Ensembles de portes quantiques universelles

Critères d'universalité

Emmanuel Jeandel

ENS Lyon

Le problème

Etant donné un jeu de portes quantiques sur n bits $\mathcal{O}$, est-ce que $\mathcal{O}$ est universel au sens faible, c'est à dire :

Est-ce que toute porte quantique sur n bits peut être simulée avec une précision ε par un circuit avec portes dans $\mathcal{O}$?

Formulation mathématique

Etant donné un ensemble de matrices $n \times n$ unitaires $\mathcal{X}$, est-ce que le groupe engendré par $\mathcal{X}$ est dense dans l'ensemble des matrices $n \times n$ unitaires ?

(Prendre le jeu de portes $\mathcal{O}$ et y ajouter les portes de croisement de fils.)

Remarque: on a pris le groupe et pas le monoïde, mais c'est la même chose.

Le cas classique

Etant donné un ensemble de m permutations sur n éléments $\mathcal{X}$, est-ce que cet ensemble engendre S_n ?

[Sims 67] Il existe un algorithme qui opère en temps polynomial, et même en temps $O(n^5 + mn^2)$ [Knuth 86] et espace $O(n^2)$ [Jerrum 86].

Idée de la preuve : Etant donné $\beta_1 \dots \beta_n$, on note G_k le stabilisateur de $\beta_1 \dots \beta_k$.
Alors $|G| = \prod |G_k : G_{k+1}|$ et $|G_k : G_{k+1}|$ est égal au cardinal de l'orbite de β_i dans G_i.

Approches

Trois approches pour résoudre le problème

- Méthode des invariants : Comment montrer qu'un ensemble de portes n'est pas universel.
- Méthode par groupes de Lie : Comment montrer qu'un ensemble de portes est universel.
- Méthode algébrique : Déterminer exactement le groupe engendré.

Une matrice

(Derksen, Koiran, J.)

Le problème

Etant donné une matrice unitaire $\mathcal{X}$, que peut-on dire du groupe engendré par $\mathcal{X}$?

Forme

A un changement de base près, c'est une matrice de la forme

$$\mathcal{X} = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \lambda_n \end{pmatrix}$$

où les λ_i sont des racines de l'unité.

Exemple 1.

$$\mathcal{X} = \begin{pmatrix} \frac{-12}{25} & \frac{-4}{5} & \frac{9}{25} \\ \frac{3}{5} & 0 & \frac{4}{5} \\ \frac{-16}{25} & \frac{3}{5} & \frac{12}{25} \end{pmatrix} \text{ et } \mathcal{P}\mathcal{X}\mathcal{P}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & j & 0 \\ 0 & 0 & j^2 \end{pmatrix}, j = e^{i\pi/3}$$

$\overline{\langle \mathcal{X} \rangle} = \{\mathcal{I}, \mathcal{X}, \mathcal{X}^2\}$

Exemple 2.

$$\mathcal{X} = \frac{1}{65}\begin{pmatrix} 32 & 56 & 4 & 7 \\ -56 & 32 & -7 & 4 \\ -4 & -7 & 32 & 56 \\ 7 & -4 & -56 & 32 \end{pmatrix} \text{ et } \mathcal{P}\mathcal{X}\mathcal{P}^{-1} = \begin{pmatrix} e^{i\theta} & 0 & 0 & 0 \\ 0 & e^{-i\theta} & 0 & 0 \\ 0 & 0 & e^{i\omega} & 0 \\ 0 & 0 & 0 & e^{-i\omega} \end{pmatrix} \begin{cases} \theta = \arccos(3/5) \\ \omega = \arccos(5/13) \end{cases}$$

$$\overline{\langle \mathcal{P}\mathcal{X}\mathcal{P}^{-1} \rangle} = \left\{ \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & u & 0 \\ 0 & 0 & 0 & u^{-1} \end{pmatrix}, \begin{matrix} |t| = 1 \\ |u| = 1 \end{matrix} \right\}$$

