# Automates quantiques et indécidabilité

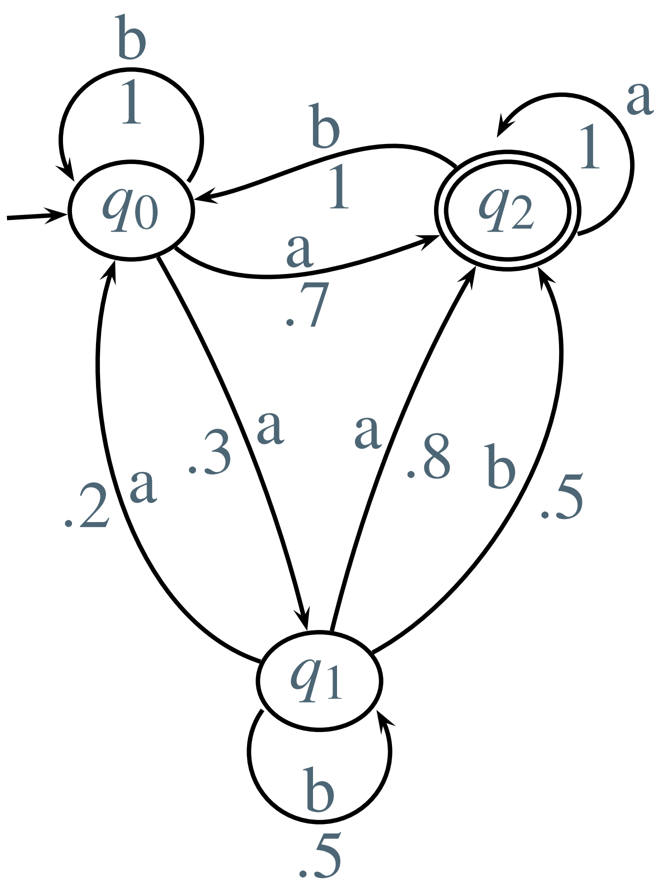
*Rapport de stage de DEA*

Emmanuel Jeandel

Effectué sous la direction de Natacha PORTIER et Pascal KOIRAN
ENS Lyon
MC2

# Le modèle Measure Once

# Automates Probabilistes




$$
\begin{aligned}
q_0 \quad & \rightarrow_a \quad .7q_2 + .3q_1 \\
& \rightarrow_b \quad .7q_0 + .15q_1 + .15q_2
\end{aligned}
$$

$$ACC(ab) = .15$$

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

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

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

# Le modèle probabiliste

- 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 $\alpha_i$
- 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

# Le cas quantique

- 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 $\alpha_i$
- 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

*De tous les arts, le plus grand parce que le plus bref est celui de la définition*

Gérard Klein

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

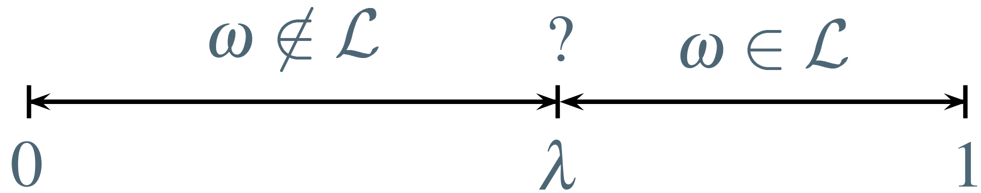
- D'un vecteur de $H$ de norme 1 appelé configuration initiale, et noté $\mathbf{s}$.
- D'états d'acceptation, $\mathcal{P}$ étant l'opérateur de projection orthogonale sur l'espace engendré par ces états.
- D'un alphabet $\Sigma$ et de matrices unitaires $\mathcal{X}_i$ pour chaque lettre $i$ de l'alphabet

