Théorie classique des invariants et information quantique

Jean-Gabriel Luque*

D'après des travaux réalisés en collaboration avec Emmanuel Briand[1] et Jean-Yves Thibon[2].

Résumé

Nous donnons une application de la théorie classique des invariants à l'étude de l'intrication en information quantique.

1 Introduction

La théorie des invariants des hypermatrices consiste en l'étude du problème suivant: étant donné un ensemble fini d'espaces vectoriels $V_1, V_2, \cdots, V_k$, étudier les orbites du groupe $G = GL(V_1) \otimes \cdots \otimes GL(V_k)$ dans l'espace $\mathcal{V} = V_1 \otimes \cdots \otimes V_k$. Les hypermatrices sont simplement des éléments de l'espace $\mathcal{V}$. Nous ne traiterons ici que le cas où $V_1 = \cdots = V_k = \mathbb{C}^2$. Le problème de classification des hypermatrices n'est résolu que dans quelques rares cas. Il a été étudié dans le cadre de la théorie classique des invariants. Par exemple, le cas de trois espaces de dimension 2 a été résolu complètement par Le Paige en 1881 [30]. Récemment, le sujet est redevenu à la mode à cause de ses implications en information quantique [2, 3, 19, 27]. Plus précisément, cette classification devrait servir à définir les états intriqués et à construire des mesures d'intrications. Dans cet article, nous brossons un rapide tableau des interconnections entre les deux disciplines en donnant pour exemple les calculs des covariants des systèmes de 3 et 4-qubits.

*Jean-Gabriel.Luque@univ-mlv.fr
[1]Emmanuel.Briand@univ-mlv.fr
[2]Jean-Yves.Thibon@univ-mlv.fr

2 Prérequis sur les fonctions symétriques

Dans cette section, nous donnons une liste de définitions et propriétés des fonctions symétriques que nous utiliserons pour calculer des dimensions d'espaces de covariants. Nous ne rentrerons pas dans le détail de la justification des définitions ni dans celui des preuves. Pour plus d'information, nous invitons le lecteur à consulter le livre de Macdonald [25].
Considérons un alphabet ordonné $X = \{x_1 < x_2 < \cdots < x_n, \cdots\}$. Nous utiliserons essentiellement trois familles de fonctions symétriques.

1. Les fonctions élémentaires

$$e_n = \sum_{y_1 < \cdots < y_n \in X} y_1 \cdots y_n \tag{1}$$

dont la série génératrice est

$$E_X(t) = \sum_{i \geq 0} e_i t^i = \prod_{x \in X} (1 + xt). \tag{2}$$

Remarquons que lorsque $X = \{x_1 \leq \cdots \leq x_n\}$ est fini, la série génératrice est un polynôme dont $\{-\frac{1}{x_1}, \cdots, -\frac{1}{x_n}\}$ est l'ensemble des racines.

2. Les fonctions complètes

$$h_n = \sum_{y_1 \leq \cdots \leq y_n \in X} y_1 \cdots y_n. \tag{3}$$

de série génératrice

$$\sigma_1(X) = \sum_{r \geq 0} h_r t^r = \prod_{x \in X} (1 - x_i t)^{-1} \tag{4}$$

3. Les fonctions de Schur s_λ, indexées par des partitions,

$$s_\lambda = \det(h_{\lambda_i - i + j})_{1 \leq i,j \leq n} \tag{5}$$

où $\lambda = (\lambda_1 \geq \cdots \geq \lambda_n)$. Les fonctions de Schur ont un grand intérêt en théorie des représentations. En particulier, ce sont les caractères des représentations polynomiales irréductibles de $GL(\mathbb{C}^p)$ [25, 6]. Nous verrons dans la section suivante comment cela va nous permettre de calculer la dimension des algèbres de covariants.

L'algèbre des fonctions symétriques, notée Sym, est munie d'un produit scalaire $\langle\, ,\, \rangle_{Sym}$ tel que les fonctions de Schur forment une base orthonormale. On peut définir naturellement un produit scalaire $\langle\, ,\, \rangle_{Sym^{\otimes k}}$ sur $Sym^{\otimes k}$. L'algèbre Sym possède un coproduit $\delta(f(X))$ défini par

$$\delta h_k = \sum_{|\lambda|=k} s_\lambda \otimes s_\lambda \tag{6}$$

où $|\lambda| = \lambda_1 + \cdots + \lambda_n$ si $\lambda = (\lambda_1 \geq \cdots \geq \lambda_n)$. Le produit intérieur est l'unique produit $*$ vérifiant

$$\langle f, g_1 * g_2 \rangle_{Sym} = \langle \delta(f), g_1 \otimes g_2 \rangle_{Sym^{\otimes 2}} \tag{7}$$

Le plethysme ou la composition $f[g]$ de f par g se définit de la façon suivante: on écrit la fonction g comme la somme

$$g = \sum_\alpha u_\lambda x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

alors $f[g] = f(Y)$ où l'alphabet Y vérifie

$$E_Y(t) = \prod_\alpha (1 + x_1^{\alpha_1} \cdots x_n^{\alpha_n} t)^{u_\alpha}.$$

Autrement dit, l'alphabet Y est formé des monômes de g répétés avec leur multiplicités.
Par exemple si on pose $g = p_n = \sum x_i^n$, $f[g] = f(x_1^n, \cdots, x_k^n, \cdots)$.

3 Invariants et covariants des formes multilinéaires

Les concomitants des formes multilinéaires ou des hypermatrices, ont fait l'objet de nombreux travaux jusque dans les années 40. Nous donnons dans la bibliographie une liste d'articles et d'ouvrages dans lesquels sont décrits avec détail les calculs et les résultats résumés dans cette section [5, 7, 8, 9, 15, 16, 18, 26, 31, 32, 33, 34, 36, 40, 41, 42, 43, 44]. Nous brosserons, ici, un (trés) rapide tour d'horizon des outils de la théorie des invariants classiques que nous appliquerons dans un second temps à la description des états intriqués.

