partie 1

bases mutuellement non biaisées (MUBs) dans $\mathbb{C}^d$

partie 2

caractérisation de l'intrication d'états multiqubits symétriques

Maurice R. Kibler
Institut de Physique des 2 Infinis
IN2P3/CNRS et Université Claude Bernard
Lyon, France

exposé au groupe de travail « modélisation quantique »
ISC-PIF, Centrale-Supélec-CNAM-UPSUD-AFSCET, Paris, 27/02/2020

PARTIE 1

BASES MUTUELLEMENT NON BIAISÉES (MUBs)

dans la partie 1 il sera question de

• MUBs et mécanique quantique – résultats et problèmes ouverts – MUBs, physique et mathématiques – 3 conjectures et une proposition – intérêts des MUBs

• construction des MUBs via SU(2) et moments angulaires (ou spins) généralisés

• construction des MUBs via corps de Galois ($d = p^m$, p premier impair, $m \in \mathbb{N}^*$)

• construction des MUBs via anneaux de Galois ($d = 2^m$, $m \in \mathbb{N}^*$)

DÉFINITION DES MUBs

du particulier au général

- matrices de Pauli

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \; \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- $\Rightarrow$ 3 bases orthonormées de $\mathbb{C}^2$

$$\sigma_z : \quad B_2 = \{|20\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv |0\rangle, \quad |21\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |1\rangle\}$$

$$\sigma_y : \quad B_1 = \left\{|10\rangle := 2^{-\frac{1}{2}}(|0\rangle + \mathrm{i}|1\rangle), \quad |11\rangle := 2^{-\frac{1}{2}}(|0\rangle - \mathrm{i}|1\rangle)\right\}$$

$$\sigma_x : \quad B_0 = \left\{|00\rangle := 2^{-\frac{1}{2}}(|0\rangle + |1\rangle), \quad |01\rangle := 2^{-\frac{1}{2}}(|0\rangle - |1\rangle)\right\}$$

- telles que

$$\forall \alpha \in \mathbb{Z}_2, \; \forall \beta \in \mathbb{Z}_2 : |\langle a\alpha | b\beta \rangle| = \begin{cases} \delta_{\alpha,\beta} \text{ si } a = b \\ \frac{1}{\sqrt{2}} \text{ si } a \neq b \end{cases}$$

du particulier au général (fin)

- 2 bases orthonormées distinctes de $\mathbb{C}^d$

$$B_a = \{|a\alpha\rangle : \alpha \in \mathbb{Z}_d\}, \quad B_b = \{|b\beta\rangle : \beta \in \mathbb{Z}_d\}$$

sont dites non biaisées si

$$\forall \alpha \in \mathbb{Z}_d,\ \forall \beta \in \mathbb{Z}_d : |\langle a\alpha|b\beta\rangle| = \frac{1}{\sqrt{d}}$$

- on a équiprobabilité

$$|b\beta\rangle = \sum_{\alpha \in \mathbb{Z}_d} |a\alpha\rangle\langle a\alpha|b\beta\rangle, \quad |\langle a\alpha|b\beta\rangle|^2 = \frac{1}{d}$$

- ensemble de bases **mutuellement** non biaisées (MUBs) : ensemble de bases non biaisées 2 à 2

- toute transformation unitaire ou anti-unitaire sur un ensemble de MUBs conduit à un autre ensemble de MUBs

LIEN ENTRE MUBs

et

MÉCANIQUE QUANTIQUE

lien avec les observables complémentaires de N. Bohr

- les bases non biaisées sont des bases de vecteurs propres d'observables 2 à 2 complémentaires ou conjuguées

- un système préparé dans n'importque quel état de B_b a une probabilité de distribution uniforme (à savoir, $\frac{1}{d}$) d'être trouvé dans n'importe quel état de B_a

- $\Rightarrow$ incertitude complète sur la mesure dans une base B_a relative à une observable A préparée dans une base B_b relative à une observable B qui est non biaisée avec la précédente

lien avec les observables complémentaires de N. Bohr (fin)

- **Ex 1 :** x et p_x en dimension infinie

$$[x, p_x] = \mathrm{i}\hbar \;\Rightarrow\; \Delta x \Delta p_x \geq \frac{\hbar}{2}$$

- **Ex 2 :** σ_x, σ_y et σ_z en dimension $d = 2$

$$[\sigma_x, \sigma_y] = 2\mathrm{i}\sigma_z \;\Rightarrow\; \Delta S_x \Delta S_y \geq \frac{\hbar}{2}|\langle S_z \rangle|$$

- **N.B. :** $A = \sigma_x$ et $B = \sigma_y$ satisfont (avec $d = 2$)

$$AB - \mathrm{e}^{\mathrm{i}\frac{2\pi}{d}} BA = 0 \;\Rightarrow\; [A, B] = (1 - \mathrm{e}^{-\mathrm{i}\frac{2\pi}{d}})AB$$

à comparer aux relations satisfaites par une paire de Weyl

RÉSULTATS BIEN CONNUS*

et

PROBLÈMES OUVERTS

* Schwinger (1960) — Ivanović (1981) — Wooters et Fields (1989) — Calderbank *et al.* (1997) — Bandyopadhyay *et al.* (2002) — Lawrence *et al.* (2002) — Pittenger et Rubin (2004)

$N =$ nombre maximum de MUBs dans $\mathbb{C}^d$?

- cas d arbitraire

$$3 \leq N \leq d+1$$

($\Rightarrow N = 3$ pour $d = 2$, N ne peut excéder $d+1$)

- cas $d = p^m$ (p premier, $m \in \mathbb{N}^*$)

$$N = d+1$$

($d+1 =$ nombre minimum de mesures pour déterminer une matrice densité)

- cas $d = \prod_i p_i^{m_i}$ composite (p_i premier, $m_i \in \mathbb{N}^*$)

$$\min(p_i^{m_i}) + 1 \leq N \leq d+1$$

($\Rightarrow 3 \leq N \leq 7$ pour $d = 6$)

$N =$ **nombre maximum de MUBs dans** $\mathbb{C}^d$ **?** (fin)

- **définition**

pour $N = d + 1$, on a un **ensemble complet** de MUBs

- **problèmes ouverts**

*** N pour $d \neq p^m$?

*** N pour $d = 6$?

exemples

- pour $d = 6 = 2 \times 3$, on a

$$3 \leq N \leq 7$$

on n'a jamais trouvé plus de 3 MUBs et il a été conjecturé que $N = 3$

- pour $d = 15 = 3 \times 5$ and $d = 21 = 3 \times 7$, on a au moins 4 MUBs

- pour $d = 676 = 2^2 \times 13^2$

$$2^2 + 1 = 5 \leq N \leq 677$$

mais on au moins 6 MUBs.

résultat général

• soit un ensemble de $d^2 - 1$ opérateurs unitaires, de trace nulle et mutuellement orthogonaux agissant sur $\mathbb{C}^d$

• si cet ensemble peut être partitionné en $d + 1$ sous ensembles contenant chacun $d - 1$ opérateurs qui commutent

alors les vecteurs propres communs relatifs à chaque sous ensemble fournissent une base de $\mathbb{C}^d$ et l'ensemble des $d + 1$ bases obtenues est un **ensemble complet de $d + 1$ MUBs**

• c'est le cas pour $d = p^m$ (p premier, $m \in \mathbb{N}^*$)

LIENS ENTRE

MUBs, PHYSIQUE ET MATHÉMATIQUES

- **liens avec la physique**

– matrices de Pauli généralisées – moment angulaire généralisé – matrice densité – espace de phase discret – distribution de Wigner discrète – états de phase discrets – formalisme de l'intégrale de chemin

- **liens avec les mathématiques**

– transformation de Fourier (quadratique) – corps et anneaux de Galois – théorie des groupes (groupes finis cycliques et groupes de Lie) – théorie des nombres – géométrie finie (géométrie projective) – "2-designs" sphériques – polytopes convexes – analyse combinatoire – carrés latins mutuellement orthogonaux – théorie des graphes – matrices de Hadamard

- **liens** $\Rightarrow$

des méthodes de construction des MUBs et des conjectures sur les MUBs

liens entre MUBs et mathématiques

le fait que la limite $N = d + 1$ soit atteinte lorsque $d = p^m$, p premier et $m \in \mathbb{N}^*$, permet de jeter un pont vers les mathématiques

- corps et anneaux finis
- géométrie projective
- groupes de Lie

TROIS CONJECTURES

et

UNE PROPOSITION

conjecture 1 [Zauner (1999)]

si $d = 6$, le nombre maximum de MUBs est égal à 3

N.B.

• en dépit de très nombreux travaux théoriques et numériques, il n'a jamais été trouvé plus de 3 MUBs pour $d = 6$

Golden KCIK Award

attribué par le **National Quantum Information Centre (KCIK)** (Pologne) à quiconque résoudra un des cinq problèmes ouverts en information quantique, en particulier :

KCIK Problem N°2. Construct a set of at least 4 mutually unbiased bases (MUBs) of order six or prove that there are no 7 MUBs in H_6.

2020 euros par problème résolu - pour plus d'information voir :

Horodecki, Rudnicki, Zyczkowski - arXiv :2002.03233, 2020

conjecture 2 [Saniga, Planat, Rosu (2004)]

dans le cas où d n'est pas une puissance d'un premier, le problème de l'existence d'un **ensemble complet de** $d+1$ **MUBs** dans $\mathbb{C}^d$ est équivalent à celui de l'existence d'un **plan projectif** fini d'ordre d

N.B.