La probabilité qu'un mot $\omega$ soit accepté est :

$$ACC(\omega) = \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\|^2$$

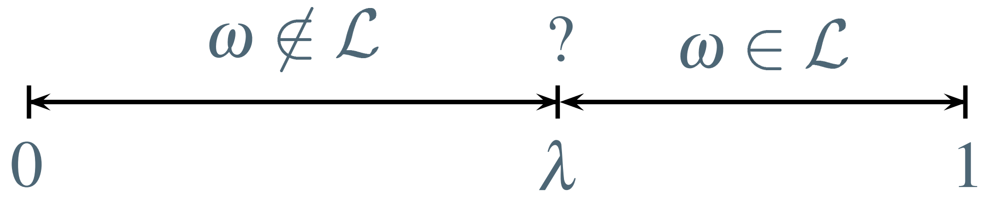
# Propriétés

- Acceptation

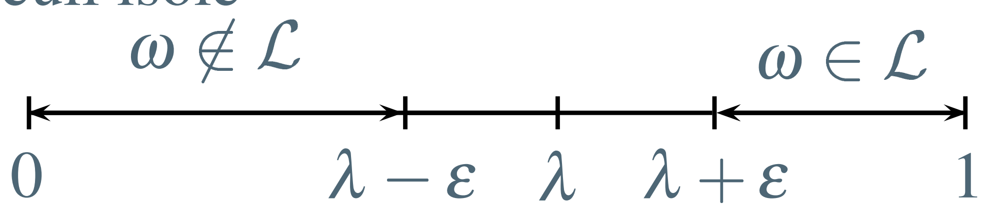


# Propriétés

- Acceptation



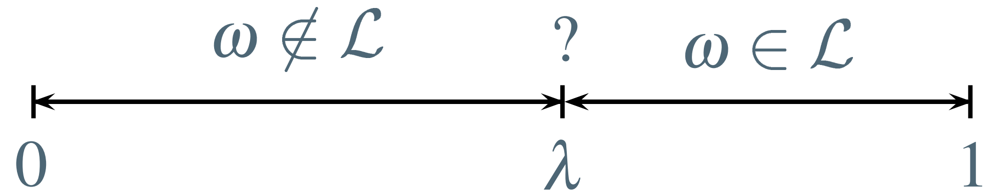

- Seuil isolé



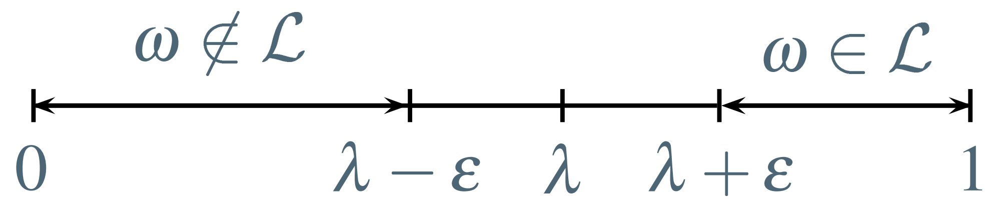

Un langage reconnu avec seuil isolé est rationnel. De plus, c'est un langage de groupe (reconnu par un automate fini dont les matrices sont de permutation)

# 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 $\mathrm{ACC}(uvw) > \lambda$, il existe $k>1$ tel que $\mathrm{ACC}(uv^k w) > \lambda$
Pour tout $\varepsilon$, il existe $k$ tel que $\|\mathcal{X}_v^k - \mathcal{I}\| < \varepsilon$

# Résultats de décidabilité

*Nature's Laws govern which things can be done, and which can't. The trouble is, when we set out to do something, we don't always know which of these categories it's in.*

Donald Simanek

Les questions

- Est-ce qu'il existe $\omega$ tel que $ACC_\omega \geq \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega \leq \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega = \lambda$ ?

sont toutes trois indécidables.

En revanche, les questions

- Est-ce qu'il existe $\omega$ tel que $ACC_\omega > \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega < \lambda$ ?

sont décidables.