3.1 Algèbre des covariants polynomiaux

Les hypermatrices sont simplement des tableaux dont les éléments sont indéxés par plus de deux indices. Plus formellement, il s'agit des éléments de l'espace $V_1 \otimes \cdots \otimes V_k$, où $V_1, \cdots, V_k$ sont des espaces vectoriels. L'entier k est le nombre d'indices de l'hypermatrice et chacun des indices est pris entre 1 et la dimension de l'espace V_i correspondant. Dans notre cas, très particulier, on a $V = V_1 = \cdots = V_k = \mathbb{C}^p$ (nous ferons le tous le raisonnement de ce paragraphe dans le cas où p est un entier quelconque, mais dans les paragraphes suivants nous poserons $p = 2$).
Considérons, donc, une hypermatrice $A \in V^{\otimes k}$. On définit la *forme fondamentale* comme étant le polynôme multilinéaire

$$A(\mathbf{x}_1, \cdots, \mathbf{x}_k) = \sum_{i_1, \cdots, i_k} A_{i_1 \cdots i_k} x_1^{i_1} \cdots x_k^{i_k} \tag{8}$$

où $\mathbf{x}_i = (x_i^1, \cdots, x_i^p)$. Nous allons nous interesser à l'action du groupe

$$G = GL(\mathbb{C}^p) \otimes \cdots \otimes GL(\mathbb{C}^p) \tag{9}$$

Un invariant relatif de degré d et de poids $\omega = (\omega_1, \cdots, \omega_k)$ est un polynôme $F \in \mathcal{R}_d = S^d(V)^{\otimes k}$ en les entrées de l'hypermatrice tel que pour tout $g = (g_1, \cdots, g_k) \in G$, on ait

$$F(g \cdot A) = \det(g_1)^{\omega_1} \cdots \det(g_k)^{\omega_k} F(A)$$

L'exemple le plus simple d'invariant est le déterminant des matrices usuelles. On peut étendre cette définition de façon naturelle aux hypermatrices ayant un nombre pair d'indices [37, 23]

$$\mathrm{DET}(M) = \frac{1}{p!} \sum_{\sigma_1, \cdots, \sigma_{2k} \in \mathfrak{S}_p} \epsilon(\sigma_1 \cdots \sigma_{2k}) \prod_{i=1}^{p} M_{\sigma_1(i) \cdots \sigma_{2k}(i)}, \tag{10}$$

Nous laissons au lecteur le soin de vérifier qu'il s'agit aussi d'un invariant.
Un covariant de degré $d = (d_0, d_1, \cdots, d_k)$ est un invariant relatif de G dans $\mathcal{R}_d = S^{d_0}(V^{\otimes k}) \otimes S^{d_1}(V^*) \otimes \cdots \otimes S^{d_k}(V^*)$. On notera $Inv(d, \omega)$ l'algèbre des invariants de degré d et de poids ω et $Cov(d, \omega)$ celle des covariants. L'exemple le plus simple de covariant est la forme fondamentale.
Nous avons vu que les fonctions de Schur spécialisées à l'alphabet $\{x_1, \cdots, x_p\}$ sont les caractères des représentations polynomiales irréductibles de $GL(\mathbb{C}^p)$. Les représentations irréductibles de G ont donc pour caractère des produits de fonctions de Schur $S_\lambda = s_{\lambda^1}(X_1) \cdots s_{\lambda^k}(X_k)$ où les λ^i sont des partitions

et les X_i des alphabets finis. Dans notre cas particulier, la représentation à une dimension

$$\det(g)^{\omega} = \det(g_1)^{\omega_1} \cdots \det(g_k)^{\omega_k}$$

a pour caractère un produit de fonctions de Schur rectangulaires

$$s_{(\omega_1^p)}(X_1) s_{(\omega_2^p)}(X_2) \cdots s_{(\omega_k^p)}(X_k) \tag{11}$$

Le caractère de la représentation de G dans $\mathcal{V}$ est $h_d(X_1 \cdots X_k)$ où les X_i sont des alphabets de p lettres. La dimension de l'espace des invariants peut donc être obtenue par le produit scalaire

$$\dim \mathrm{Inv}(d, \omega) = \langle h_d(X_1 X_2 \cdots X_k)\,,\; s_{(\omega_1^p)}(X_1) s_{(\omega_2^p)}(X_2) \cdots s_{(\omega_k^p)}(X_k) \rangle_G \tag{12}$$

En identifiant le produit sur différents alphabets à un produit tensoriel, cette égalité peut être réécrite de la façon suivante

$$\begin{aligned} \dim \mathrm{Inv}(d, \omega) \;&= \langle \delta^k(h_d), s_{(\omega_1^p)} \otimes \cdots \otimes s_{(\omega_k^p)} \rangle_{Sym^{\otimes k}} \\ &= \langle h_d, s_{(\omega_1^p)} * \cdots * s_{(\omega_k^p)} \rangle_{Sym}\,. \end{aligned} \tag{13}$$

où δ est le coproduit de Sym et $*$ le produit intérieur des fonctions symétriques. Si les fonctions ne sont pas toutes du même degré, le produit intérieur est nul. Ceci implique

$$\omega_1 = \omega_2 = \cdots = \omega_k = d. \tag{14}$$

De la même façon, on obtient

$$\begin{aligned} \dim \mathrm{Cov}(d; \omega) \;&= \langle h_{d_0}(X_1 X_2 \cdots X_k)\,,\; (s_{(\omega_1^p)} h_{d_1})(X_1) \cdots (s_{(\omega_k^p)} h_{d_k})(X_1) \rangle_G \\ &= \langle h_{d_0}\,,\; (s_{(\omega_1^p)} h_{d_1}) * \cdots * (s_{(\omega_k^p)} h_{d_k}) \rangle_{Sym}\,. \end{aligned} \tag{15}$$