- illustre le lien entre MUBs et géométrie projective

conjecture 2 (fin : définition d'un plan projectif)

• un plan projectif d'ordre d est une structure de d^2+d+1 lignes et d^2+d+1 points avec

– chaque ligne a $d+1$ points

– chaque point appartient à $d+1$ lignes

– deux lignes se croisent en un seul point

– deux points appartiennent à une seule ligne

• exemple : le plan de Fano ($d=2$, $d^2+d+1=7$, $d+1=3$)

• théorème : un plan projectif existe pour $d=p^m$ (p premier, $m \in \mathbb{N}^*$)

conjecture 3 [inspirée de Kostrikin *et al.* (1981), Zassenhauss et Patera (1988), Boykin *et al.* (2007)]

dans le cas où d n'est pas une puissance d'un premier, le problème de l'existence d'un **ensemble complet de** $d+1$ **MUBs** dans $\mathbb{C}^d$ est équivalent à celui de l'existence d'une décomposition orthogonale de $sl(d,\mathbb{C})$ en $d+1$ sous algèbres de Cartan de dimension $d-1$

N.B.

- illustre le lien entre MUBs et groupes de Lie

conjecture 3 (fin : à propos de décomposition orthogonale)

* décomposition orthogonale d'une algèbre de Lie L sur $\mathbb{C}$ = décomposition de L en une somme directe de sous algèbres de Cartan qui sont 2 à 2 orthogonales

* conjecture (Kostrikin) : $L = sl(d, \mathbb{C})$ admet une décomposition orthogonale sii d est une puissance d'un nombre premier

* si la conjecture est vraie : on a non existence de $d + 1$ MUBs lorsque d n'est pas la puissance d'un nombre premier

* extension au cas de $sl(d, A)$ où A est un anneau fini commutatif avec une identité (Songpon Sriwongsa et Yi Ming Zou)

proposition [Albouy, Kibler (2007)]
trouver un **ensemble complet de** $d+1$ **(**d **arbitraire) MUBs**

$$B_a = \{|a\alpha\rangle : \alpha = 0, 1, \cdots, d-1\}, \quad a = 0, 1, \cdots, d$$

i.e., $d(d+1)$ vecteurs dans $\mathbb{C}^d$ satisfaisant

$$|\langle a\alpha|b\beta\rangle| = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{\sqrt{d}}(1-\delta_{a,b}) \tag{1}$$

revient à trouver $d+1$ ensembles

$$S_a = \{w(a\alpha) : \alpha = 0, 1, \cdots, d-1\}, \quad a = 0, 1, \cdots, d$$

de vecteurs

$$w(a\alpha) = \Big(w_0(a\alpha), w_1(a\alpha), \cdots, w_{d^2-1}(a\alpha)\Big) \in \mathbb{C}^{d^2}$$

i.e., $d(d+1)$ vecteurs dans $\mathbb{C}^{d^2}$ satisfaisant

$$w(a\alpha)\cdot w(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b}) \tag{2}$$

proposition (suite)

• si $\exists$ un ensemble complet de $d+1$ MUBs dans $\mathbb{C}^d$ alors $\exists$ $d+1$ ensembles

$$S_a = \{w(a\alpha) : \alpha = 0, 1, \cdots, d-1\}, \quad a = 0, 1, \cdots, d$$

de vecteurs

$$w(a\alpha) = \Big(w_0(a\alpha), w_1(a\alpha), \cdots, w_{d^2-1}(a\alpha)\Big) \in \mathbb{C}^{d^2}$$

tels que

$$w(a\alpha) \cdot w(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \qquad (2)$$

et réciproquement

• si on ne peut pas trouver $d(d+1)$ vecteurs de $\mathbb{C}^{d^2}$ satisfaisant (2), alors il n'existe pas d'ensemble complet de MUBs dans $\mathbb{C}^d$

proposition (fin)

- chaque ensemble S_a contient d vecteurs orthonormés dans $\mathbb{C}^{d^2}$ mais ne constitue pas une base

- est-il plus facile de trouver les $w(a\alpha)$ que les $|a\alpha\rangle$?

- (2) a $d(d+1)$ solutions pour $d = p^m$ (p premier, $m \in \mathbb{N}^*$)

- (2) a-t-elle $d(d+1)$ solutions pour d arbitraire ?

- la relation (2) pour $a \neq b$

$$w(a\alpha) \cdot w(b\beta) = \cos^{-1}\left(\frac{1}{d}\right)$$

(vraie pour $a, b = 0, 1, \cdots, d$ et $\alpha, \beta = 0, 1, \cdots, d-1$) fait penser à des 2-designs sphériques

extension de la notion de MUBs

• WMUBs = weak mutually unbiased bases (Vourdas et coll.)

dans le cadre de la MQ sur l'anneau $\mathbb{Z}_d$:

$$|\langle a\alpha|b\beta\rangle|^2 = \frac{1}{f}, \quad b \neq a, \quad f|d$$

avec WMUBs $\hookrightarrow$ MUBs pour $f \hookrightarrow d$

• κ-MUBs = κ-mutually unbiased bases en dimension d (Kalev et Gilad)

$$|\langle a\alpha|b\beta\rangle|^2 = \delta_{ab}\delta_{\alpha\beta}\kappa + \frac{1}{d}(1-\delta_{ab}) + \frac{1-\kappa}{d-1}(1-\delta_{\alpha\beta})\delta_{ab}, \quad \frac{1}{d} \leq \kappa \leq 1$$

avec κ-MUBs $\rightarrow$ MUBs pour $\kappa \rightarrow 1$

INTÉRÊTS DES MUBs

1. **mécanique quantique en dimension finie**
- tomographie d'états quantiques
- fonction de Wigner discrète
- problème du roi méchant
- formalisme de l'intégrale de chemin

2. **information classique**
- codes correcteurs d'erreurs (code $\mathbb{Z}_{2^2}$-Kerdock)
- protocoles de communication en réseau

3. **information quantique**
- cryptographie quantique (exemple : protocole BB84)
- codes correcteurs d'erreurs quantiques
- téléportation quantique (transporter un qubit)
- détection de l'intrication
- codage quantique

CONSTRUCTION DES MUBs

nombreuses méthodes de construction ; ici on s'intéresse à

- **méthodes physiques**

– moment angulaire ou spin généralisé

– transformation de Fourier <quadratique>

- **méthodes mathématiques**

– utilisation de la méthode de Weyl et Heisenberg

– groupes de Lie $\left(\text{par exemple : SU(2) ou SL(2,}\mathbb{C}\text{)}\right)$

– corps de Galois pour $d = p^m$ (p premier impair, $m \in \mathbb{N}^*$)

– anneaux de Galois pour $d = 2^m$ ($m \in \mathbb{N}^*$)

APPROCHE VIA LE GROUPE SU(2)

su(2) ou moment angulaire généralisé

- $[J_x, J_y] = \mathrm{i} J_z, \quad [J_y, J_z] = \mathrm{i} J_x, \quad [J_z, J_x] = \mathrm{i} J_y$
- $J^2 = J_x^2 + J_y^2 + J_z^2$ (opérateur de Casimir)
- J_z (générateur de Cartan)
- $\{J^2, J_z\}$ (ensemble complet d'opérateurs qui commutent)

vecteurs propres communs de J^2 et J_z

$$B_{2j+1} = \{|j, m\rangle : m = j, j-1, \cdots, -j\}, \quad 2j \in \mathbb{N}$$

$\Rightarrow$ **base standard** pour la rep irr (j) de su(2)

décomposition polaire de su(2)

- introduisons les opérateurs échelle

$$J_+ := J_x + \mathrm{i}J_y, \quad J_- := J_x - \mathrm{i}J_y$$

- on a la décomposition

$$J_+ = HV_a, \quad J_- = V_a^\dagger H, \quad J_z = \frac{1}{2}(H^2 - V_a^\dagger H^2 V_a)$$

avec H hermitien et V_a unitaire définis par

$$H|j,m\rangle = \sqrt{(j+m)(j-m+1)}|j,m\rangle$$
$$V_a|j,m\rangle = \omega^{(j-m)a}|j, m+1 \bmod (2j+1)\rangle$$

où

$$\omega = \mathrm{e}^{\mathrm{i}\frac{2\pi}{2j+1}}, \quad a \in \mathbb{Z}_{2j+1}$$

le schéma $\{J^2, V_a\}$ comme alternative au schéma $\{J^2, J_z\}$

- $\{J^2, V_a\}$: ensemble complet d'opérateurs qui commutent

- pour j ($2j \in \mathbb{N}$) et a ($a \in \mathbb{Z}_{2j+1}$) fixés, les vecteurs propres communs de J^2 et V_a sont

$$|a\alpha\rangle = \frac{1}{\sqrt{2j+1}} \sum_{m=-j}^{j} \omega^{\frac{1}{2}(j+m)(j-m+1)a+(j+m)\alpha} |j, m\rangle$$

avec $\alpha \in \mathbb{Z}_{2j+1}$; de plus

$$V_a|a\alpha\rangle = \omega^{ja-\alpha}|a\alpha\rangle$$

(spectre de V_a non dégénéré)

- problème ouvert : pour $j \in \mathbb{N}$, analogue pour le schéma $\{J^2, V_a\}$ des harmoniques sphériques du schéma $\{J^2, J_z\}$?

retour vers les MUBs

• pour j et a fixés, les $2j+1$ vecteurs propres $|a\alpha\rangle$ fournissent une base orthonormée

$$B_a = \{|a\alpha\rangle : \alpha \in \mathbb{Z}_{2j+1}\}$$

pour la rep irr (j) de su(2)

• pour j fixé, il existe $2j+1$ bases B_a

• question : les bases B_a $(a = 0, 1, \cdots, 2j)$ et la base standard B_{2j+1} forment-elles un ensemble complet de MUBs dans $\mathbb{C}^{2j+1}$?

application aux MUBs

• en posant

$$d = 2j + 1, \quad n = j + m, \quad |n\rangle = |j, m\rangle$$

les vecteurs propres de V_a deviennent

$$|a\alpha\rangle = \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} \omega^{\frac{1}{2}n(d-n)a + n\alpha} |n\rangle, \quad \omega = \mathrm{e}^{\mathrm{i}\frac{2\pi}{d}}$$