# La correspondance de POST

Etant donnée une liste de couple $(u_i, v_i)$, pour $i \leq n$, le problème de la correspondance de POST est de savoir s'il existe $\omega$ tel que $u_\omega = v_\omega$. Ce problème est indécidable.

| $i$ | $u_i$ | $v_i$ |
|---|---|---|
| 0 | $a$ | $ab$ |
| 1 | $bc$ | $ca$ |
| 2 | $abc$ | $c$ |

Une solution : 0102

$$a/b\ \ c/a/a\ \ b\ \ c$$
$$a\ \ b/c\ \ a/a\ \ b/c$$

| $i$ | $u_i$ | $v_i$ |
|---|---|---|
| 0 | $a$ | $ab$ |
| 1 | $bc$ | $ca$ |
| 2 | $ab$ | $ac$ |

Aucune solution

# Codage des mots

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

génère un groupe libre à deux générateurs.
De plus, il existe un vecteur $\mathbf{a}$ tel que pour tous $\omega$ et $\omega'$,

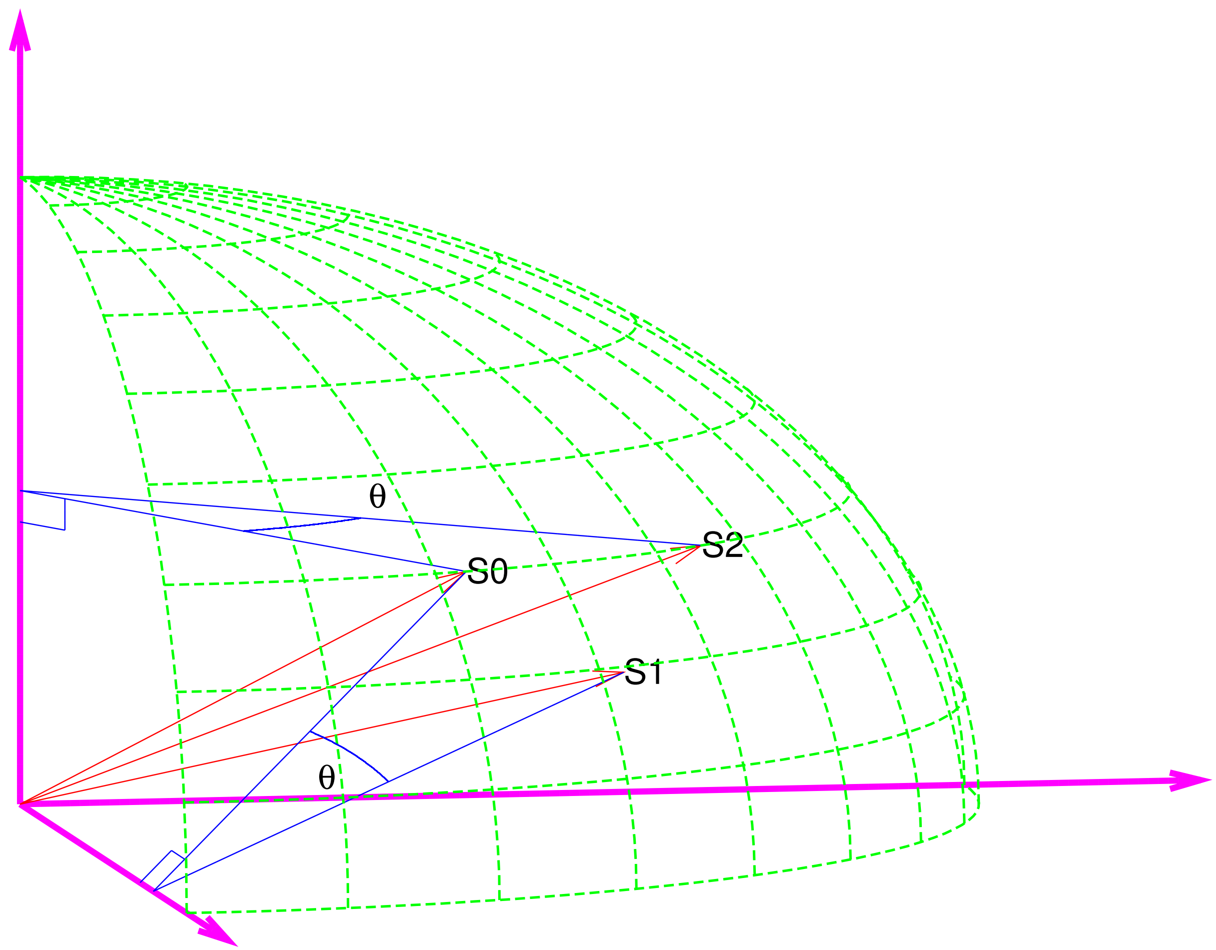
$$\omega = \omega' \iff \mathcal{X}_\omega \mathbf{a} = \mathcal{X}_{\omega'} \mathbf{a}$$