3.2 Transvectants

Le calcul des transvectants est basé sur l'utilisation des opérateurs Ω de Cayley. Il s'agit de l'outil fondamental pour la construction de systèmes complets de covariants. Il a été, notamment, utilisé par Gordan et Hilbert, afin de prouver que les anneaux de covariants sont finiment engendrés. Cette notion, initialement définie pour les formes binaires, s'étend naturellement à plusieurs variables.
L'opérateur Ω de Cayley est

$$\Omega_{\mathbf{xy}} = \begin{vmatrix} \frac{\partial}{\partial x_1} & \frac{\partial}{\partial y_1} \\ \frac{\partial}{\partial x_2} & \frac{\partial}{\partial y_2} \end{vmatrix} \tag{16}$$

Nous noterons $\mathbf{x} = (x_1, x_2)$. Le produit de deux formes $f(\mathbf{x})$ et $g(\mathbf{y})$, peut être identifié au produit tensoriel $f(\mathbf{x}) \otimes g(\mathbf{x})$. Si nous définissons l'application trace tr : $f \otimes g \to fg$, nous pouvons alors écrire $\mathrm{tr}(f(\mathbf{x})g(\mathbf{y})) = f(\mathbf{x})g(\mathbf{x})$. Si f et g sont deux fonctions de k variables binaires $\mathbf{x}^i$ ($i = 1 \cdots k$), on définit pour tout k-uplet $(i_1, \cdots, i_k) \in \mathbb{N}^k$ le transvectant multiple de f par g:

$$(f, g)^{i_1 i_2 \dots i_p} = \mathrm{tr}\, \Omega^{i_1}_{\mathbf{x}^1\mathbf{y}^1} \Omega^{i_2}_{\mathbf{x}^2\mathbf{y}^2} \cdots \Omega^{i_k}_{\mathbf{x}^k\mathbf{y}^k} f(\mathbf{x}^1, \dots, \mathbf{x}^k) g(\mathbf{y}^1, \dots, \mathbf{y}^k)\,, \qquad (17)$$

On peut montrer que l'on peut construire un système complet de covariants en appliquant un nombre fini de fois la transvection à partir de la forme fondamentale. C'est le principe de l'algorithme de Gordan adapté aux formes binaires multilinéaires [42]. Pour des raisons pratiques de programmation, nous avons choisi d'utiliser plutôt la méthode de Peano [33] qui consiste à fabriquer les covariants de degrés d en utilisant des transvectants du type $(A, C_{d-1})^{i_1, \dots, i_k}$ où C_{d-1} est un covariant de degré $d-1$ en les éléments de l'hypermatrice. Dans le cas des formes multilinéaires, on peut, en plus se restreindre aux C_{d-1} irréductibles (qui n'est pas une combinaison algébrique de covariants de degrés inférieurs).

4 Intrication des qubits

4.1 Élements de mécanique quantique

Le plus simple des systèmes de la mécanique quantique est celui de la particule libre de spin $\frac{1}{2}$ (un éléctron par exemple), il va illustrer nos propos tout au long de ce paragraphe. La notion de spin est née de l'interprétation, en 1925 par Uhlenbeck et Goudsmitt, d'une expérience de Stern et Gerlach, consistant à projeter sur un écran un jet d'atomes de Lithium en le faisant passer dans l'entrefer d'un électro-aimant, obtenant alors deux raies. Les deux raies ont révélé l'existence d'une "sorte de" moment cinétique pour les particules: le spin. Ce moment cinétique $\overrightarrow{S}$ est soumis aux règles de quantifications suivantes

$$|\overrightarrow{S}|^2 = s(s+1)\hbar^2 \qquad (18)$$

$$S_Z = m_S \hbar \qquad (19)$$

où S_Z représente la projection de $\overrightarrow{S}$ suivant une direction arbitraire, s est le spin de la particule c'est un demi-entier positif (ici il vaut $\frac{1}{2}$), m_s est un demi-entier (positif ou négatif) vérifiant $|m_s| \leq s$. Donc, m_s admet deux valeurs possibles $-\frac{1}{2}$ et $\frac{1}{2}$ expliquant respectivement la raie du bas $|\downarrow\rangle$ et la raie du haut $|\uparrow\rangle$.

On peut noter que les photons sont des particules de spin 1 et donc m_s peut posséder 3 valeurs (on appelle cela des qtrits).
Avant d'être mesuré notre système (composé d'une particule de spin $\frac{1}{2}$) est dans une superposition d'états.

$$|\phi\rangle = \alpha|\downarrow\rangle + \beta|\uparrow\rangle \tag{20}$$

avec $\alpha, \beta \in \mathbb{C}$. Une telle superposition d'états s'appelle un qubit et par analogie avec l'informatique nous noterons $|\downarrow\rangle = |0\rangle$ et $|\uparrow\rangle = |1\rangle$. Dès lors, on peut raisonner mathématiquement en n'oubliant l'aspect quantique (pour plus de précision sur ces propriétés classiques nous invitons le lecteur à consulter un des nombreux ouvrages sur le sujet comme [20]). En effet, $|\phi\rangle$ appartient à un $\mathbb{C}$-espace vectoriel de dimension 2 et en choisissant convenablement les bases, nous pouvons assimiler les états quantiques du système à des vecteurs de $\mathbb{C}^2$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{21}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{22}$$

$$|\phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{23}$$

4.2 Le paradoxe EPR et intrication des 2-qubits

Le raisonnement précédent est valable pour des systèmes constitués de deux particules. Dans ce cas, le système possède quatre états de base $||0\rangle\rangle = |00\rangle = |0\rangle\otimes|0\rangle$, $||1\rangle\rangle = |01\rangle = |0\rangle\otimes|1\rangle$, $||2\rangle\rangle = |10\rangle = |1\rangle\otimes|0\rangle$, $||3\rangle\rangle = |11\rangle = |1\rangle\otimes|1\rangle$.
Et les superpositions d'états sont de la forme

$$|\phi\rangle = a_0||0\rangle\rangle + a_1||1\rangle\rangle + a_2||2\rangle\rangle + a_3||3\rangle\rangle. \tag{24}$$

