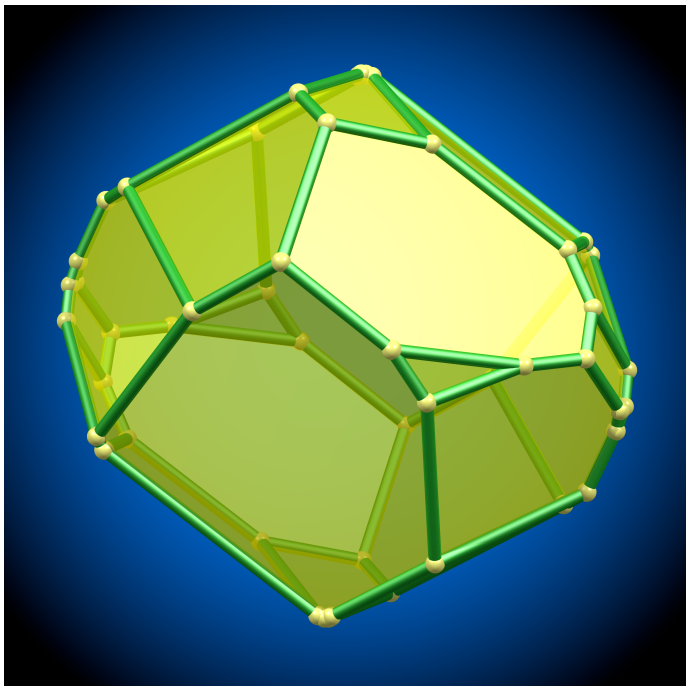
Institut Camille Jordan
UMR 5208 du CNRS

Géométrie de l'intrication quantique



Guillaume Aubrun

Habilitation à diriger des recherches

Université Claude Bernard Lyon 1

Université Claude Bernard Lyon 1
Spécialité : **Mathématiques**
N. d'ordre 0182017

Géométrie de l'intrication quantique

Habilitation à diriger des recherches

Soutenue publiquement le 27 mars 2017 par

Guillaume Aubrun

devant le Jury composé de :

M. Franck Barthe	IMT, Toulouse	Rapporteur
M. Benoît Collins	Université de Kyoto	Examinateur
M. Christophe Garban	ICJ, Lyon	Examinateur
Mme Alice Guionnet	UMPA, ENS Lyon	Examinatrice
M. Iordanis Kerenidis	LIAFA, Paris 7	Examinateur
M. Gilles Pisier	IMJ, Paris 6 et Texas A&M	Examinateur
M. Quanhua Xu	LMB, Besançon	Rapporteur

Avant-propos

Introduction

Ce mémoire d'habilitation à diriger des recherches synthétise les activités de recherche que j'ai effectuées entre 2006 et 2016 en tant que maître de conférences à l'Université Claude Bernard Lyon 1.

Mes travaux s'inscrivent à l'interface de l'analyse fonctionnelle, des probabilités et de la théorie quantique de l'information. Les liens entre l'analyse fonctionnelle et la physique quantique sont évidents, ne serait-ce que par l'omniprésence de l'espace de Hilbert dans le formalisme quantique. En outre, des connexions plus surprenantes et très fécondes ont été récemment mises à jour : par exemple entre les inégalités de Bell et les espaces d'opérateurs, ou entre le problème de Connes sur les algèbres de von Neumann et la question, soulevée par Tsirelson, de savoir comment modéliser la localité en physique quantique.

La branche de l'analyse fonctionnelle dont je suis spécialiste est la *théorie locale des espaces de Banach*, qui étudie les propriétés, notamment géométriques, des espaces vectoriels normés de dimension finie mais grande. J'utiliserai plutôt la terminologie de *géométrie des convexes*, afin d'insister sur l'importance jouée par certains convexes dépourvus de symétrie centrale et qui ne sont donc pas directement reliés à une norme, ce qui est parfois source de difficultés supplémentaires. De tels ensembles apparaissent naturellement en théorie quantique de l'information, par exemple pour décrire le phénomène de l'intrication quantique. Ces ensembles sont de dimension gigantesque : il y a 65535 degrés de liberté dans la description de l'état d'un octet quantique. C'est un cadre idéal pour mettre en œuvre les méthodes de géométrie des convexes.