Exemple 2. (Suite)

$$\overline{\langle \mathcal{X} \rangle} = \left\{ \frac{1}{4} \begin{pmatrix} t+t^{-1}+u+u^{-1} & i(t-t^{-1}+u-u^{-1}) & i(t^{-1}-t+u-u^{-1}) & t+t^{-1}-u-u^{-1} \\ i(t^{-1}-t+u^{-1}-u) & t+t^{-1}+u+u^{-1} & -t-t^{-1}+u+u^{-1} & i(t^{-1}-t+u-u^{-1}) \\ i(t-t^{-1}+u^{-1}-u) & -t-t^{-1}+u+u^{-1} & t+t^{-1}+u+u^{-1} & i(t-t^{-1}+u-u^{-1}) \\ t+t^{-1}-u-u^{-1} & i(t-t^{-1}+u^{-1}-u) & i(t^{-1}-t+u^{-1}-u) & t+t^{-1}+u+u^{-1} \end{pmatrix} \middle| \begin{matrix} |t|=1 \\ |u|=1 \end{matrix} \right\}$$

En éliminant les complexes :

$$\overline{\langle \mathcal{X} \rangle} = \left\{ \frac{1}{2} \begin{pmatrix} t_1+u_1 & t_2+u_2 & u_2-t_2 & t_1-u_1 \\ -t_2-u_2 & t_1+u_1 & u_1-t_1 & u_2-t_2 \\ t_2-u_2 & u_1-t_1 & t_1+u_1 & t_2-u_2 \\ t_1-u_1 & t_2-u_2 & -t_2-u_2 & t_1+u_1 \end{pmatrix} \middle| \begin{matrix} t_1^2+t_2^2=1 \\ u_1^2+u_2^2=1 \end{matrix} \right\}$$

Exemple 3.

$$\mathcal{X} = \frac{1}{25}\begin{pmatrix} 4 & 22 & 2 & 11 \\ -22 & 4 & -11 & 4 \\ -2 & -11 & 4 & 22 \\ 11 & -2 & -22 & 4 \end{pmatrix} \text{ et } \mathcal{P}\mathcal{X}\mathcal{P}^{-1} = \begin{pmatrix} e^{i\theta} & 0 & 0 & 0 \\ 0 & e^{-i\theta} & 0 & 0 \\ 0 & 0 & e^{2i\theta} & 0 \\ 0 & 0 & 0 & e^{-2i\theta} \end{pmatrix}, \ \theta = \arccos(3/5)$$

$$\overline{\langle \mathcal{P}\mathcal{X}\mathcal{P}^{-1} \rangle} = \left\{ \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & t^2 & 0 \\ 0 & 0 & 0 & t^{-2} \end{pmatrix}, \quad |t| = 1 \right\}$$

Principe

Etant donné $\lambda_1 \dots \lambda_n$, on cherche toutes les relations multiplicatives entre les λ_i, c'est à dire les tuples $(p_1 \dots p_n)$ tels que $\lambda_1^{p_1} \lambda_2^{p_2} \cdots \lambda_n^{p_n}$

[Masser 88] Il existe une base v_i du réseau dont chaque vecteur a des entrées bornées par

$$(cnh)^{n-1} D^{n-1} \frac{(\log(D+2))^{3n-3}}{(\log\log(D+2))^{3n-4}}$$

où c est une certaine constante, D est le degré de l'extension algébrique, h une majoration sur la hauteur des nombres algébriques $\lambda_1 \dots \lambda_n$.

Invariants

Principe

Etant donné un groupe G qui agit sur un $\mathbb{R}$-espace vectoriel E, un invariant f est un polynôme qui vérifie

$$\forall g \in G, \forall v, f(g \cdot v) = f(v)$$

On note souvent $\mathbb{R}[E]^G$ l'ensemble des invariants.

Dans notre cas, l'espace vectoriel est l'ensemble des matrices $n \times n$, et l'action est la multiplication.

$$\forall \mathcal{X} \in G, \forall \mathcal{Y}, f(\mathcal{X}\mathcal{Y}) = f(\mathcal{Y})$$

Exemples

- $\det^2$ est un invariant pour tout $G \subset U(\mathbb{R}, n)$.
- $f(\mathcal{X}) = \|\mathcal{X}v\|^2$ est un invariant pour tout $G \subset U(\mathbb{R}, n)$.
- pour $G = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-2} \end{pmatrix}, t \in \mathbb{R}^\star \right\}$

  comme $\begin{pmatrix} t & 0 \\ 0 & t^{-2} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ta & tb \\ t^{-2}c & t^{-2}d \end{pmatrix}$

  $f(\begin{pmatrix} A & B \\ C & D \end{pmatrix}) = A^2(C+D)$ est un invariant.