• **théorème** : pour $d = p$, p premier (pair ou impair), the p bases

$$B_a = \{|a\alpha\rangle : \alpha \in \mathbb{F}_p\}, \quad a \in \mathbb{F}_p$$

et la base standard (ou canonique ou de calcul)

$$B_p = \{|n\rangle : n \in \mathbb{F}_p\}$$

forment un **ensemble complet de $p + 1$ MUBs de $\mathbb{C}^p$**

• pour d arbitraire, au moins 2 des bases B_a ($a \in \mathbb{Z}_d$) et la base B_d constituent 3 MUBs

démo (basée sur sommes de Gauss généralisées)

(1) la base B_p est non biaisée avec les p bases $B_0, B_1, \cdots, B_{p-1}$
(2) considérons

$$\langle a\alpha|b\beta\rangle = \frac{1}{p}\sum_{k=0}^{p-1} \mathrm{e}^{\mathrm{i}\frac{\pi}{p}\{(a-b)k^2+[(b-a)p+2(\beta-\alpha)]k\}}$$

for $b \neq a$; introduisons la somme de Gauss généralisée

$$S(u,v,w) = \sum_{k=0}^{|w|-1} \mathrm{e}^{\mathrm{i}\frac{\pi}{w}(uk^2+vk)}$$

où u, v, w entiers ; u, w co-premiers ; $uw \neq 0$; $uw+v$ pair ; alors

$$\langle a\alpha|b\beta\rangle = \frac{1}{p}S(u,v,w),\ u = a-b,\ v = -(a-b)p-2(\alpha-\beta),\ w = p$$

or $|S(u,v,w)| = \sqrt{p}$ et donc $|\langle a\alpha|b\beta\rangle| = \frac{1}{\sqrt{p}}$ (**c.q.f.d.**)

exemple : $d = 3$

- formule générale pour $|a\alpha\rangle \Rightarrow$

$$B_a = \left\{ |a\alpha\rangle = \frac{1}{\sqrt{3}} \left(\omega^{a+2\alpha} |0\rangle + \omega^{a+\alpha} |1\rangle + |2\rangle \right) : \alpha = 0, 1, 2 \right\}$$

avec

$$\omega = \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}}, \quad a = 0, 1, 2$$

- aux 3 bases B_a ($a = 0, 1, 2$) il faut ajouter la base canonique

$$B_3 = \{ |n\rangle : n = 0, 1, 2 \}$$

- d'où $d + 1 = 4$ MUBs

MUBs pour $d = p^m$ (p premier, $m > 1$)

• si d est remplacé par p^m dans la formule donnant $|a\alpha\rangle \in \mathbb{C}^d$ on n'obtient pas un ensemble complet of $p^m + 1$ MUBs de $\mathbb{C}^{p^m}$

• mais la formule donnant $|a\alpha\rangle \in \mathbb{C}^p$ peut être utilisée pour dériver un ensemble complet de $p^m + 1$ MUBs de $\mathbb{C}^{p^m}$ par produit tensoriel d'ordre m des $|a\alpha\rangle$

• cela revient à remplacer V_a par un produit tensoriel du type $V_{a_1} \otimes V_{a_2} \otimes \cdots \otimes V_{a_m}$

MUBs pour $d = p^m$ (p premier, $m > 1$) (suite)

example : $d = 2^2$

- soit 2 systèmes de qubits correspondant à $j_1 = \frac{1}{2}$ and $j_2 = \frac{1}{2}$
- $\Rightarrow$ bases de $\mathbb{C}^4$ à partir de produits tensoriels $|a\alpha\rangle \otimes |b\beta\rangle$, vecteurs propres de $V_a \otimes V_b$
- $B_{ab} = \{|a\alpha\rangle \otimes |b\beta\rangle : \alpha, \beta = 0, 1\}$ est une base orthonormée de $\mathbb{C}^4$
- les bases B_{00} et B_{11} sont 2 bases non biaisées
- il en est de même pour les bases B_{01} et B_{10}

MUBs pour $d = p^m$ (p premier, $m > 1$) (fin)

- $\Rightarrow$ les bases B_{00}, B_{11}, B_{01} et B_{10} ne constituent pas des MUBs

- par contre les 4 bases

$$
\begin{aligned}
W_{00} &= \{|0\alpha\rangle \otimes |0\beta\rangle : \alpha, \beta = 0, 1\} \equiv B_{00} \\
W_{11} &= \{|1\alpha\rangle \otimes |1\beta\rangle : \alpha, \beta = 0, 1\} \equiv B_{11} \\
W_{01} &= \{\lambda|0\alpha\rangle \otimes |1\beta\rangle + \mu|0\alpha \oplus 1\rangle \otimes |1\beta \oplus 1\rangle : \alpha, \beta = 0, 1\} \\
W_{10} &= \{\lambda|1\alpha\rangle \otimes |0\beta\rangle + \mu|1\alpha \oplus 1\rangle \otimes |0\beta \oplus 1\rangle : \alpha, \beta = 0, 1\}
\end{aligned}
$$

où

$$\lambda = \frac{1 - \mathrm{i}}{2}, \quad \mu = \frac{1 + \mathrm{i}}{2}$$

sont des MUBs et constituent avec la base canonique

$$\{|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle\}$$

un **ensemble complet de d+1 = 5 MUBs**

SOUS PRODUITS DE L'APPROCHE

SU(2) – MOMENT ANGULAIRE GÉNÉRALISÉ

1. matrices de Hadamard

• l'introduction dans $|a\alpha\rangle$ de $(H_a)_{n\alpha}$ défini par

$$(H_a)_{n\alpha} = \frac{1}{\sqrt{d}}\,\omega^{\frac{1}{2}n(d-n)a+n\alpha}, \quad n,\alpha = 0,1,\cdots,d-1$$

conduit à

$$|a\alpha\rangle = \sum_{n\in\mathbb{Z}_d} (H_a)_{n\alpha}\,|n\rangle$$

• la matrice H_a d'éléments $(H_a)_{n\alpha}$ est une matrice de Hadamard généralisée

• en termes de vecteur colonne, le vecteur $|a\alpha\rangle$ est donné par la colonne α de H_a

1. **matrices de Hadamard** (fin)

- pour d arbitraire

$$\langle a\alpha|b\beta\rangle = \left(H_a{}^{\dagger} H_b\right)_{\alpha\beta}$$

- pour $d = p$ premier

$$\left|\left(H_a{}^{\dagger} H_b\right)_{\alpha\beta}\right| = \frac{1}{\sqrt{p}}$$

- $\Rightarrow$ le produit $H_a{}^{\dagger} H_b$ est une autre matrice de Hadamard généralisée pour $d = p$ premier

2. paires de Weyl

- l'opérateur V_a se décompose suivant

$$V_a = Z^a X, \quad a = 0, 1, \cdots, d-1$$

où X et Z sont définis par

$$\begin{aligned} X|n\rangle &= |n+1 \text{ mod } d\rangle \\ Z|n\rangle &= \omega^{-n}|n\rangle \end{aligned}$$

avec $n = 0, 1, \cdots, d-1$

- les opérateurs

$$X = V_0, \quad Z = V_1 V_0^\dagger$$

sont reliés par

$$H_0^\dagger X H_0 = Z \;\Leftrightarrow\; X = H_0 Z H_0^\dagger$$

2. **paires de Weyl** (suite)

- forme matricielle de V_a

$$V_a = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ \omega^{-a} & 0 & \cdots & 0 & 0 \\ 0 & \omega^{-2a} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & 0 & \vdots \\ 0 & 0 & \cdots & \omega^{-(d-1)a} & 0 \end{pmatrix}$$

- forme matricielle de X et Z

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega^{d-1} & 0 & \cdots & 0 \\ 0 & 0 & \omega^{d-2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{1} \end{pmatrix}$$

2. **paires de Weyl** (fin)

- le couple (X, Z) est une paire de Weyl

- les opérateurs X et Z satisfont les relations de cyclicité

$$X^d = Z^d = I_d$$

et la relation de ω-commutation

$$XZ - \omega ZX = O_d \;\Leftrightarrow\; [X, Z] = (1 - \omega^{-1})XZ$$

avec I_d et O_d matrice identité et matrice nulle, respectivement

- pour $d = 2$: $X = \sigma_x$, $Z = \sigma_z$ et $XZ = -\mathrm{i}\sigma_y$

3. algèbre de Lie W_∞

- en posant

$$T_m = \omega^{-\frac{1}{2}m_1 m_2} X^{m_1} Z^{m_2}, \quad m \equiv (m_1, m_2) \in \mathbb{N}^{*2}$$

on obtient

$$[T_m, T_n] = 2\mathrm{i} \sin\left(\frac{\pi}{d} m \times n\right) T_{m+n}$$

où

$$m \times n = m_1 n_2 - m_2 n_1, \quad m + n = (m_1 + n_1, m_2 + n_2)$$

de sorte que

- les T_m engendrent l'algèbre de Lie W_∞ (étudiée par Fairlie *et al.*, 2002)

4. groupe de Weyl

les d^2 matrices de Pauli généralisées

$$X^a Z^b, \quad a, b \in \mathbb{Z}_d$$

— forment une base pour tout opérateur agissant sur $\mathbb{C}^d$

— génèrent l'algèbre de Lie de U(d)