Les phénomènes asymptotiques de la géométrie des convexes sont indissociables des probabilités : le fléau de la grande dimension, qui rend souvent les approches numériques ou combinatoires irréalistes, devient une bénédiction lorsque l'on utilise la *méthode probabiliste* en laissant le hasard choisir

pour nous là où la complexité dépasse notre raison. Les probabilités ne sont pas une fin en soi, mais un outil, puissant et multiforme, pour appréhender la grande dimension. Cet aspect est présent dans l'ensemble de mes travaux.

Décrivons maintenant la composition du mémoire. Le Chapitre 1 présente des résultats classiques de géométrie des convexes, dont le théorème de Dvoretzky sur l'existence de sections presque euclidiennes, et son corollaire dû à Figiel–Lindenstrauss–Milman qui implique que tout convexe est, d'une certaine manière, complexe. Le choix des résultats présentés est bien sûr orienté par les applications ultérieures.

Le Chapitre 2 introduit le concept d'intrication quantique et l'ensemble convexe, noté Sep, qui lui est associé. On définit également certaines notions élémentaires liées : canaux quantiques, transposition partielle.

Le Chapitre 3 étudie l'ensemble Sep avec un œil de géomètre des convexes. On estime en particulier différents invariants géométriques qui lui sont associés. Certaines de ces estimations sont étonnamment subtiles et nécessitent de recourir à des résultats généraux valides pour *tous* les convexes.

Le cœur de ce mémoire est le Chapitre 4, où l'on utilise les informations obtenues au chapitre précédent pour démontrer des théorèmes en théorie quantique de l'information. On obtient ainsi une nouvelle preuve, géométrique, de la violation de l'additivité de la capacité des canaux quantiques à transmettre de l'information classique. On démontre également, géométriquement, une borne inférieure sur la complexité de l'intrication. On obtient enfin des résultats d'approximation parcimonieuse pour des mesures quantiques et pour des canaux mélangeants.

Le Chapitre 5 est consacré à l'étude des propriétés des états quantiques aléatoires. On démontre l'existence, en fonction de la dimension de l'environnement, d'une transition de phase pour la dichotomie intrication vs séparabilité, mais aussi pour ses relaxations naturelles que sont la transposition partielle et le réalignement. On obtient ainsi une image précise des aspects génériques de l'intrication en grande dimension.

J'ai enfin regroupé dans le Chapitre 6 une brève description de mes autres travaux. Certains sont liés au phénomène de la catalyse quantique et à la propriété de multiplicativité des normes ℓ_p. Un article étudie la fonction maximale associée à des cubes de grande dimension.

En règle générale, je ne donne pas de preuve des résultats énoncés, mais je commente de façon informelle les idées principales sous-jacentes. Une grande partie du matériel présenté ici se trouve aussi, de manière beaucoup plus détaillée, dans le livre *Alice and Bob meet Banach*, coécrit avec Stanisław Szarek, qui est en voie d'être publié et dont la rédaction a été une de mes occupations majeures de ces dernières années.

Remerciements

Je souhaite remercier l'ensemble des membres du jury, et tout particulièrement les rapporteurs (Franck Barthe, Patrick Hayden et Quanhua Xu) pour avoir accepté de consacrer du temps à la lecture du manuscrit.

Je voudrais également remercier toutes les personnes avec qui j'ai eu l'occasion de travailler au cours de ces dix dernières années : mes co-auteurs (au premier rang desquels se trouve Staszek Szarek), mes collègues mathématiciens et administratifs de l'Institut Camille Jordan et d'ailleurs, et aussi mes étudiants, de la licence jusqu'au doctorat.

Merci enfin à mes amis et à ma famille.