Invariants

Si G est compact, alors

$$G = \{\mathcal{X} | f(\mathcal{X}) = f(\mathcal{I}), \forall f \text{ invariant } \}$$

Idée de la preuve : Sur un groupe compact, on peut intégrer.

Si $Y \notin G$, il existe f polynôme tel que
$0 < f(M) < 1/4$ sur $G.Y$, et $3/4 < f(M) < 1$ sur G, et

$$g(X) = \int f(MX) dM$$

est un invariant qui permet de conclure.

Universalité

- Un invariant sur $G = \overline{\langle X_i \rangle}$ est un polynôme f qui vérifie $\forall i, \forall \mathcal{Y}, f(\mathcal{X}_i \mathcal{Y}) = f(\mathcal{Y})$
- Pour montrer qu'un ensemble de portes X_i n'est pas universel, il suffit donc de trouver
  - Un invariant f pour les X_i
  - Une matrice unitaire M telle que $f(M) \neq f(\mathcal{I})$.
- Peut-on utiliser le fait que l'ensemble des invariants est finiment généré ?

Algèbres de Lie

(Barenco, Deutsch, Ekert)

Principe

A tout groupe compact G, on peut associer son espace tangent en l'identité H. Dans ce cas, on sait

- Tout groupe compact connexe est déterminé uniquement par son espace tangent.
- En particulier, l'espace tangent associé au groupe unitaire est l'ensemble des matrices anti-hermitiennes

L'idée est donc de calculer l'espace tangent en l'identité et de voir s'il est égal à toutes les matrices anti-hermitiennes

Instruments

- H est une algèbre de Lie : Pour tous $A, B \in H$, $[A, B] = AB - BA \in H$
- L'exponentielle d'un élément de H est dans G.
- Si $X \in H$ et $T \in G$, $TXT^{-1} \in H$.

D'où la méthode

- Trouver X d'ordre infini, et calculer le groupe $\overline{\langle X \rangle}$. En déduire un élément T de l'espace tangent.
- En utilisant les opérations MTM^{-1} et $[A, B]$, en construire plus
- Espérer en avoir suffisament pour générer toutes les matrices anti-hermitiennes

Méthode algébrique

(Derksen, Koiran, J.)

Variétés algébriques

Une variété algébrique est l'ensemble des zéros de polynômes P_i dans $\mathbb{R}$, et est entièrement décrit par l'idéal engendré par les P_i qui est finiment généré.

- Une variété est dite irréductible si elle ne peut pas se décomposer en deux sous-variétés.
- Toute suite croissante de variétés irréductibles est stationnaire
- Etant donné A un ensemble, on note $\overline{A}$ le plus petit ensemble algébrique qui contient A.
- Si A et B sont des variétés irréductibles, $\overline{AB}$ l'est aussi.
- Tout groupe compact connexe est irréductible.

Méthode

Etant donné $X_1 \ldots X_n$, on veut calculer $\overline{\langle X_1 \ldots X_n \rangle}$

Prendre $G = \{\mathcal{I}\}, H = \{\mathcal{I}\}$, $S = \{\mathcal{I}\}$.
Pour tout Y dans $\langle X_1 \ldots X_n \rangle$ pas encore dans G

- $H = \overline{H \cdot \overline{\langle Y \rangle}_0}$
- $H = \overline{H \cdot YHY^{-1}}$
- $G = S \cdot H$
- Si $Y \notin G$, $S = S \cup \{Y\}$

Idée de Preuve

H finit par stationner. Dans ce cas, on a alors

- pour tous les X_i, $X_i H X_i^{-1} \subset H$
- H est donc un sous-groupe de $G_? = \overline{\langle X_1 \dots X_n \rangle}$ et il est même distingué.
- Pour tout $s \in S_k$, il existe i tel que $s^i \in H$.
- $S = \cup S_k$ est tel que S/H ne contient que des éléments d'ordre fini. Et $S/H \subset G_?/H$ qui est un groupe algébrique linéaire. Donc S/H est fini, l'algorithme termine.

On vérifie alors que $G_? = S \cdot H$.

Conclusion

- Trois méthodes pour savoir si un ensemble de portes est universel, donc deux algorithmes.
- Peut-on trouver un algorithme efficace ?
- Peut-on dire quelque chose des portes universelles au sens fort ?