— sont des éléments d'un groupe fini d'ordre d^3, à savoir, le groupe de Pauli

$$\Pi_d = \Big(\{\omega^a X^b Z^c : a, b, c \in \mathbb{Z}_d\}, \times\Big)$$

qui est un sous groupe fini de U(d) ; le groupe Π_d est une discrétisation du groupe de Heisenberg et Weyl qui est un groupe de Lie dont l'algèbre de Lie est définie par

$$[Q, P] = \mathrm{i}H, \quad [H, Q] = 0, \quad [H, P] = 0$$

5. décomposition de sl$(p, \mathbb{C})$

• $\{X^a Z^b : a, b \in \mathbb{Z}_d\}$ et $\{X^a Z^b : a, b \in \mathbb{Z}_d\} \setminus \{X^0 Z^0\}$ engendrent les algèbres de Lie gl$(d, \mathbb{C})$ et sl$(d, \mathbb{C})$, respectivement

• **théorème :** pour $d = p$ premier, on a la décomposition

$$\text{sl}(p, \mathbb{C}) = \mathcal{V}_0 \oplus \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_p$$

où chacune des $p + 1$ sous algèbres $\mathcal{V}_0, \mathcal{V}_1, \cdots, \mathcal{V}_p$ est une sous algèbre de Cartan générée par $p - 1$ opérateurs qui commutent ; plus précisément

$$\mathcal{V}_0 = \{X^0 Z^a : a = 1, 2, \cdots, p-1\}$$

et

$$\mathcal{V}_{a+1} = \{X^b Z^{ab} : b = 1, 2, \cdots, p-1\}, \quad a \in \mathbb{F}_p$$

avec $V_a \in \mathcal{V}_{a+1}$ associé à la base B_a et $\mathcal{V}_0$ associé à la base canonique B_p

5. décomposition de sl($p, \mathbb{C}$) (fin)

exemples

– cas $p = 2$

$$\mathrm{sl}(2,\mathbb{C}) \text{ or } \mathrm{su}(2) = \mathcal{V}_0 \oplus \mathcal{V}_1 \oplus \mathcal{V}_2 = \sigma_x \oplus \sigma_y \oplus \sigma_z$$

en termes de matrices de Pauli

– cas $p = 3$

$$\mathrm{sl}(3,\mathbb{C}) \text{ or } \mathrm{su}(3) = \mathcal{V}_0 \oplus \mathcal{V}_1 \oplus \mathcal{V}_2 \oplus \mathcal{V}_3 =$$
$$\{X^0Z^1, X^0Z^2\} \oplus \{X^1Z^0, X^2Z^0\} \oplus \{X^1Z^1, X^2Z^2\} \oplus \{X^1Z^2, X^2Z^1\}$$

en termes de matrices X^aZ^b

CONSTRUCTION DES MUBS VIA LES CORPS DE GALOIS

(cas $d = p^m$, p premier impair, $m > 1$)

la structure de corps

– définition 1

un ensemble $\mathbb{K} \neq \emptyset$ muni de 2 lois internes, notées $+$ avec 0 pour neutre et $\times$ avec 1 pour neutre, est un corps sii

- $\mathbb{K}$ est un groupe commutatif pour $+$
- $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ est un groupe pour $\times$
- la loi $\times$ est distributive par rapport à la loi $+$

– définition 2

un corps fini est appelé corps de Galois

la structure de corps (suite)

– **théorème 1** (Wedderburn)

un corps de Galois est nécessairement commutatif (la loi $\times$ est commutative)

– **théorème 2**

• un corps de Galois a p^m éléments (p premier, $m \in \mathbb{N}^*$)

• tous les corps de Galois de cardinal p^m sont isomorphes, d'où la notation $\mathbb{GF}(p^m)$ pour un corps de Galois à p^m éléments

• le corps de Galois $\mathbb{GF}(p^m)$ est une **extension** du corps de Galois $\mathbb{GF}(p) \equiv \mathbb{Z}_p$ noté aussi $\mathbb{F}_p$

la structure de corps (fin)

exemple : tables (addition multiplication) de $\mathbb{GF}(2^2)$ d'éléments 0, 1, α, $1+\alpha$ (extension de $\mathbb{F}_2$ par α tel que $1+\alpha+\alpha^2=0$)

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

questions et réponses sur le lien entre MUBs et corps de Galois

Q1 comment passer de la base

$$B_a = \{|a\alpha\rangle : \alpha \in \mathbb{F}_p\}$$

de $\mathbb{C}^p$, avec $a \in \mathbb{F}_p$, à une base de $\mathbb{C}^{p^m}$?

Q2 comment obtenir un ensemble complet de $p^m + 1$ MUBs de $\mathbb{C}^{p^m}$?

questions et réponses sur le lien entre MUBs et corps de Galois (suite)

R1 pour passer des p bases $B_a = \{|a\alpha\rangle : \alpha \in \mathbb{F}_p\}$ de $\mathbb{C}^p$ à p^m bases

$$B_a = \{|a\alpha\rangle : \alpha \in \mathbb{GF}(p^m)\}$$

de $\mathbb{C}^{p^m}$, avec $a \in \mathbb{GF}(p^m)$, **'intuiter'** B_a **de** $\mathbb{C}^{p^m}$ **qui pour** $m = 1$ **donne** B_a **de** $\mathbb{C}^p$ **(via Tr**$(x) = x$ **pour** $x \in \mathbb{F}_p$**)**

R2 passer de la base $B_p = \{|n\rangle : n \in \mathbb{F}_p\}$ de $\mathbb{C}^p$ à la base

$$B_{p^m} = \{|n\rangle : n \in \mathbb{GF}(p^m)\}$$

de $\mathbb{C}^{p^m}$

questions et réponses sur le lien entre MUBs et corps de Galois (fin)

• en partant de la formule (**valable pour p pair ou impair**)

$$|a\alpha\rangle = \frac{1}{\sqrt{p}} \sum_{n\in\mathbb{F}_p} \omega^{\frac{1}{2}n(p-n)a+n\alpha}|n\rangle$$

puis en remplaçant $\frac{1}{2}n(p-n)a + n\alpha$ par $\mathrm{Tr}[\frac{1}{2}n(p-n)a + n\alpha]$ et $\mathbb{F}_p$ par $\mathbb{GF}(p^m)$ $\Rightarrow$ **absurdité**

• solution : partir d'une autre formule donnant les $|a\alpha\rangle$ de B_a ; en fait, pour p impair, les p bases orthonormées

$$B_a{}' = \left\{|a\alpha\rangle' = \frac{1}{\sqrt{p}} \sum_{n\in\mathbb{F}_p} \omega^{an^2+\alpha n}|n\rangle : \alpha \in \mathbb{F}_p\right\}$$

(avec $a \in \mathbb{F}_p$) fournissent une alternative aux p bases B_a

MUBs de $\mathbb{C}^{p^m}$ (p premier impair) via $\mathbb{GF}(p^m)$

- recette : pour passer du vecteur

$$\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \omega^{ax^2+\alpha x} |x\rangle$$

de $\mathbb{C}^p$ à un vecteur de $\mathbb{C}^{p^m}$, faire $\frac{1}{\sqrt{p}} \to \frac{1}{\sqrt{p^m}}$, $x \in \mathbb{F}_p \to x \in \mathbb{GF}(p^m)$ et remplacer

$$\omega^{ax^2+\alpha x}, \quad a, \alpha, x \in \mathbb{F}_p$$

par

$$\chi(ax^2 + \alpha x) = \omega^{\mathrm{Tr}(ax^2+\alpha x)}, \quad a, \alpha, x \in \mathbb{GF}(p^m)$$

où χ est le vecteur caractère additif de $\mathbb{GF}(p^m)$

- ceci conduit aux 2 propositions suivantes

MUBs de $\mathbb{C}^{p^m}$ (p premier impair) via $\mathbb{GF}(p^m)$ (suite)

proposition 1 :
pour p premier impair et $m \in \mathbb{N}^*$, l'ensemble

$$B_a = \{|a\alpha\rangle : \alpha \in \mathbb{GF}(p^m)\}$$

où

$$|a\alpha\rangle = \frac{1}{\sqrt{p^m}} \sum_{x \in \mathbb{GF}(p^m)} \omega^{\mathsf{Tr}(ax^2+\alpha x)}|x\rangle,\ a \in \mathbb{GF}(p^m),\ \omega = \mathsf{e}^{\mathsf{i}\frac{2\pi}{p}}$$

constitue une base orthonormée de $\mathbb{C}^{p^m}$

proposition 2 :
pour p premier impair et $m \in \mathbb{N}^*$, les p^m bases B_a, $a \in \mathbb{GF}(p^m)$, constituent avec la base canonique B_{p^m} un ensemble complet de $p^m + 1$ MUBs de $\mathbb{C}^{p^m}$

MUBs de $\mathbb{C}^{p^m}$ (p premier impair) via $\mathbb{GF}(p^m)$ (fin)

démo : soit $|a\alpha\rangle \in B_a$ et $|b\beta\rangle \in B_b$; on a

$$\langle a\alpha|b\beta\rangle = \frac{1}{p^m} \sum_{x\in\mathbb{GF}(p^m)} \omega^{\mathsf{Tr}[(b-a)x^2+(\beta-\alpha)x]}, \quad a,b,\alpha,\beta \in \mathbb{GF}(p^m)$$

et en utilisant la formule (valable pour p premier impair)

$$\left| \sum_{x\in\mathbb{GF}(p^m)} \omega^{\mathsf{Tr}(ux^2+vx)} \right| = \sqrt{p^m}, \quad u \in \mathbb{GF}(p^m)^*, \quad v \in \mathbb{GF}(p^m)$$

on obtient

$$|\langle a\alpha|b\beta\rangle| = \delta_{\alpha,\beta} \text{ si } b = a \text{ ou } \frac{1}{\sqrt{p^m}} \text{ si } b \neq a$$

$\Rightarrow B_a$ est une base orthonormée et (B_a, B_b), $b \neq a$, est un couple de bases non biaisées ; chaque base B_a est non biaisée avec la base canonique ; d'où un total de $p^m + 1$ MUBs