On appelle ces objets des 2-qubits et ils appartiennent donc à un $\mathbb{C}$-espace vectoriel de dimension 4 assimilable à l'espace des $\mathbb{C}$-matrices 2×2,

$$||0\rangle\rangle = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \tag{25}$$

$$||1\rangle\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{26}$$

$$||2\rangle\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{27}$$

$$||3\rangle\rangle = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \tag{28}$$

$$|\phi\rangle = \begin{pmatrix} a_0 + a_1 & a_0 + a_2 \\ a_2 + a_3 & a_1 + a_4 \end{pmatrix} \tag{29}$$

Quelle interprétation physique peut-on alors donner aux superpositions d'états? Par exemple, nous pouvons factoriser le 2-qubit

$$\begin{aligned} |\phi\rangle = \quad & \alpha_1\alpha_2||0\rangle\rangle + \alpha_1\beta_2||1\rangle\rangle + \alpha_2\beta_1||2\rangle\rangle + \alpha_2\beta_2||3\rangle\rangle \\ & = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle + \alpha_2\beta_2|11\rangle \\ = \quad & (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \end{aligned} \tag{30}$$

On peut alors en donner une interprétation simple: une des particules est dans l'état $\alpha_1|0\rangle + \beta_1|1\rangle$ l'autre dans $\alpha_2|0\rangle + \beta_2|1\rangle$.
Mais il existe des états non-factorisables comme $|W\rangle = |00\rangle + |11\rangle$. Quelle interprétation en donner? Et, tout d'abord, existent-ils dans la nature?
Ce sont les questions qui sont au centre du paradoxe d'Einstein-Podolsky-Rosen (EPR). Ces trois physiciens proposèrent en 1935, un modèle théorique prévoyant la non-localité de l'information comme un phénomène physique implémentable. La plupart des expériences utilisent des lasers et donc concernent des photons (de spin 1) mais la grandeur intéressante n'est pas ici le spin mais la polarisation du faisceau. Le principe est le suivant, un atome émet deux photons de polarisations orthogonales dans deux directions opposées, les photons sont récupérés dans 4 capteurs (un par direction et par polarisation). On obtient donc une superposition d'états, et le fait de mesurer l'état de l'un des photons donne automatiquement et immédiatement l'état de l'autre (même s'ils sont séparés par une très grande distance). Mais cela ne permet pas encore de conclure sur la non-localité de l'information, en effet on pourrait imaginer que la mesure déclenche un échange d'informations via l'émission de particules messagères. Ce sont les inégalités de Bell (très délicates à tester expérimentalement) qui permettent d'éliminer cette éventualité. Les

premières experiences ont eu lieu à la fin des années 70 et la plus célébre d'entre elles est sans doute celle d'Alain Aspect (lire [1] pour des informations plus précises sur le tests des inégalités de Bell et dans [14] le lecteur pourra trouver de la documentation sur l'information quantique).
Oublions à nouveau l'aspect physique du problème. Nous avons alors deux types d'états: factorisables et non-factorisables (ou intriqués). Existe-t-il un moyen de les discriminer?
Dans le cas des 2 qubits, la réponse est assez simple, il suffit d'utiliser l'interprétation matricielle et de constater que l'intrication est équivalente à la non-nullité du déterminant de la matrice $|\phi\rangle$ (le calcul est laissé au soin du lecteur).
Rien n'empêche, du moins théoriquement, d'imaginer que l'on construit des k-qubits. Dans ce cas, la notion intrication n'est pas aussi claire. Dans les deux paragraphes suivants nous allons étudier les cas $k = 3$ et $k = 4$.

4.3 Intrication des 3-qubits

Considérons maintenant l'espace des 3-qubits. C'est à dire, les états de la forme

$$|\phi\rangle = a_0||0\rangle\rangle+a_1||1\rangle\rangle+a_2||2\rangle\rangle+a_3||3\rangle\rangle+a_4||4\rangle\rangle+a_5||5\rangle\rangle+a_6||6\rangle\rangle+a_7||7\rangle\rangle \quad (31)$$

où les a_i sont des nombres complexes et $||n\rangle\rangle = |n_2n_1n_0\rangle = |n_2\rangle \otimes |n_1\rangle \otimes |n_0\rangle$ avec $n = 4n_2 + 2n_1 + n_0$. Les états sont des hypermatrices "cubiques" à 3 indices et de dimension 2.
Peut-on étendre la notion d'intrication aux 3-qubits? On peut assez facilement lister quelques ensembles d'états qui correspondraient à des niveaux d'intrication différents.

1. Les états complètements factorisés

$$(a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \otimes (c_0|0\rangle + c_1|1\rangle) \quad (32)$$

2. Les états partiellement factorisés

$$(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \quad (33)$$

3. Les états non-factorisables

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad (34)$$

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \quad (35)$$

La classification que nous venons de donner est naïve et ne prend pas en compte la géométrie des hypermatrices. La stratégie utilisée pour les 2-qubits consiste à évaluer le déterminant. Nous allons, dans un premier temps, appliquer la même méthode au cas présent, en nous basant sur la définition des états intriqués, donnée par Klyachko [19] comme étant des états n'annulant pas au moins un des invariants.
Il n'y a qu'un seul invariant pour les hypermatrices à trois indices de dimension 2: l'hyperdéterminant de Cayley [4, 12]

$$\begin{aligned}\Delta = \; & (a_0^2a_7^2 + a_1^2a_6^2 + a_2^2a_5^2 + a_3^2a_4^2) - 2(a_0a_1a_6a_7 + a_0a_2a_5a_7 + a_0a_3a_4a_7) \\ & -2(a_1a_2a_5a_6 + a_1a_3a_6a_4 + a_2a_3a_5a_4) + 4(a_0a_3a_5a_6 + a_1a_2a_4a_7)\end{aligned} \tag{36}$$