Liste des travaux de recherche

J'ai adopté la convention suivante pour la bibliographie : les travaux dont je suis auteur ou co-auteur, listés ci-après, sont cités par une référence de la forme [An] où n est un nombre. Les autres citations, de la forme [n], sont regroupées en fin de manuscrit.

[A1] G. Aubrun et S. Szarek. *Alice and Bob meet Banach. The Interface of Asymptotic Geometric Analysis and Quantum Information Theory*. American Mathematical Society, Providence, RI, à paraître dans la série *Mathematical Surveys and Monographs*.

[A2] G. Aubrun et S. Szarek. Dvoretzky's Theorem and the Complexity of Entanglement Detection, *Discrete Analysis* **1** (2017).

[A3] G. Aubrun, Quantum entanglement in high dimensions, notes de cours d'une école d'hiver à Métabief (décembre 2014), à paraître dans *Lecture Notes in Mathematics*.

[A4] G. Aubrun, F. Sukochev et D. Zanin. Catalysis in the trace class and weak trace class ideals, *Proc. AMS* **144**, 2461–2471 (2016).

[A5] G. Aubrun et C. Lancien. Zonoids and sparsification of quantum measurements, *Positivity* **20**, 1–23 (2016).

[A6] G. Aubrun et C. Lancien. Locally restricted measurements on a multipartite quantum system : data hiding is generic, *Quant. Inf. Comput.* **15**, 513–540 (2015).

[A7] G. Aubrun. Is a random state entangled?, *XVIIth International Congress on Mathematical Physics*. World Sci. Publ., Hackensack, NJ, 534–541 (2014).

[A8] G. Aubrun, S. Szarek et D. Ye. Entanglement thresholds for random induced states, *Comm. Pure Appl. Math.* **67**, 129–171 (2014).

[A9] G. Aubrun et I. Nechita. Realigning random states, *J. Math. Phys.* **53**, 102210 (2012).

[A10] G. Aubrun, S. Szarek et D. Ye. Phase transitions for random states and a semi-circle law for the partial transpose, *Phys. Rev. A* **85**, 030302 (2012).

[A11] G. Aubrun. Partial transposition of random states and non-centered semicircular distributions, *Random Matrices Theory and Appl.* **1**, 1250001 (2012).

[A12] G. Aubrun et I. Nechita. The multiplicative property characterizes ℓ_p and L_p norms, *Confluentes Math.* **3**, 637 (2011).

[A13] G. Aubrun, S. Szarek et E. Werner. Hastings's additivity counterexample via Dvoretzky's theorem, *Comm. Math. Phy.* **305**, 85–97 (2011).

[A14] G. Aubrun, S. Szarek et E. Werner. Non-additivity of Rényi entropy and Dvoretzky's theorem, *J. Math. Phys.* **51**, 022102 (2010).

[A15] G. Aubrun. Maximal inequality for high-dimensional cubes, *Confluentes Math.* **1**, 169–179 (2009).

[A16] G. Aubrun. On almost randomizing channels with a short Kraus decomposition, *Comm. Math. Phys.* **288**, 1103–1116 (2009).

[A17] G. Aubrun et I. Nechita. Stochastic ordering for iterated convolutions and catalytic majorization, *Ann. Inst. Henri Poincaré Probab. Stat.* **45** (3), 611–625 (2009).

[A18] G. Aubrun et I. Nechita. Catalytic majorization and ℓ_p norms, *Comm. Math. Phys.* **278** 133–144 (2008).

Les travaux suivants ont été effectués durant ma thèse.

[A19] G. Aubrun. Sampling convex bodies : a random matrix approach, *Proc. AMS* **135**, 1293–1303 (2007).

[A20] G. Aubrun. Random points in the unit ball of ℓ_p^n, *Positivity* **10**, 755–759 (2006).

[A21] G. Aubrun. Tensor product of convex sets and the volume of separable states on N qudits, *Phys. Rev. A* **73** (2006).