CONSTRUCTION DES MUBS VIA LES ANNEAUX DE GALOIS

(cas $d = 2^m$, $m > 1$)

la structure d'anneau

– **définition 1 :** un ensemble $R \neq \emptyset$ muni de 2 lois internes ($+$ avec 0 pour neutre et $\times$) est un anneau, noté $(R, +, \times)$, sii

- $(R, +)$ est un groupe commutatif
- la loi $\times$ est associative et distributive par rapport à la loi $+$

– **définition 2 :** l'anneau est dit unitaire si il contient une unité pour la loi $\times$

– **ex 1 :** l'anneau $\mathbb{Z}$ des entiers
– **ex 2 :** l'anneau $2\mathbb{Z}$ des entiers pairs
– **ex 3 :** l'anneau des matrices carrées sur $\mathbb{R}$ ou $\mathbb{C}$
– **ex 4 :** l'anneau $\mathbb{Z}_4$ des entiers modulo 4 (se généralise à $\mathbb{Z}_d$ des entiers modulo d)

la structure d'anneau (suite)

- tables de multiplication et d'addition de $\mathbb{Z}_4$

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_4, \times)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- présence du diviseur de zéro 2 ($2 \times 2 = 0$) en plus de 0

la structure d'anneau (suite)

idéal principal d'un anneau commutatif

• un sous ensemble $I \neq \emptyset$ d'un anneau commutatif $(R, +, \times)$ tel que

$$\forall r \in R,\ \forall i \in I,\ \forall j \in I : i + j \in I,\ i \times r \in I$$

est appelé **idéal** de $(R, +, \times)$

• un idéal I d'un anneau commutatif $(R, +, \times)$ est dit **principal** si il est généré par un élément a de R $(I = a \times R)$

• l'**idéal principal** généré par a est noté $\langle a \rangle$

anneau de Galois

c'est un anneau fini, unitaire et commutatif tel que l'ensemble de ses diviseurs de 0 incluant 0 constitue un idéal principal $\langle p \rangle$ avec p premier

la structure d'anneau (suite)

contre-exemple

$\mathbb{Z}_6$ est un anneau fini, unitaire et commutatif pour lequel l'ensemble des diviseurs de 0 est $\{0, 2, 3, 4\}$; cet ensemble n'est pas un idéal de $\mathbb{Z}_6$; donc, $\mathbb{Z}_6$ **n'est pas un anneau de Galois**

exemples

$\mathbb{Z}_4$, $\mathbb{Z}_8$ et $\mathbb{Z}_9$ sont des anneaux finis, unitaires et commutatifs pour lesquels les diviseurs de 0 incluant 0 constituent un idéal principal ; donc, $\mathbb{Z}_4$**,** $\mathbb{Z}_8$ **et** $\mathbb{Z}_9$ **sont des anneaux de Galois**

	ensemble des diviseurs de 0	idéal principal $\langle p \rangle$
$\mathbb{Z}_4 = \mathbb{Z}_{2^2}$	$\{0, 2\}$	$\langle 2 \rangle$
$\mathbb{Z}_8 = \mathbb{Z}_{2^3}$	$\{0, 2, 4, 6\}$	$\langle 2 \rangle$
$\mathbb{Z}_9 = \mathbb{Z}_{3^2}$	$\{0, 3, 6\}$	$\langle 3 \rangle$

la structure d'anneau (suite)

l'anneau de Galois $\mathbb{Z}_{p^s}$

• l'anneau $\mathbb{Z}_{p^s}$ des entiers modulo p^s, p premier et $s \in \mathbb{N}^*$, est un anneau de Galois (1 est l'identité de $\mathbb{Z}_{p^s}$, les diviseurs de 0 incluant 0 de $\mathbb{Z}_{p^s}$ constituent l'idéal principal $\langle p \rangle$ de $\mathbb{Z}_{p^s}$)

• $\mathbb{Z}_{p^s}$ a p^s éléments

• si $s = 1$, $\mathbb{Z}_{p^1} = \mathbb{Z}_p$ pour lequel le seul diviseur de 0 est 0 ; l'idéal $\langle 0 \rangle$ de $\mathbb{Z}_p$ est un idéal principal $\Rightarrow$ $\mathbb{Z}_p$ est un anneau de Galois qui est en fait le corps de Galois $\mathbb{F}_p$

la structure d'anneau (fin)

l'anneau de Galois $\mathbb{GR}(p^s, m)$

• l'anneau $\mathbb{GR}(p^s, m)$ est une extension de $\mathbb{GR}(p^s, 1) \equiv \mathbb{Z}_{p^s}$ au même titre que le corps $\mathbb{GF}(p^m)$ est une extension de $\mathbb{GF}(p)$

• $\mathbb{GR}(p^s, m)$ possède $(p^s)^m$ éléments

• si $s = 1$, on a $\mathbb{GR}(p, m) = \mathbb{GF}(p^m)$

• pour l'application aux MUBs, on utilise $\mathbb{GR}(2^2, m)$ qui a 4^m éléments

MUBs de $\mathbb{C}^{2^m}$ ($p = 2$, premier pair) via $\mathbb{GR}(2^2, m)$

– nécessité de remplacer le corps de Galois $\mathbb{GF}(2^m)$

• pour $d = 2^m$, $m \in \mathbb{N}^*$, l'utilisation du corps de Galois $\mathbb{GF}(2^m)$ ne permet pas de construire un ensemble complet de $2^m + 1$ MUBs de $\mathbb{C}^{2^m}$

• pour $d = 2^m$ (cas correspondant à m qubits), on peut utiliser l'anneau de Galois $\mathbb{GR}(2^2, m)$ pour construire $2^m + 1$ MUBs de $\mathbb{C}^{2^m}$

MUBs de $\mathbb{C}^{2^m}$ ($p = 2$, premier pair) via $\mathbb{GR}(2^2, m)$ (suite)

– étiquetage des états dans le cadre de $\mathbb{GR}(2^2, m)$

• les 2^m vecteurs de la base canonique B_{2^m} sont étiquetés à l'aide des 2^m éléments de l'ensemble de Teichmüller T_m associé à l'anneau de Galois $\mathbb{GR}(2^2, m)$; ainsi

$$B_{2^m} = \{|x\rangle : x \in T_m\}$$

• les 2^m vecteurs de chacune des 2^m bases B_a sont étiquetés à l'aide des 2^m éléments de l'ensemble de Teichmüller T_m

• plus précisément, on a les 2 propositions suivantes

MUBs de $\mathbb{C}^{2^m}$ ($p = 2$, premier pair) via $\mathbb{GR}(2^2, m)$ (suite)

proposition 1 : pour a et α dans T_m, soit

$$|a\alpha\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in T_m} \chi[(a + 2\alpha)x]|x\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in T_m} \mathrm{e}^{\mathrm{i}\frac{2\pi}{4}\mathrm{Tr}(ax+2\alpha x)}|x\rangle$$

où χ est le vecteur caractère additif de $\mathbb{GR}(2^2, m)$ et la trace prend ses valeurs dans $\mathbb{Z}_4$; pour a fixé dans T_m, l'ensemble

$$B_a = \{|a\alpha\rangle : \alpha \in T_m\}$$

constitue une base orthonormée de $\mathbb{C}^{2^m}$

proposition 2 : les 2^m bases B_a, avec $m \in \mathbb{N}^*$ et $a \in T_m$, constituent avec la base canonique B_{2^m} un ensemble complet de 2^m+1 MUBs de $\mathbb{C}^{2^m}$

MUBs de $\mathbb{C}^{2^m}$ ($p = 2$, premier pair) via $\mathbb{GR}(2^2, m)$ (fin)

démo : soit $|a\alpha\rangle \in B_a$ et $|b\beta\rangle \in B_b$; on a

$$\langle a\alpha|b\beta\rangle = \frac{1}{2^m} \sum_{x \in T_m} \mathrm{e}^{\mathrm{i}\frac{2\pi}{4}\mathrm{Tr}[(b-a+2\beta-2\alpha)x]}$$

et en utilisant

$$\left| \sum_{x \in T_m} \mathrm{e}^{\mathrm{i}\frac{\pi}{2}\mathrm{Tr}(ux)} \right| = \begin{cases} 0 \text{ if } u \in 2T_m,\ u \neq 0 \\ 2^m \text{ if } u = 0 \\ \sqrt{2^m} \text{ otherwise} \end{cases}$$

on obtient

$$|\langle a\alpha|b\beta\rangle| = \delta_{\alpha,\beta} \text{ if } b = a \quad \text{or} \quad \frac{1}{\sqrt{2^m}} \text{ if } b \neq a$$

$\Rightarrow B_a$ est une base orthonormée et (B_a, B_b), $b \neq a$, est un couple de bases non biaisées ; chaque base B_a est non biaisée avec la base canonique ; d'où un total de $2^m + 1$ MUBs

FIN DE LA PARTIE 1

nombreuses références dans le livre et articles suivants :

• Galois Fields and Galois Rings Made Easy, iste press et elsevier (Londres, 2017)

• dans : J. Phys. A : Math. Theor. 41 (2008) 375302 (19pp)

• dans : J. Phys. A : Math. Theor. 42 (2009) 353001 (28pp)

en accès libre :

• Quantum Information : A Brief Overview and Some Mathematical Aspects, dans : Mathematics 2018, 6(12), 273 (Special Issue : Computer Algebra in Scientific Computing)

`https://www.mdpi.com/2227-7390/6/12/273`

PARTIE 2

CARACTÉRISATION DE L'INTRICATION D'ÉTATS MULTI-QUBITS SYMÉTRIQUES*

*travail en collaboration avec Mohammed Daoud

dans la partie 2 il sera question de

- qubits et algèbre de Weyl et Heisenberg généralisée
- états de Dicke
- qudits séparables
- description de Majorana
- introduction de la perma-concurrence
- exemples
- conclusions partie 2