On peut remarquer que $\Delta(|GHZ\rangle) \neq 0$ par contre $\Delta(|W\rangle) = 0$. Donc, les états $|GHZ\rangle$ et $|W\rangle$ ne sont pas intriqués de la même façon et l'invariant Δ ne permet pas de discriminer entre les états du "type" de $|W\rangle$ et les états factorisés, ni entre les cas 1 et 2.
En fait, de façon générale la connaissance des invariants ne suffit pas pour établir une classification des orbites du groupe G, il faut connaître l'algèbre des concomitants qui dans le cas des formes binaires est égale à celle des covariants.
Nous allons calculer une base de cette algèbre en utilisant les transvectants. Un outils qui permet de guider les calculs est la connaissance de la série de Hilbert de l'algèbre. Notons la

$$C(t;\mathbf{u};\mathbf{v}) = \sum_{d,\,\omega} \dim \mathrm{Cov}(d,\omega) t^{d_0} u_1^{d_1} u_2^{d_2} u_3^{d_3} v_1^{\omega_1} v_2^{\omega_2} v_3^{\omega_3} \tag{37}$$

L'identité (15) permet d'en donner une expression comme un produit scalaire sur les fonctions symétriques

$$C(t;\mathbf{u};\mathbf{v}) = \langle \sigma_1[tu_1s_1 + t^2v_1s_{11}]\,,\, \sigma_1[u_2s_1 + v_2s_{11}] * \sigma_1[u_3s_1 + v_3s_{11}]\rangle \tag{38}$$

Or sur deux variables on a

$$\sigma_1[vs_{11}] = \sum_{l\geq 0} v^l s_{ll} \tag{39}$$

et

$$\sigma_1[us_1 + vs_{11}] = \sum_{\ell(\lambda)\leq 2} u^{\lambda_1-\lambda_2} v^{\lambda_2} s_\lambda(X)\,. \tag{40}$$

Cette somme peut être écrite en utilisant l'opérateur[3] $\Omega_{\geq}^{\mathbf{u}}$ de MacMahon

$$\sum_{\lambda_1\in\mathbb{Z}\;,\lambda_2\geq 0} t^{|\lambda|} u^{\lambda_1-\lambda_2} v^{\lambda_2} s_\lambda(X) = \left(1 - \frac{v}{u^2}\right)\sigma_t\left[\left(u + \frac{v}{u}\right)X\right]\,. \tag{41}$$

[3] Ne pas confondre avec l'opérateur Ω de Cayley vu plus haut.

D'où

$$C(t;\mathbf{u};\mathbf{v}) = \Omega^{\mathbf{u}}_{\geq} \prod_{i=1}^{3}\left(1-\frac{v_i}{u_i^2}\right)\sigma_t\left[\prod_{i=1}^{3}\left(u_i+\frac{v_i}{u_i}\right)\right]. \qquad (42)$$

où $\Omega^{u}_{\geq}$ désigne l'opérateur (linéaire) de MacMahon qui envoie chaque monôme contenant une puissance négative de u sur 0. En décomposant en fractions élémentaires pour chacun des u_i et en éliminant les termes donnant des puissances négatives en les u_i dans le développement en série de Laurent, on obtient

$$C(t;\mathbf{u};\mathbf{1}) = \frac{1-t^6u_1^2u_2^2u_3^2}{(1-tu_1u_2u_3)(1-t^2u_1^2)(1-t^2u_2^2)(1-t^2u_3^2)(1-t^3u_1u_2u_3)(1-t^4)} \qquad (43)$$

(Les puissances des v_i n'apportant aucune information, nous avons posé $v_i = 1$).

En fait un système complet de covariants est connu depuis la fin du XIX$^{\text{ième}}$ siècle. En 1881, C. Le Paige a donné la liste des covariants en utilisant la méthode des transvectants [30, 31]

$$A = \sum_i a_{4i_2+2i_1+i_0} x_{i_2} y_{i_1} z_{i_0}\,, \qquad (44)$$

$$H_x(\mathbf{x}) = (A,A)^{011} = \det\left(\frac{\partial^2 A}{\partial y_j \partial z_k}\right), \qquad (45)$$

$$H_y(\mathbf{y}) = (A,A)^{101} = \det\left(\frac{\partial^2 A}{\partial x_i \partial z_k}\right), \qquad (46)$$

$$H_z(\mathbf{z}) = (A,A)^{110} = \det\left(\frac{\partial^2 A}{\partial x_i \partial y_j}\right), \qquad (47)$$

$$T(\mathbf{x},\mathbf{y},\mathbf{z}) = (A,H_x)^{100} = \begin{vmatrix} \frac{\partial A}{\partial x_1} & \frac{\partial A}{\partial x_2} \\ \frac{\partial H_x}{\partial x_1} & \frac{\partial H_x}{\partial x_2} \end{vmatrix}, \qquad (48)$$

$$\Delta = (A,T)^{111}. \qquad (49)$$

On voit bien comment la série $C(t;\mathbf{u};\mathbf{1})$ peut aider à décrire l'algèbre. Dans le dénominateur, le facteur $1-tu_1u_2u_3$ correspond à la forme fondamentale, les facteurs $1-t^2u_1^2$, $1-t^2u_2^2$ et $1-t^2u_3^2$ respectivement aux covariants H_x, H_y et H_z, $1-t^3u_1u_2u_3$ à T et $1-t^4$ à Δ. Le numérateur correspond à une syzygy

$$T^2 + \frac{1}{2}H_xH_yH_z + \Delta A^2 = 0\,. \qquad (50)$$

Dans un article postérieur, C. Le Paige, a donné une liste de formes normales sur lesquelles il a évalué les différents covariants (voir aussi Schwartz [36])