[A22] G. Aubrun. A sharp small deviation inequality for the largest eigenvalue of a random matrix, *Séminaire de probabilités*, volume XXXVIII LNM 1857 (2005).

[A23] G. Aubrun et M. Fradelizi, Two-point symmetrization and convexity, *Arch. Math.* **82**, 282–288 (2004).

Notations et conventions

Les lettres C et c désignent des constantes finies strictement positives non spécifiées. Si on assigne à C une valeur suffisamment grande et à c une valeur suffisamment petite, tous les énoncés de ce mémoire sont vrais. Lorsque x et y sont des quantités strictement positives, on écrira $x = O(y)$ si $x \leqslant Cy$, $x = \Omega(y)$ si $x \geqslant cy$, et $x = \Theta(y)$ si $cy \leqslant x \leqslant Cy$.

Les autres notations utilisées sont standard : on note $\mathsf{M}_{m,n}$ l'espace des matrices $m \times n$ à coefficients complexes, et $\mathsf{M}_n \coloneqq \mathsf{M}_{n,n}$. On désigne par $\mathsf{M}_n^{\mathrm{sa}}$ le sous-espace de M_n formé des matrices hermitiennes et par $\mathcal{PSD}_n$ le cône des matrices hermitiennes positives. La matrice identité est notée I. On identifiera librement M_n avec l'espace des applications linéaires sur $\mathbb{C}^n$. Pour $p \in [1, +\infty]$, on considérera la p-norme de Schatten $\|\cdot\|_p$ sur M_n ; la même notation désignera la norme ℓ_p sur $\mathbb{R}^n$.

J'utilise la convention des physiciens pour le produit scalaire d'un espace de Hilbert (il est antilinéaire en son premier argument), ainsi que la notation de Dirac, tellement commode que je ne comprends pas qu'elle ne soit pas universellement adoptée : si x et y sont des vecteurs d'un espace de Hilbert, on désigne par $|x\rangle\langle y|$ l'application linéaire de rang 1 qui à z associe $\langle y|z\rangle x$.

Un certain nombre de mes résultats concernant des modèles aléatoires sont énoncés avec la mention « avec grande probabilité ». J'ai choisi cette formulation pour gagner en concision quitte à perdre en précision. Des énoncés plus détaillés se trouvent dans les articles publiés. Dans la plupart des cas, il faut comprendre que la probabilité que l'objet aléatoire ait la propriété annoncée tend vers 1, exponentiellement vite, lorsque la dimension sous-jacente tend vers l'infini.

Chapitre 1

Convexité en grande dimension

Ce chapitre présente une sélection de résultats très classiques sur la géométrie des corps convexes de grande dimension. On détaillera dans les chapitres ultérieurs plusieurs applications en théorie quantique de l'information.

1.1 Polarité, volume et largeur moyenne

Rappelons quelques définitions élémentaires de géométrie des convexes. On travaille dans un espace euclidien de dimension finie V, que l'on peut identifier à $\mathbb{R}^n$. On dit que $K \subset V$ est un *corps convexe* si K est compact, convexe, et si 0 est dans l'intérieur de K. Cette dernière condition n'est pas la définition la plus courante (qui est de demander que K soit d'intérieur non vide) mais elle mène à des énoncés plus naturels.

Un exemple de corps convexe est la boule-unité pour la norme euclidienne de V, notée B_V. Si $K \subset V$ est un corps convexe, son *rayon interne* $r_{\text{int}}(K)$ est le plus grand nombre $\lambda > 0$ vérifiant $\lambda B_V \subset K$, et son *rayon externe* $r_{\text{ext}}(K)$ est le plus petit nombre $\lambda > 0$ vérifiant $K \subset \lambda B_V$.