QUBITS
et
ALGÈBRE DE WEYL ET HEISENBERG GÉNÉRALISÉE

algèbre d'opérateurs associés à $N = 1$ qubit

- Hilbert $\mathcal{H}_2$ à 2 dimensions avec une base orthonormée $\{|0\rangle,\ |1\rangle\}$

- en MQ : $|0\rangle$ and $|1\rangle$ représentent les états d'un système à 2 niveaux ($|0\rangle = |\frac{1}{2}, \frac{1}{2}\rangle$ et $|1\rangle = |\frac{1}{2}, -\frac{1}{2}\rangle$)

- opérateur $\downarrow$: $q^- = |0\rangle\langle 1| \ \Rightarrow\ q^-|1\rangle = |0\rangle,\ q^-|0\rangle = 0$

- opérateur $\uparrow$: $q^+ = |1\rangle\langle 0| \ \Rightarrow\ q^+|0\rangle = |1\rangle,\ q^+|1\rangle = 0$

- opérateur nombre : $K = |1\rangle\langle 1| \ \Rightarrow\ K|1\rangle = |1\rangle,\ K|0\rangle = 0$

$$(q^-)^\dagger = q^+,\ K^\dagger = K,\ [q^-, q^+] = \mathbb{I} - 2K,\ [K, q^\pm] = \pm q^\pm$$

$$(q^-)^2 = (q^+)^2 = 0$$

extension à $N > 1$ qubits

- N qubits : Hilbert $\mathcal{H}_{2^N}$ à 2^N dimensions

$$\mathcal{H}_{2^N} = \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2$$

avec une base orthonormée

$$\{|n_1 n_2 \cdots n_N\rangle = |n_1\rangle \otimes |n_2\rangle \otimes \cdots \otimes |n_N\rangle : n_i = 0, 1\}$$

- N opérateurs $\downarrow$: $\{q_1^-, q_2^-, \cdots, q_N^-\}$
- N opérateurs $\uparrow$: $\{q_1^+, q_2^+, \cdots, q_N^+\}$
- N opérateurs nombre : $\{K_1, K_2, \cdots, K_N\}$

$$(q_i^-)^\dagger = q_i^+, \;\; K_i^\dagger = K_i, \;\; [q_i^-, q_j^-] = [q_i^+, q_j^+] = 0$$

$$[q_i^-, q_j^+] = \delta_{i,j}(\mathbb{I} - 2K_i), \;\; [K_i, q_j^\pm] = \pm\delta_{i,j} q_i^\pm$$

extension à $N > 1$ qubits (suite)

- **définition**

$$q^- = \sum_{i=1}^{N} q_i^-, \quad q^+ = \sum_{i=1}^{N} q_i^+, \quad K = \sum_{i=1}^{N} K_i$$

- **conséquence**

$$(q^\pm)^k = k! \sum_{i_1<\cdots<i_k} q_{i_1}^\pm q_{i_2}^\pm \cdots q_{i_k}^\pm$$

donc pour $k = N$

$$(q^\pm)^N = N! q_1^\pm q_2^\pm \cdots q_N^\pm \;\Rightarrow\; (q^\pm)^{N+1} = 0$$

et pour $N = 1$ qubit on retrouve $(q^\pm)^2 = 0$

extension à $N > 1$ qubits (fin)

contact avec l'algèbre de Weyl et Heisenberg généralisée $\mathcal{A}_\kappa$

on vérifie que

(1) $$[q^-, q^+] = N\mathbb{I} - 2K, \quad [K, q^\pm] = \pm q^\pm$$

qui généralise le case $N = 1$; en posant

$$a^\pm = \frac{1}{\sqrt{N}} q^\pm$$

alors (1) donne

$$[a^-, a^+] = \mathbb{I} + 2\kappa K, \ [K, a^\pm] = \pm a^\pm, \ (a^-)^\dagger = a^+, \ K^\dagger = K$$

où $\kappa = -\frac{1}{N} \Rightarrow a^-$, a^+, K et $\mathbb{I}$ génèrent l'algèbre $\mathcal{A}_\kappa$

résumé

• l'algèbre $\mathcal{A}_\kappa$ peut être décrite par N qubits

• $\kappa = -\frac{1}{N} < 0 \Rightarrow$ l'algèbre $\mathcal{A}_\kappa$ admet des représentations de dimensions finies

• **les états de Dicke** (à définir ci-après) peuvent servir pour construire une représentation de dimension $d = N + 1$ de l'algèbre $\mathcal{A}_\kappa$

ÉTATS DE DICKE

• **l'espace $\mathcal{F}_{N,k}$**

l'espace de Hilbert $\mathcal{H}_{2^N}$ peut être partionné suivant

$$\mathcal{H}_{2^N} = \bigoplus_{k=0}^{N} \mathcal{F}_{N,k}$$

où $\mathcal{F}_{N,k}$ est engendré par l'ensemble orthonormal

$$\{|n_1 n_2 \cdots n_N\rangle \mid n_1 + n_2 + \cdots + n_N = k\}$$

chaque vecteur $|n_1 n_2 \cdots n_N\rangle$ de $\mathcal{F}_{N,k}$ contient $N-k$ qubits $|0\rangle$ et k qubits $|1\rangle$ and $\dim \mathcal{F}_{N,k} = C_N^k$

• **définition**

l'état de Dicke $|N;k\rangle$ est la superposition normalisée symétrique de tous les états de $\mathcal{F}_{N,k}$

$$|N;k\rangle = (C_N^k)^{-\frac{1}{2}} \sum_{|x\rangle \in \mathcal{F}_{N,k}} |x\rangle$$

- **cas** $N = 1$

$$|1;0\rangle = |0\rangle, \quad |1;1\rangle = |1\rangle$$

- **cas** $N = 2$

$$|2;0\rangle = |00\rangle, \quad |2;1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |2;2\rangle = |11\rangle$$

- **cas** $N = 3$

$$\begin{aligned} |3;0\rangle &= |000\rangle \\ |3;1\rangle &= \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \\ |3;2\rangle &= \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle) \\ |3;3\rangle &= |111\rangle \end{aligned}$$

• **cas** $N = 4$

on a les $d = N + 1 = 5$ états de Dicke

$$
\begin{aligned}
|4;0\rangle &= |0000\rangle \\
|4;1\rangle &= \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \\
|4;2\rangle &= \frac{1}{\sqrt{6}}(|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle) \\
|4;3\rangle &= \frac{1}{2}(|0111\rangle + |1011\rangle + |1101\rangle + |1110\rangle) \\
|4;4\rangle &= |1111\rangle
\end{aligned}
$$

où chaque vector $|4;k\rangle$ est une combinaison linéaire symétrique (par rapport au groupe S_4) des vecteurs de $\mathcal{F}_{4,k}$

l'espace $\mathcal{G}_d$ avec $d = N + 1$

noter que

$$\langle N; k|N; \ell\rangle = \delta_{k,\ell}, \quad k, \ell = 0, 1, \cdots, N$$

de sorte que l'ensemble

$$\{|N; k\rangle : k = 0, 1, \cdots, N\}$$

des $N + 1$ vecteurs symétriques $|N; k\rangle$ constitue un sous espace orthonormal de $\mathcal{H}_{2^N}$; soit $\mathcal{G}_d$ ce sous espace de dimension $d = N + 1$

états de Dicke et représentations de $\mathcal{A}_\kappa$

on montre que

$$\begin{aligned} q^+|N;k\rangle &= \sqrt{F(N,k+s+\frac{1}{2})}|N;k+1\rangle \\ q^-|N;k\rangle &= \sqrt{F(N,k+s-\frac{1}{2})}|N;k-1\rangle \\ K|N;k\rangle &= k|N;k\rangle \end{aligned}$$

où

$$s=\frac{1}{2}, \quad F(N,\ell)=\ell(N-\ell+1), \quad 0\leq\ell\leq N+1$$

avec pour cas limites

$$q^+|N;N\rangle = q^-|N;0\rangle = 0,\ K|N;N\rangle = N|N;N\rangle,\ K|N;0\rangle = 0$$

états de Dicke et représentations de $\mathcal{A}_\kappa$ (fin)

• **proposition 1**

l'ensemble

$$\{|N;k\rangle : k = 0, 1, \cdots, N\}$$

constitue une base pour une représentation de dimension $d = N + 1$ de l'algèbre de Weyl et Heisenberg $\mathcal{A}_\kappa$ avec $\kappa = -\frac{1}{N}$

• **cas limite**

pour $N \to \infty$, on retrouve les résultats familiers pour l'oscillateur harmonique

décomposition d'un état de Dicke

on montre que

$$|N;k\rangle = \sqrt{\frac{N-k}{N}}|N-1;k\rangle \otimes |0\rangle + \sqrt{\frac{k}{N}}|N-1;k-1\rangle \otimes |1\rangle$$

où $0 \leq k \leq N$

- $k \neq 0$ and $k \neq N$: 2 termes dans la décomposition de $|N;k\rangle$
- $k = 0$: $|N;0\rangle$ est un simple produit tensoriel

$$|N;0\rangle = |N-1;0\rangle \otimes |0\rangle = \cdots = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$$

- $k = N$: $|N;N\rangle$ est un simple produit tensoriel

$$|N;N\rangle = |N-1;N-1\rangle \otimes |1\rangle = \cdots = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle$$

au passage : états de Dicke et moment angulaire

• l'algèbre de Lie su(2) du groupe SU(2) en termes d'opérateurs de moment angulaire J_+, J_- and J_z est

$$[J_z, J_\pm] = \pm J_\pm, \quad [J_+, J_-] = 2J_z$$

• la représentation irréductible (j) de su(2) dans la base $\{|j,m) : m = -j, -j+1, \cdots, j\}$ est donnée par

$$\begin{aligned} J_+|j,m) &= \sqrt{(j-m)(j+m+1)}|j,m+1) \\ J_-|j,m) &= \sqrt{(j+m)(j-m+1)}|j,m-1) \\ J_z|j,m) &= m|j,m) \end{aligned}$$