Formes canoniques	Δ	H_x	H_y	H_z	T
$F_1 = x_1y_1z_1 + x_2y_2z_2 \sim \|GHZ\rangle$	-1	$2x_1x_2$	$2y_1y_2$	$2z_1z_2$	$x_1y_1z_1 - x_2y_2z_2$
$F_2 = x_1y_1z_2 + x_1y_2z_1 + x_2y_1z_1 \sim \|W\rangle$	0	$-2x_1^2$	$-2y_1^2$	$-2z_1^2$	$2x_1y_1z_1$
$F_{3x} = x_1y_1z_2 + x_1y_2z_1$	0	$-2x_1^2$	0	0	0
$F_{3y} = x_1y_1z_2 + x_2y_1z_1$	0	0	$-2y_1^2$	0	0
$F_{3z} = x_1y_2z_1 + x_2y_1z_2$	0	0	0	$-2z_1^2$	0
$F_4 = x_1y_1z_1$	0	0	0	0	0

Le système de covariants permet bien de discriminer entre $|W\rangle$ et les états factorisés. Remarquons que dans le tableau ci-dessus, F_1 et F_2 représentent les états non factorisables (assimilés respectivement à $|GHZ\rangle$ et $|W\rangle$), les formes F_{3x}, F_{2y} et F_{2z} sont partiellement factorisables et, enfin F_4 est complétement factorisable.

4.4 Intrication des 4-qubits

Nous allons appliquer ici la méthode précédente afin de trouver un système de complet de covariants des 4-qubits. On veut donc classer suivant leur niveau d'intrication, les états de la forme

$$|\phi\rangle = \sum_{i=0}^{15} a_i||i\rangle\rangle \tag{51}$$

avec $||n\rangle\rangle = |n_3n_2n_1n_0\rangle = |n_3\rangle \otimes |n_2\rangle \otimes |n_1\rangle \otimes |n_0\rangle$ si $n = 8n_3 + 4n_2 + 2n_1 + n_0$. Les formes normales auxquelles ont peut ramener un 4-qubit sous l'action de G sont connues depuis peu. Elles ont été trouvées en 2002 par Verstraete, Dehaene, De Moor et Verschelde [46] et sont résumées dans la liste ci-dessous.

$$\begin{aligned}
G_{abcd} &= a(|0000\rangle + |1111\rangle) + b(|0011\rangle + |1100\rangle) + c(|0101\rangle + |1010\rangle +) \\
&\quad d(|0110\rangle + |1001\rangle) \\
L_{abc_2} &= a(|0000\rangle + |1111\rangle) + b(|0011\rangle + |1100\rangle) + c(|0101\rangle + |1010\rangle) + \\
&\quad |0110\rangle \\
L_{a_2b_2} &= a(|0000\rangle + |1111\rangle) + b(|0101\rangle + |1010\rangle) + |0110\rangle + |0011\rangle \\
L_{ab_3} &= a(|0000\rangle + |1111\rangle) + \tfrac{a+b}{2}(|0101\rangle + |1010\rangle) + \tfrac{a-b}{2}(|0110\rangle + |1001\rangle) + \\
&\quad \tfrac{i}{\sqrt{2}}(|0001\rangle + |0010\rangle + |0111\rangle + |1011\rangle) \\
L_{a_4} &= a(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle) + i(|0001\rangle - |1011\rangle) + |0110\rangle \\
L_{a_20_{3\oplus\bar{1}}} &= a(|0000\rangle + |1111\rangle) + (|0011\rangle + |0101\rangle + |0110\rangle) \\
L_{0_{5\oplus\bar{3}}} &= |0000\rangle + |0101\rangle + |1000\rangle + |1110\rangle \\
L_{0_{7\oplus\bar{1}}} &= |0000\rangle + |1011\rangle + |1101\rangle + |1110\rangle \\
L_{0_{3\oplus\bar{1}}0_{3\oplus\bar{1}}} &= |0000\rangle + |1110\rangle
\end{aligned}$$

Le premier article concernant les formes quadrilinéaires binaires a été écrit en 1881 par Le Paige [32]. Il y est donné la liste des covariants de degré inférieur

ou égal à 4, ainsi que quelques syzygies. Peano a décrit complétement la spécialisations $x = y$ et $z = t$. Quelques cinquante années plus tard, Gilham [10, 11] puis Todd [41] ont donné les solutions complétes pour les spécialisation $x = y \neq z \neq t$ et $x = y = z \neq t$ (qui font intervenir un sous groupe de G).
La série génératrice

$$C(t;\mathbf{u};\mathbf{v}) = \Omega_{\geq}^{\mathbf{u}} \prod_{i=1}^{4} \left(1 - \frac{v_i}{u_i^2}\right) \sigma_t \left[\prod_{i=1}^{4} \left(u_i + \frac{v_i}{u_i}\right)\right] . \tag{52}$$

est bien plus difficile à calculer que dans le cas des 3-qubits. Mais en posant $u_i = 0$ et $v_i = 1$ après chaque étape d'élimination, on arrive à calculer assez rapidement (quelques dizaines de minutes) la série de Hilbert-Poincaré de l'algèbre des invariants.

$$C(t;\mathbf{0};\mathbf{1}) = \frac{1}{(1-t^2)(1-t^4)^2(1-t^6)} . \tag{53}$$

Cela ressemble à la série d'une algèbre libre. Mais il faut tout de même le vérifier en calculant un système complet d'invariants. En se guidant sur les degrés indiqués par la série, on peut proposer la liste suivante

$$H = a_0a_{15} - a_1a_{14} - a_2a_{13} + a_3a_{12} - a_4a_{11} + a_5a_{10} + a_6a_9 - a_7a_8 , \tag{54}$$

$$L = \begin{vmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{vmatrix}, M = \begin{vmatrix} a_0 & a_8 & a_2 & a_{10} \\ a_1 & a_9 & a_3 & a_{11} \\ a_4 & a_{12} & a_6 & a_{14} \\ a_5 & a_{13} & a_7 & a_{15} \end{vmatrix} \tag{55}$$