On peut tester l'égalité des mots en testant l'égalité sur des vecteurs.

# Codage des mots

*Figures won't lie, but liars will figure*

General Charles H. Grosvenor



# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)

# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)
- $\forall \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| \leq \lambda$ (plus dur)

# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)
- $\forall \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| \leq \lambda$ (plus dur)
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, \|\mathbf{s}^T \mathcal{X} \mathcal{P}\| \leq \lambda$

# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)
- $\forall \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| \leq \lambda$ (plus dur)
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, \|\mathbf{s}^T \mathcal{X} \mathcal{P}\| \leq \lambda$
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, f(\mathcal{X}) \leq \lambda$

# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)
- $\forall \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| \leq \lambda$ (plus dur)
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, \|\mathbf{s}^T \mathcal{X} \mathcal{P}\| \leq \lambda$
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, f(\mathcal{X}) \leq \lambda$
- $\forall \mathcal{X} \in \overline{\{\mathcal{X}_a, \mathcal{X}_b\}^\star}, f(\mathcal{X}) \leq \lambda$

# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)
- $\forall \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| \leq \lambda$ (plus dur)
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, \|\mathbf{s}^T \mathcal{X} \mathcal{P}\| \leq \lambda$
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, f(\mathcal{X}) \leq \lambda$
- $\forall \mathcal{X} \in \overline{\{\mathcal{X}_a, \mathcal{X}_b\}^\star}, f(\mathcal{X}) \leq \lambda$
- $\forall \mathcal{X} \in \overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}, f(\mathcal{X}) \leq \lambda$

# Décidabilité

- $\exists \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| > \lambda$ (facile)
- $\forall \omega, \|\mathbf{s}^T \mathcal{X}_\omega \mathcal{P}\| \leq \lambda$ (plus dur)
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, \|\mathbf{s}^T \mathcal{X} \mathcal{P}\| \leq \lambda$
- $\forall \mathcal{X} \in \{\mathcal{X}_a, \mathcal{X}_b\}^\star, f(\mathcal{X}) \leq \lambda$
- $\forall \mathcal{X} \in \overline{\{\mathcal{X}_a, \mathcal{X}_b\}^\star}, f(\mathcal{X}) \leq \lambda$
- $\forall \mathcal{X} \in \overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}, f(\mathcal{X}) \leq \lambda$
- $\overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}$ est l'ensemble des racines d'un certain polynôme.

  $$\forall \mathcal{X}, P(\mathcal{X}) = 0 \implies f(\mathcal{X}) \leq \lambda$$

  Et on sait décider

# Décidabilité

$G = \overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}$ est un groupe de matrices compact donc un groupe de Lie compact, donc un groupe algébrique sur $\mathbb{R}$.
C'est l'ensemble des zéros communs des $P \in \mathbb{R}[X_1 \ldots X_{n^2}]$

$$\begin{cases} P(g \cdot X) & = & P(X) \quad \forall g \in G \\ P(\mathcal{I}) & = & 0 \end{cases}$$