• changement de notations

$$k = j - m, \quad N - k = j + m \quad \Leftrightarrow \quad j = \frac{N}{2}, \quad m = -k + \frac{N}{2}$$

d'où $-j \leq m \leq j \;\Leftrightarrow\; 0 \leq k \leq N \;\Rightarrow\; |j,m) \equiv |N;k\rangle$

états de Dicke et moment angulaire (suite)

- avec le changement de notation

$$\begin{aligned} J_+|N;k\rangle &= \sqrt{k(N-k+1)}|N;k-1\rangle \\ J_-|N;k\rangle &= \sqrt{(N-k)(k+1)}|N;k+1\rangle \\ J_z|N;k\rangle &= \left(\frac{N}{2}-k\right)|N;k\rangle \end{aligned}$$

- ce qui conduit à l'identification

$$J_+ = q^-, \quad J_- = q^+, \quad J_z = \frac{N}{2}\mathbb{I} - K$$

- d'où un lien entre su(2) et $\mathcal{A}_\kappa$ avec $\kappa = -\frac{1}{N}$

états de Dicke et moment angulaire (fin)

- corollaire

$$|j,m) = \sqrt{\frac{(j-m)!(j+m)!}{(2j)!}} \times$$

$$\sum_{\{\sigma\}} \sigma \left(\underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{j+m} \otimes \underbrace{|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle}_{j-m} \right)$$

- exemple typique

$$|1,1) = |0\rangle \otimes |0\rangle,\ |1,-1) = |1\rangle \otimes |1\rangle,\ |1,0) = \frac{1}{\sqrt{2}}\Big[|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle\Big]$$

correspond à la décomposition de Clebsch et Gordan

$$(\frac{1}{2}) \otimes (\frac{1}{2}) = (j=0) \oplus (j=1)$$

restreinte à la partie symétrique $(j=1)$

ÉTATS QUDITS SYMÉTRIQUES

factorisation d'un qudit

• **qudit dans $\mathcal{G}_d$**

l'état le plus général dans $\mathcal{G}_d$ peut être consideré comme un qudit $|\psi_d\rangle$ (système à d niveaux) constitué de $N = d - 1$ qubits ($|\psi_d\rangle$ est une superposition d'états $|N; k\rangle$)

$$|\psi_d\rangle = \sum_{k=0}^{N} c_k |N; k\rangle, \quad N = d - 1, \quad c_k \in \mathbb{C}$$

• **question**

sous quelle condition le vecteur $|\psi_d\rangle$ peut être factorisé suivant

$$|\psi_d\rangle = |\phi_{d-1}\rangle \otimes |\varphi_1\rangle$$

incluant un état $|\phi_{d-1}\rangle$ à $N - 1$ qubits un état $|\varphi_1\rangle$ à 1 qubit ?

factorisation d'un qudit (suite)

- **proposition 2 :** si le qudit

$$|\psi_d\rangle = \sum_{k=0}^{N} c_k |N;k\rangle, \qquad \sum_{k=0}^{N} |c_k|^2 = 1$$

est séparable, alors il est complètement séparable et s'écrit

$$|\psi_d\rangle = |z\rangle \otimes |z\rangle \otimes \cdots \otimes |z\rangle$$

où le vecteur

$$|z\rangle = \frac{1}{\sqrt{1+\bar{z}z}}(|0\rangle + z|1\rangle)$$

est un état cohérent de SU(2) et z satisfait les contraintes

$$(1+\bar{z}z)^{\frac{N}{2}} = \frac{1}{c_0}, \qquad z = \frac{c_{k+1}}{c_k}\sqrt{\frac{k+1}{N-k}}, \qquad k = 0, 1, \cdots, N-1$$

factorisation d'un qudit (exemple typique)

cas $d = 3 \Leftrightarrow N = 2$

$$|\psi_3\rangle = c_0|2;0\rangle + c_1|2;1\rangle + c_2|2;2\rangle, \quad |c_0|^2 + |c_1|^2 + |c_2|^2 = 1$$

où

$$|2;0\rangle = |00\rangle, \quad |2;1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |2;2\rangle = |11\rangle$$

si on introduit les contraintes de séparabilité

$$\frac{c_1}{c_0} = \sqrt{2}z, \quad \frac{c_2}{c_1} = \frac{1}{\sqrt{2}}z, \quad c_0 = \frac{1}{1+\bar{z}z}$$

on obtient

$$|\psi_3\rangle = \frac{1}{1+\bar{z}z}\left[|00\rangle + z(|01\rangle + |10\rangle) + z^2|11\rangle\right] = |z\rangle \otimes |z\rangle$$

N.B. : contraintes $\Rightarrow$ la concurrence $C = |c_1^2 - 2c_0c_2|$ est nulle

DESCRIPTION DE MAJORANA

description de Majorana (généralités)

retour au cas général où $|\psi_d\rangle$ est arbitraire ; l'état

$$|\psi_d\rangle = c_0|N;0\rangle + c_1|N;1\rangle + \cdots + c_N|N;N\rangle$$

étant symétrique sous le groupe S_N, on peut écrire

$$|\psi_d\rangle = \mathcal{N}_d \sum_{\sigma\in S_N} \sigma(|z_1\rangle \otimes |z_2\rangle \otimes \cdots \otimes |z_N\rangle)$$

en termes d'états cohérents de SU(2) ; relations entre

$$c_0, c_1, c_2, \cdots, c_N \quad \text{et} \quad \mathcal{N}_d, z_1, z_2, \cdots, z_N \ ?$$

le cas N arbitraire est compliqué ; suite avec $N = 2$

description de Majorana (exemple typique)

for $N = 2 \Leftrightarrow d = 3$, on doit comparer

$$\begin{aligned} |\psi_3\rangle &= c_0|2;0\rangle + c_1|2;1\rangle + c_2|2;2\rangle \\ &= c_0|00\rangle + \frac{1}{\sqrt{2}}c_1(|01\rangle + |10\rangle) + c_2|11\rangle \end{aligned}$$

avec

$$\begin{aligned} |\psi_3\rangle &= \mathcal{N}_3(|z_1\rangle \otimes |z_2\rangle + |z_2\rangle \otimes |z_1\rangle) \\ &= \mathcal{N}_3 \frac{1}{\sqrt{1+|z_1|^2}} \frac{1}{\sqrt{1+|z_2|^2}} \\ &\times \ [2|00\rangle + (z_1+z_2)(|01\rangle + |10\rangle) + 2z_1z_2|11\rangle] \end{aligned}$$

$\Rightarrow$ aux relations suivantes entre c_0, c_1, c_2 et $\mathcal{N}_3, z_1, z_2$

description de Majorana (exemple typique, suite)

$$\begin{aligned}
\frac{1}{2}c_0 &= \mathcal{N}_3 \frac{1}{\sqrt{1+|z_1|^2}} \frac{1}{\sqrt{1+|z_2|^2}} \\
\frac{1}{\sqrt{2}}c_1 &= \mathcal{N}_3 \frac{1}{\sqrt{1+|z_1|^2}} \frac{1}{\sqrt{1+|z_2|^2}} (z_1+z_2) \\
\frac{1}{2}c_2 &= \mathcal{N}_3 \frac{1}{\sqrt{1+|z_1|^2}} \frac{1}{\sqrt{1+|z_2|^2}} z_1 z_2
\end{aligned}$$

ainsi, z_1 and z_2 sont racines de l'équation

$$c_0 z^2 - \sqrt{2} c_1 z + c_2 = 0 \;\Rightarrow\; z = \frac{c_1 \pm \sqrt{c_1^2 - 2c_0 c_2}}{\sqrt{2} c_0}$$

N.B. : pour $c_1^2 - 2c_0 c_2 = 0$ (concurrence nulle), on a

$$|\psi_3\rangle = \frac{1}{1+\bar{z}z}\left[|00\rangle + z(|01\rangle + |10\rangle) + z^2|11\rangle\right] = |z\rangle \otimes |z\rangle$$

description de Majorana (cas général)

l'équivalence entre la représentation de Dicke

$$|\psi_d\rangle = c_0|N;0\rangle + c_1|N;1\rangle + \cdots + c_N|N;N\rangle$$

et celle de Majorana

$$|\psi_d\rangle = \mathcal{N}_d \sum_{\sigma\in S_N} \sigma(|z_1\rangle \otimes |z_2\rangle \otimes \cdots \otimes |z_N\rangle)$$

conduit à

$$c_k = N!N_1N_2\cdots N_N\mathcal{N}_d\sqrt{\frac{k!(N-k)!}{N!}}s_k(z_1z_2\cdots z_N)$$

$$N_i = \frac{1}{\sqrt{1+\bar{z}_iz_i}}, \quad |\mathcal{N}_d|^{-2} = N!\mathrm{perm}(A_N), \quad (A_N)_{ij} = \langle z_i|z_j\rangle$$

$$s_0(z_1z_2\cdots z_N) = 1, \quad s_k(z_1z_2\cdots z_N) = \sum_{1\le i_1<i_2<\cdots<i_k\le N} z_{i_1}z_{i_2}\cdots z_{i_k}$$

deux propositions (cas général)

proposition 3 : pour $c_0, c_1, \cdots, c_N$ fixés, les $z_1, z_2, \cdots, z_N$ sont racines de

$$\sum_{k=0}^{N} (-1)^k \sqrt{\frac{N!}{k!(N-k)!}} c_k z^{N-k} = 0$$

proposition 4 : le paramètre réel

$$P_d = \frac{1}{N!}\text{perm}(A_N), \quad (A_N)_{ij} = \langle z_i | z_j \rangle, \quad \frac{1}{2^{N-1}} \leq P_d \leq 1$$

caractérise l'intrication du qudit $|\psi_d\rangle$ avec $P_d = \frac{1}{2^{N-1}}$ pour un état maximalement intriqué et $P_d = 1$ pour un état séparable ; le paramètre P_d est appelé **perma-concurrence** de l'état $|\psi_d\rangle$