La *jauge* j_K d'un corps convexe $K \subset V$ est définie pour $x \in V$ par

$$j_K(x) \coloneqq \inf\{t \geqslant 0 \,:\, x \in tK\}.$$

La fonction j_K est une norme si et seulement si K est *symétrique*, c'est-à-dire vérifie $K = -K$. Si $K \subset V$ est un corps convexe, son *polaire* K° est le corps convexe défini comme

$$K^\circ = \{x \in V \,:\, \forall y \in K,\ \langle x, y\rangle \leqslant 1\}.$$

Le théorème du bipolaire affirme que $(K^\circ)^\circ = K$. Remarquons les égalités $r_{\text{int}}(K^\circ) = r_{\text{ext}}(K)^{-1}$ et $r_{\text{ext}}(K^\circ) = r_{\text{int}}(K)^{-1}$. La notion duale de la jauge

est la *largeur*, définie pour $u \in V$ par

$$w(K,u) = \max_{x \in K} \langle x, u \rangle = j_{K^\circ}(u).$$

Cette terminologie s'explique par le fait que si u est un vecteur unitaire, la somme $w(K,u) + w(K,-u)$ est la largeur de la zone délimitée par les deux hyperplans tangents à K et orthogonaux à u.

On note vol la mesure de Lebesgue sur V, aussi appelée *volume*. Il est souvent judicieux de considérer le *rayon volumique* d'un corps convexe K, défini par

$$\mathrm{vrad}(K) = \left(\frac{\mathrm{vol}\, K}{\mathrm{vol}\, B_V} \right)^{\frac{1}{\dim V}}.$$

On peut remarquer que $\mathrm{vrad}(K)$ est aussi le rayon d'une boule euclidienne de même volume que K. Un autre invariant associé à un corps convexe K est sa *largeur moyenne*, notée $w(K)$ et définie comme la valeur moyenne de $w(K,\cdot)$ sur la sphère-unité. Le rayon volumique et la largeur moyenne sont reliés par l'inégalité de Urysohn, qui s'apparente à l'inégalité isopérimétrique (en particulier, il y a égalité quand K est une boule euclidienne).

Théorème 1.1.1 (Inégalité de Urysohn)**.** *Pour tout corps convexe K, on a*

$$\mathrm{vrad}(K) \leqslant w(K).$$

Comme corollaire de l'inégalité de Urysohn, on obtient une borne supérieure sur le volume d'un polytope convexe en fonction de son nombre de sommets. Un changement de variables permet de transformer l'expression de la largeur moyenne en l'espérance du maximum d'un processus gaussien, et on peut alors utiliser la sous-additivité de la mesure de probabilité.

Corollaire 1.1.2. *Soit $P \subset \mathbb{R}^n$ un polytope à N sommets, chaque sommet ayant une norme au plus* 1*. Alors*

$$\mathrm{vrad}(P) \leqslant w(P) \leqslant C\sqrt{\frac{\log N}{n}}.$$

La notion de rayon volumique a l'avantage de bien se dualiser, comme le montre le résultat suivant.

Théorème 1.1.3 (Inégalités de Santaló et de Santaló inverse)**.** *Pour tout corps convexe K ayant son centre de gravité à l'origine, on a*

$$c \leqslant \mathrm{vrad}(K)\, \mathrm{vrad}(K^\circ) \leqslant 1. \tag{1.1}$$

TABLE 1.1 – Rayon interne, rayon volumique, largeur moyenne et rayon externe de quelques corps convexes de référence. Au sein de chaque ligne, les quantités sont dans l'ordre croissant de gauche à droite. On désigne par B_n la boule-unité euclidienne de dimension n, et par Δ_n le simplexe régulier normalisé de telle sorte que $\Delta_n^\circ = -\Delta_n$.