Et, si on pose $b_{xy} = \det\left(\frac{\partial^2 A}{\partial z_i \partial t_j}\right) = [x_0^2, x_0x_1, x_1^2] B_{xy} \begin{bmatrix} y_0^2 \\ y_0y_1 \\ y_1^2 \end{bmatrix}$,

$$D = \det(B_{xy}). \tag{56}$$

En se basant sur l'expression de la série, la liberté de l'algèbre est une conséquence de la non-nullité du Jacobien construit à partir des générateurs ci-dessus.
Les formes normales proposées par l'équipe de Verstraete vont nous servir de test. Peut-on discriminer les formes normales entre elles en utilisant seulement les invariants?
Remarquons que si on pose $X = \{a^2, b^2, c^2, d^2\}$, on a $e_1(X) = 2H(G_{abcd})$, $e_2(X) = (4M + 2L + H^2)(G_{abcd})$, $e_3 = (4D + 2HL)(G_{abcd})$, $e_4 = L(G_{abcd})$. Ce qui signifie que a^2, b^2, c^2 et d^2 sont les quatre racines de la quartique

$$X^4 - 2HX^3 + (H^2 + 2L + 4M)X^2 - (4D + 2HL)X + L \tag{57}$$

On a des propriétés similaires pour les autres formes normales

Forme	racines de $X^4 - 2HX^3 + (H^2 + 2L + 4M)X^2 - (4D + 2HL)X + L$
G_{abcd}	4 racines simples
L_{abc_2}	2 simples et 1 double
$L_{a_2b_2}$	2 doubles
L_{ab_3}	1 simple et 1 triple
L_{a_4}	1 quadruple
$L_{a_2 0_{3\oplus\bar{1}}}$	2 doubles: dont une est 0
$L_{0_{5\oplus\bar{3}}}$	1 quadruple:0
$L_{0_{7\oplus\bar{1}}}$	1 quadruple:0
$L_{0_{3\oplus\bar{1}} 0_{3\oplus\bar{1}}}$	1 quadruple:0

Là encore les invariants ne sont pas suffisants car ils ne permettent pas de séparer $L_{0_{5\oplus\bar{3}}}$, $L_{0_{7\oplus\bar{1}}}$ et $L_{0_{3\oplus\bar{1}} 0_{3\oplus\bar{1}}}$. Les résultats sur les invariants résumés ci-dessus proviennent de [24].
Il faut donc construire l'algèbre des covariants (algèbre de polynômes en les composantes de l'hypermatrice et en les 4 variables binaires $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ et $\mathbf{t}$). Le numérateur de la série de Hilbert de cette algèbre étant énorme et peu exploitable, nous ne donnerons que la forme minimale de la série en posant en plus $\mathbf{u} = \mathbf{1}$.

$$\frac{1}{(-1+t^6)(-1+t^4)^4(t^2-1)^6(t-1)}(t^{19} + t^{17} + 6\,t^{16} + 15\,t^{15} + 11\,t^{14} + 25\,t^{13} + 33\,t^{12} + 41\,t^{11} + 43\,t^{10} + 43\,t^9 + 41\,t^8 + 33\,t^7 + 25\,t^6 + 11\,t^5 + 15\,t^4 + 6\,t^3 + t^2 + 1) \quad (58)$$

À nouveau, la série ne nous a pas servi directement à calculer le système complet de covariants mais nous a guidés. Nous ne détaillerons pas ici le résultat final qui fera l'objet d'un prochain article. Nous avons construit en utilisant la méthode des transvectants un ensemble complet minimal de 170 covariants dont le degré maximal en les composantes de l'hypermatrice est 12 et dont le degré maximal en les variables binaires $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ et $\mathbf{t}$ est 6. Cet ensemble est largement suffisant pour séparer les trois dernières formes normales puisque deux (seulement) des covariants, de degrés 3 et 5, suffisent.

5 Conclusion

La technique exposée ici se heurte à des limites sérieuses liées aux coûts en temps et en espace mémoire des calculs. Il sera extrêmement difficile d'obtenir ne serait-ce que la série de Hilbert de l'algèbre des invariants des 5-qubits. Le seul cas qui semble encore traitable par ce biais est celui des 3-qtrits (trois faisceaux de photons dont le spin est intriqué). Une série génératrice des invariants

$$\frac{1}{(1-t^6)(1-t^9)(1-t^{12})} \tag{59}$$

peut-être conjecturée à partir de [5], et doit pouvoir être prouvée grâce aux méthodes exposées ici.
L'étude des covariants n'a pas seulement pour but de classer les état d'intrication. Un des challenges de l'information quantique consiste en la définition de mesures d'intrication. Celles-ci pourraient être obtenues par une utilisation astucieuse des covariants polynomiaux pour l'action de $GL_n^{\otimes k}$ [2, 3] ou bien des invariants pour l'action de $SU(n)^{\otimes k}$ [13].

Remerciements:
Je remercie Jean-Yves Thibon et Alain Lascoux pour leurs commentaires et leurs remarques.

References

[1] Alain Aspect,*Testing Bell's Inequalities*, Quantum Reflections, Cambridge University Press, 2000,69-78.

[2] J.-L. Brylinski, *Algebraic measures of entanglement*, preprint arXiv:quant-ph/0008031.

[3] J.-L. Brylinki and R. Brylinski, *Invariant polynomial functions on k qudits*, preprint arXiv:quant-ph/0010101.

[4] A. Cayley, *Mémoire sur les hyperdéterminants*, J. reine u. angew. Math. **30** (1846), 1–37.

[5] J.H. Chanler, *The invariant theory of the ternary trilinear form*, Duke Math. J. **5** (1933), 552-568.

[6] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New-York.

[7] A. Duschek, *Eine Abbildung des binären Trilinearform*, Jahresber. Dtsch. Math. Ver. **32** (1923), 234–239.

