) = \|\vec{s}^T \mathcal{X}_\omega \mathcal{P}\|$$

Propriétés

- Acceptation



- Seuil isolé



  Un langage reconnu avec seuil isolé est rationnel. De plus, c'est un langage de groupe (reconnu par un automate fini dont les matrices sont de permutation)

- Si $ACC(uvw) > \lambda$, il existe $k > 1$ tel que $ACC(uv^kw) > \lambda$
  Pour tout ϵ, il existe k tel que $\|\mathcal{X}_v^k - \mathcal{I}\| < \epsilon$

À λ donné, il est indécidable de savoir s'il existe ω tel que $ACC(\omega) \leq \lambda$ (resp. $ACC(\omega) \geq \lambda$)

Preuve : Il suffit de montrer l'indécidabilité de $ACC(\omega) = \|\vec{s}^T \mathcal{X}_\omega \mathcal{P}\| = 0$

- $\leq$ $\mathcal{Y}_i = \begin{pmatrix} \mathcal{X}_i & 0 \\ 0 & 1 \end{pmatrix}$ $\mathcal{Q} = \begin{pmatrix} \mathcal{P} & 0 \\ 0 & 1 \end{pmatrix}$ $\vec{v} = \begin{pmatrix} \sqrt{1-\lambda^2}\vec{s} \\ \lambda \end{pmatrix}$ Ainsi, $ACC'(\omega)^2 = (1-\lambda^2)ACC(\omega)^2 + \lambda^2$, et indécidabilité de $ACC'(\omega) \leq \lambda$
- $\geq$ En prenant $\mathcal{R} = \mathcal{I} - \mathcal{Q}$, $ACC^{(2)}(\omega) = \sqrt{(1-\lambda^2)(1-ACC(\omega)^2)}$

$$\mathcal{X}_0 = \begin{pmatrix} 3/5 & -4/5 & 0 \\ 4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \mathcal{X}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3/5 & -4/5 \\ 0 & 4/5 & 3/5 \end{pmatrix}$$

génère un groupe libre à deux générateurs.

De plus, il existe un vecteur a tel que $\omega = \omega' \iff \mathcal{X}_\omega a = \mathcal{X}_{\omega'} a$

$$\left\| \begin{pmatrix} \mathcal{I}/2 & -\mathcal{I}/2 \\ -\mathcal{I}/2 & \mathcal{I}/2 \end{pmatrix} \begin{pmatrix} \mathcal{X}_\omega & 0 \\ 0 & \mathcal{X}_{\omega'} \end{pmatrix} \begin{pmatrix} a \\ a \end{pmatrix} \right\|^2 = 1/2 \cdot \|\mathcal{X}_\omega a - \mathcal{X}_{\omega'} a\|^2$$

Solution

Etant donné une instance (u_i, v_i) de la correspondance de Post, on lui associe les matrices

$$\mathcal{Y}_i = \begin{pmatrix} \mathcal{X}_{u_i} & 0 \\ 0 & \mathcal{X}_{v_i} \end{pmatrix}$$

On cherche donc s'il existe ω tel que

$$\mathcal{Y}_\omega = \begin{pmatrix} \mathcal{X}_\nu & 0 \\ 0 & \mathcal{X}_\nu \end{pmatrix}$$

ω est solution de la correspondance de Post si et seulement si ω est accepté avec probabilité 0

C.Q.F.D

Décidabilité

Le problème : "il existe ω tel que $ACC(\omega) > \lambda$" est décidable.

Reformulation : Est-ce qu'il existe $g \in \{\mathcal{X}_a, \mathcal{X}_b\}^+$ tel que $f(g) > \lambda$

Idée : On peut prendre $g \in \overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}$.

Le groupe en question est un groupe de matrices compact, donc algébrique.

$$\overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle} = \{\mathcal{M} \in M_n(\mathbb{R}), P_1(\mathcal{M}) = 0, \dots, P_k(\mathcal{M}) = 0\}$$

Le problème devient :

$$\exists \mathcal{M} \in M_n(\mathbb{R}), P_1(\mathcal{M}) = 0, \dots, P_k(\mathcal{M}) = 0, f(g) > \lambda$$

ce qui est décidable

Problème

On ne sait pas calculer les P_i. On sait en revanche que $G = \overline{\langle A, B\rangle}$ est l'ensemble des zéros de

$$\mathbb{K}[X]^G = \left\{f \text{ polynôme en } n^2 \text{ variables}, \forall g \in G, f(gX) = f(X)\right\}$$

qui est finiment engendré. En énumérant $\mathbb{K}[X]^G$, on sait donner des suites de descriptions $f_1 \dots f_k$ de groupes G_i tels que $G_i \supset G$, et il existe i tel que $G_i = G$

Il suffit donc de mener en parallèle :

- Tester tous les éléments $\mathcal{X}$ de $\{\mathcal{X}_a, \mathcal{X}_b\}^+$ jusqu'à ce que $f(\mathcal{X}) > \lambda$
- Tester pour tous les surgroupes G_i obtenus précédemment, si la condition $\exists \mathcal{X} \in G_i, f(\mathcal{X}) > \lambda$ est fausse.

- $\exists\omega, ACC(\omega) \geq \lambda$ est indécidable
- $\exists\omega, ACC(\omega) > \lambda$ est décidable
- Qu'en est-il de l'existence d'un seuil isolé ?
- Peut-on donner une description du groupe $\overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}$?