La première condition se réécrit $P(\mathcal{X}_a \cdot X) = P(\mathcal{X}_b \cdot X) = P(X)$.

$$\boxed{\forall X \in G, f(X) \leq \lambda \iff \begin{array}{c} \text{Il y a un P comme ci-dessus tel que} \\ \forall X, P(X) = 0, f(X) \leq \lambda \end{array}}$$

$\Rightarrow$ C'est un théorème.
$\Leftarrow$ L'ensemble des zéros de $P$ est un ensemble qui contient $G$.

Il suffit d'essayer chaque $P$.

# Le modèle Measure Many

# Présentation du modèle

*There may be more than one way to skin a cat,*
*but you only get one try per cat*

Proverbe anglais

Dans le modèle précédent, une mesure n'était effectuée qu'à la fin du calcul. Maintenant, on effectue une mesure à *chaque étape*.

Principe de la mécanique quantique :

Une mesure est destructrice.

On a maintenant

- Des états d'acceptation
- Des états de refus
- Des états pour continuer le calcul

# Principe

Après chaque lecture d'une lettre

- On regarde avec quelle amplitude on est dans les états d'acceptation
- On regarde avec quelle amplitude on est dans les états de refus
- On continue en ne gardant que ce qui se trouve dans les états pour continuer.

Après avoir lu le mot $\omega$, on a donc une probabilité d'acceptation $ACC_{\omega}$ (probabilité de s'etre arrêté dans un état d'acceptation), et une probabilité de refus $REF_{\omega}$.

# Indécidabilité

Les questions

- Est-ce qu'il existe $\omega$ tel que $ACC_\omega \geq \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega \leq \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega = \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega > \lambda$ ?
- Est-ce qu'il existe $\omega$ tel que $ACC_\omega < \lambda$ ?

sont toutes indécidables.

# Idées de preuve

- Pour montrer $ACC_\omega = \lambda$, on utilisait

$$X_\omega \mathbf{a} = X_{\omega'} \mathbf{a} \iff \omega = \omega'$$

# Idées de preuve

- Pour montrer $ACC_\omega = \lambda$, on utilisait

$$X_\omega \mathbf{a} = X_{\omega'} \mathbf{a} \iff \omega = \omega'$$

- Pour $>$, il faut un $>$ dans le test, et par exemple :

$$\|X_\omega \mathbf{a} - X_{\omega'} \mathbf{a}\| < 1/5^{\max(|\omega|,|\omega'|)} \iff \omega = \omega'$$

On peut simuler un $\alpha^{|\omega|}$ dans ce modèle

# Idées de preuve

- Pour montrer $ACC_\omega = \lambda$, on utilisait

$$X_\omega \mathbf{a} = X_{\omega'} \mathbf{a} \iff \omega = \omega'$$

- Pour $>$, il faut un $>$ dans le test, et par exemple :

$$\|X_\omega \mathbf{a} - X_{\omega'} \mathbf{a}\| < 1/5^{\max(|\omega|,|\omega'|)} \iff \omega = \omega'$$

  On peut simuler un $\alpha^{|\omega|}$ dans ce modèle

- Autre preuve : on peut simuler les automates probabilistes avec ce modèle. Pour tout langage $L$ reconnu avec seuil $\lambda$, on peut construire (effectivement) un automate Measure Many qui reconnait $L$ avec seuil $\beta$.

# Conclusion

*Science is always wrong. It never solves a problem without creating ten more.*

George Bernard Shaw

- Indécidabilité des principaux problèmes *sauf* de l'acceptation avec seuil strict
- Intérêt porté à une description du groupe $\overline{\langle \mathcal{X}_a, \mathcal{X}_b \rangle}$, source de solutions
- Simulation des automates probabilistes par les automates quantiques MM