[8] C.W. Gilham, *The complete system of concomitants of a multiple binary form*, J. London Math. Soc **4** (1929), 166-171.

[9] C.W. Gilham, *A rational basis for the concomitants of a multiple binary form*, J. London Math. Soc **6** (1931), 203–209.

[10] C.W. Gilham, *The complete system of the binary* $(2,1,1)$ *form*, Proc. London Math. Soc. (2) **32** (1931), 259–272.

[11] C.W. Gilham, *A note on the complete system of the binary* $(2,1,1)$ *form*, Proc. London Math. Soc. (2) **38** (1935), 271–272.

[12] I.M. Gelfand, M.M. Krapranov, A.V. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*, Mathematics: Theory & Applications. Birkhuser Boston, Inc., Boston, MA, 1994, 523 pp.

[13] M. Grassl, M.Roetteler, T. Beth, *Computing Local Invariants of Qubit Systems*, Phys.Rev. A58 (1998) 1833-1839.

[14] D. Heiss (ed.), *Fundamentals of Quantum Information*, Springer 2002.

[15] F.L. Hitchcock, *A new method in the theory of quantics*, J. Math. and Phys. **8** (1929), 81–105.

[16] F.L. Hitchcock, *The expression of a tensor or polyadic as a sum of products*, J. Math. and Phys. **6** (1927), 164–189.

[17] F.L. Hitchcock, *Multiple invariants and generalized rank of a p-way matrix or tensor*, J. Math. and Phys. **7** (1927), 40–79.

[18] E. Kasner, *The cogredient and digredient theories of multiple binary forms*, Trans. Amer. Math. Soc. **4** (1903), 86–102.

[19] A.A. Klyachko, *Coherent states, entanglement, and geometric invariant theory*, preprint arXiv:quant-ph/0206012.

[20] L. Landau et E. Liftchitz, *Physique théorique Tome 3: Mécanique quantique*, édition Mir 1966.

[21] D.E. Littlewood, *The theory of group characters*, 2nd. ed., Oxford, 1950.

[22] D.E. Littlewood, *A university algebra*, William Heinemann Ltd., 1958.

[23] J.-G. Luque, J.-Y. Thibon, *Hankel hyperdeterminants and Selberg integrals*, preprint math-ph/0211044, à paraître dans Journ. Phys. A.

[24] J.-G. Luque, J.-Y. Thibon, *Polynomial invariants of four qubits*, quant-ph/0212069, à paraître dans Phys. Rev. A.

[25] I.G. Macdonald,*Symmetric functions and Hall polynomials*, 2nd ed., Clarendon Press, Oxford, 1995.

[26] W. F. Meyer, *Allgemeine Formen und Invariantentheorie*, Bd. 1,*Binäre Formen*, G.J. Göschen'sche Verlagshandlung, Leipzig, 1909.

[27] A. Miyake, *Topological classification of multipartite entangled states by the hyperdeterminant*, preprint arXiv:quant-ph/0206111.

[28] Olver, *Classical invariant theory*, Cambridge.

[29] C. Le Paige, *Mémoire sur quelques applications de la théorie des formes algébriques à la géométrie*, Mém. couronnés et mém. savants étrang. publiés Acad. Roy. sci. Belgique **42** (1879), 1–71.

[30] C. Le Paige, *Sur les formes trilinéaires*, C.R. Acad. Sci. Paris **92** (1881), 1103–1105.

[31] C. Le Paige, *Sur la théorie des formes binaires à plusieurs séries de variables*, Bull. Acad. Roy. Sci. Belgique (3), bf 2 (1881), 40–53.

[32] C. Le Paige, *Sur la forme quadrilinéaire*, Atti Acc. R. di Sc. Torino **17**, (1881-82), 299–319.

[33] G. Peano, *Formazione invariantive della correspondanza*, Giornale di Matematiche **20** (1882), 79–101.

[34] W. Saddler, *Triple binary forms; the complete system for a single* $(1,1,1)$ *form with its geometrical interpretation*, Proc. Cambridge Phil. Soc. **22** (1925), 688–693.

[35] T. Scharf, J.-Y. Thibon and B.G. Wybourne, *Reduced notation, inner plethysm and the symmetric group*, J. Phys. A: Math. Gen. **24** (1993), 7461-7478.

[36] E. Schwartz,*Ueber binäre trilineare Formen*, Math. Zeitschr. **12** (1922), 18–35.

[37] N.P. Sokolov, *Spatial matrices and their applications* (in Russian), Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1960.

[38] V. Tapia, *Algebraic invariants, determinants, and Cayley-Hamilton theorem for hypermatrices. The fourth-rank case*, preprint arXiv:math-ph/0208010.

[39] J.-Y. Thibon, *Hopf algebras of symmetric functions and tensor products of symmetric group representations*, International Journal of Algebra and Computation, **2** (1991), 207-221.

[40] R.M. Thrall and J.H. Chanler, *Ternary trilinear forms in the field of complex numbers*, Duke Math. J. **4** (1938), 678–690.

[41] J.A. Todd, *The complete system of the binary* $(3,1)$ *form*, Proc. Cambridge Phil. Soc. **42** (1946), 196–205.

[42] J.A. Todd, *The complete system of the binary* $(4,1)$ *form*, Proc. Cambridge Phil. Soc. **42** (1946), 206–216.

[43] H.W. Turnbull, *Gordan's theorem for double binary forms*, Proc. Edin. Math. Soc. **xli** (1922-23), 116-127.

[44] H.W. Turnbull, *Double binary forms*, Proc. Roy. Soc. Edinburgh **43** (1923), 43–50.

[45] H.W. Turnbull, *A Geometrical interpretation of the complete system of the double binary* $(2,2)$ *form*, Proc. Roy. Soc. Edinburgh **44** (1923-34), 23–50.

[46] F. Verstraete, J. Dehaene, B. De Moor and H. Verschelde, *Four qubits can be entangled in nine different ways*, Phys. Rev. A. **65** (2002), 052112-??.