CARACTÉRISATION DE L'INTRICATION

exemples d'états symétriques à $N = 2, 3, 4$ qubits

exemple

pour $N = 2 \Leftrightarrow d = 3$, on a

$$\begin{aligned} |\psi_3\rangle &= c_0|00\rangle + c_1\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) + c_2|11\rangle \\ &= \mathcal{N}_3(|z_1\rangle \otimes |z_2\rangle + |z_2\rangle \otimes |z_1\rangle) \end{aligned}$$

$$c_0 z^2 - \sqrt{2}c_1 z + c_2 = 0 \;\Rightarrow\; z_1, z_2 = \frac{c_1 \pm \sqrt{c_1^2 - 2c_0c_2}}{\sqrt{2}c_0}$$

la formule pour P_d donne

$$P_3 = \frac{1}{2!}\text{perm}(A_2) = \frac{1}{2}\text{perm}\begin{pmatrix} \langle z_1|z_1\rangle & \langle z_1|z_2\rangle \\ \langle z_2|z_1\rangle & \langle z_2|z_2\rangle \end{pmatrix}$$

$$P_3 = \frac{1}{2}(1 + |\langle z_1|z_2\rangle|^2) = \frac{1}{1+C}$$

séparable : $C = 0 \Leftrightarrow P_3 = 1$, **maximalement intriqué :** $C = 1 \Leftrightarrow P_3 = \frac{1}{2}$

exemples d'états maximalement intriqués

- pour les 3 états de Bell

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

on obtient $P_3 = \frac{1}{2}$

- pour l'état

$$|\psi_4\rangle \equiv |\phi\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$$

et l'état de Greenberger, Horne et Zeilinger

$$|\psi_4\rangle \equiv |\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

on obtient $P_4 = \frac{1}{4}$

- pour l'état $|\psi_5\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ on obtient $P_5 = \frac{1}{8}$

exemples d'états à 3 qubits ($\frac{1}{4} \leq P_4 < 1$)

- $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(000 + 111)$: $P_4 = 0.25$
- $|\phi\rangle = \frac{1}{2}(000 + 011 + 101 + 110)$: $P_4 = 0.25$
- $|\psi\rangle = \frac{1}{2}(001 + 010 + 100 + 111)$: $P_4 = 0.25$
- $|\rho\rangle = \frac{1}{\sqrt{8}}(000 + 001 + 010 + 100 - 011 - 101 - 110 + 111)$: $P_4 = \frac{4\sqrt[3]{2}}{6+4\sqrt[3]{2}+3\sqrt[3]{4}} \approx 0.32$
- $|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(001 + 010 + 100)$: $P_4 = \frac{1}{3}$
- $|\chi\rangle = \frac{1}{2}(000 + 001 + 010 + 100)$: $P_4 = 0.4$

CONCLUSIONS

• **résultat**

- introduction d'un paramètre P_d, appelé **perma-concurrence**, pour caractériser le degré d'intrication d'un qudit $|\psi_d\rangle$ construit à partir d'une assemblée de $N = d - 1$ qubits

- la perma-concurrence P_d généralise au cas $N > 2$ la concurrence de Wootters qui s'applique au cas d'un état à $N = 2$ qubits arbitraire

• **extension difficile**

difficile d'étendre ce travail à des états à N qubits anti-symétriques, et plus généralement, à des états à N qubits se transformant comme une représentation irreductible du groupe symétrique S_N

nombreuses références dans les articles suivants :

en accès libre :

• Generalized Weyl-Heisenberg Algebra, Qudit Systems and Entanglement Measure of Symmetric States via Spin Coherent States, dans : Entropy 2018, 20(4), 292 (Special Issue : Entropy and Information in the Foundation of Quantum Physics)

`https://www.mdpi.com/1099-4300/20/4/292`

• Generalized Weyl-Heisenberg Algebra, Qudit Systems and Entanglement Measure of Symmetric States via Spin Coherent States. Part II : The Perma-Concurrence Parameter, dans : Symmetry 2019, 11(7), 875

`https://www.mdpi.com/2073-8994/11/7/875`

MERCI POUR VOTRE ATTENTION

DÉBUT DES ANNEXES SUR LA PARTIE 1

ANNEXE 1

DÉMONSTRATION DE LA PROPOSTION $\mathbb{C}^d - \mathbb{C}^{d^2}$

démo de la proposition

• si on connaît d+1 MUBs càd les $|a\alpha\rangle \in \mathbb{C}^d$ satisfaisant $|\langle a\alpha|b\beta\rangle| = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{\sqrt{d}}(1-\delta_{a,b}) \Rightarrow$ les $\Pi_{a\alpha} = |a\alpha\rangle\langle a\alpha|$ sont connus $\Rightarrow$ les matrices $\Pi_{a\alpha} = \sum_{pq} w_{pq}(a\alpha)E_{pq}$ (avec $\Pi_{a\alpha}$ matrice $d \times d$ de rang 1 et d'éléments $w_{pq}(a\alpha) \in \mathbb{C}$) sont connues $\Rightarrow$ les vecteurs $w(a\alpha) \in \mathbb{C}^{d^2}$ de composantes $w_{pq}(a\alpha) = \langle p|a\alpha\rangle\overline{\langle q|a\alpha\rangle}$ sont connus et

$$\mathrm{tr}(\Pi_{a\alpha}^{\dagger}\Pi_{b\beta}) = |\langle a\alpha|b\beta\rangle|^2 \;\Rightarrow\; w(a\alpha)\cdot w(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b})$$

• si on connaît les $w(a\alpha) \in \mathbb{C}^{d^2}$ satisfaisant $w(a\alpha)\cdot w(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b})$ avec $w_{pq}(a\alpha) = \langle p|a\alpha\rangle\overline{\langle q|a\alpha\rangle} \Rightarrow$ les matrices $\sum_{pq} w_{pq}(a\alpha)E_{pq}$ sont connues et toute colonne de la matrice $\sum_{pq} w_{pq}(a\alpha)E_{pq}$ donne le vecteur $|a\alpha\rangle \in \mathbb{C}^d$ à une constante multiplicative près

ANNEXE 2

LE PROBLÈME DU ROI MÉCHANT

annexe : problème du roi méchant (1)

• the king invites the physicist to prepare a certain silver atom in any state

• the king's men then measure one of the three cartesian spin components of this atom - they either measure σ_x, σ_y or σ_z without telling the physicist which one of the measurements is actually done

• then it is again the physicist's turn, and she can perform any experiment of her choosing

• only after she's finished, the king will tell her which spin component had been measured by his men

• to save her neck, the physicist must then state correctly the measurement result that the king's men had obtained

annexe : problème du roi méchant (2)

en d'autres mots :

- on mesure σ_x ou σ_y or σ_z pour une particule de spin 1/2 au temps t

- comment procéder pour qu'à l'aide de mesures faites avant t et après t, on puisse affirmer : si σ (σ_x ou σ_y or σ_z) a été mesuré, alors on a obtenu "tel résultat" ("haut" ou "bas")

ANNEXE 3

ÉIÉMENTS DE BASE À PROPOS DE

L'ORDINATEUR QUANTIQUE

des bits aux qubits

loi de Moore $\Rightarrow$ 10 nm en 2020

$\Rightarrow$ en faveur de l'ordinateur quantique où les **bits** 0 et 1 sont remplacés par des quantum bits ou **qubits**

$$|\phi\rangle = c_0|0\rangle + c_1|1\rangle, \quad c_0 \in \mathbb{C}, \quad c_1 \in \mathbb{C}, \quad |c_0|^2 + |c_1|^2 = 1$$

et même par des **qudits**

$$|\phi\rangle = \sum_{k=1}^{d-1} c_k|k\rangle, \quad c_k \in \mathbb{C}, \quad k = 0, 1, \cdots, d-1, \quad \sum_{k=1}^{d-1} |c_k|^2 = 1$$

réalisation des qubits

- particules de spin $\frac{1}{2}$ (RMN)
- systèmes électroniques à deux niveaux
- systèmes vibrationnels à 1 et 2 phonons
- états de polarisation d'un photon
- électrodynamique quantique en cavité
- etc.

de façon schématique

ordinateur quantique :

ensemble de qubits dont l'état est contrôlé et manipulé à travers des **transformations unitaires** réalisées par des **portes quantiques**

la mesure de qubits issus d'un circuit de portes quantiques donne le résultat d'un calcul quantique

information quantique et calcul quantique

au carrefour de :

- physique quantique
- mathématique
- informatique

pourquoi physique quantique ?

points forts :

• superposition $\Rightarrow$ parallèlisme quantique massif (algorithmes de Shor, de Grover, etc.) : avec n qubits $\Rightarrow$ 2^n calculs en une seule opération

• intrication $\Rightarrow$ téléportation quantique et calcul quantique

• toute mesure perturbe $\Rightarrow$ cryptographie quantique

points faibles :

• linéarité et superposition $\Rightarrow$ impossibilité de cloner un état

• problème de décohérence $\Rightarrow$ nécessité de codes correcteurs quantiques

pourquoi mathématique ?

- théorie des nombres
- géométrie finie (géométrie projective)
- corps et anneaux finis
- analyse combinatoire
- théorie des graphes
- théorie des groupes finis
- théorie des groupes de Lie

FIN DES ANNEXES SUR LA PARTIE 1