K	$r_{\mathrm{int}}(K)$	$\mathrm{vrad}(K)$	$w(K)$	$r_{\mathrm{ext}}(K)$
B_n	1	1	1	1
$[-1,1]^n$	1	$\sim \sqrt{2n/\pi e}$	$\sim \sqrt{2n/\pi}$	$\sqrt{n}$
$([-1,1]^n)^\circ$	$1/\sqrt{n}$	$\sim \sqrt{2e/\pi n}$	$\sim \sqrt{2\log n}/\sqrt{n}$	1
Δ_n	$1/\sqrt{n}$	$\sim \sqrt{e/2\pi}$	$\sim \sqrt{2\log n}$	$\sqrt{n}$

La borne inférieure dans (1.1) (dite de Santaló inverse, [4, 25, 28]) est considérablement plus difficile à montrer que la borne supérieure. La conjecture de Mahler, ouverte en dimensions 3 et plus, stipule que sous l'hypothèse du théorème, le produit $\mathrm{vrad}(K)\,\mathrm{vrad}(K^\circ)$ est minimal pour les simplexes.

1.2 Théorème de Dvoretzky

Un espace normé $(X, \|\cdot\|)$ est dit *C-euclidien* s'il existe une norme euclidienne $|\cdot|$ sur X vérifiant $|\cdot| \leqslant \|\cdot\| \leqslant C|\cdot|$. Le théorème de Dvoretzky est le résultat suivant, initialement conjecturé par Grothendieck.

Théorème 1.2.1 (Dvoretzky, [8])**.** *Soit X un espace normé de dimension infinie. Alors pour tout $n \in \mathbb{N}$ et $\varepsilon > 0$, X contient un sous-espace de dimension n qui est $(1+\varepsilon)$-euclidien.*

La version la plus utile pour les applications est une forme quantitative du théorème de Dvoretzky, due à Milman, qui donne une formule étonnamment précise pour la dimension maximale d'un sous-espace presque euclidien d'un espace de dimension finie donné. Il est plus agréable de travailler avec des corps convexes qu'avec des normes, et on aura besoin de se dispenser de l'hypothèse d'invariance par symétrie centrale.

Introduisons maintenant la *dimension de Dvoretzky* d'un corps convexe $K \subset \mathbb{R}^n$. Elle est définie comme

$$\delta(K) = \left(\frac{w(K^\circ)}{r_{\mathrm{ext}}(K^\circ)}\right)^2 n = w(K^\circ)^2 r_{\mathrm{int}}(K)^2 n.$$

On remarque que $\delta(K) \leqslant n$, puisque la valeur moyenne $w(K^\circ)$ de j_K sur la sphère-unité est inférieure à la valeur maximale $r_{\mathrm{ext}}(K^\circ)$. La dimension de Dvoretzky donne la dimension maximale d'une section presque euclidienne générique : c'est le contenu du théorème de Dvoretzky–Milman.

Théorème 1.2.2 (Dvoretzky–Milman, [27]). *Pour tout corps convexe $K \subset \mathbb{R}^n$, tout $0 < \varepsilon < 1$, et tout $k \leqslant c\varepsilon^2\delta(K)$, si E est un sous-espace de dimension k choisi aléatoirement selon la mesure de Haar sur la grassmannienne $\mathsf{Gr}(k, \mathbb{R}^n)$, alors les inclusions*

$$(1-\varepsilon)w(K^\circ)^{-1}B_E \subset K \cap E \subset (1+\varepsilon)w(K^\circ)^{-1}B_E$$

ont lieu avec grande probabilité. Ici B_E désigne la boule-unité euclidienne dans E.

Le Théorème 1.2.2 est un des grands succès de la méthode probabiliste en théorie locale des espaces de Banach et utilise de manière cruciale la propriété de *concentration de la mesure*. Le cas le plus emblématique, celui la boule-unité de l'espace ℓ_1^n dont la dimension de Dvoretzky est de l'ordre de n, a été beaucoup considéré du fait de ses applications en informatique théorique ; malgré de nombreux efforts, les méthodes constructives ne parviennent pas à faire aussi bien que le Théorème 1.2.2.

La conclusion du Théorème 1.2.2 peut s'énoncer différemment : les oscillations de la jauge j_K, vue comme fonction définie sur la sphère-unité, sont petites sur une sous-sphère choisie aléatoirement. La condition importante sur la jauge est le contrôle de la constante de Lipschitz, égale à $r_{\mathrm{int}}(K)^{-1}$ et qui apparaît dans la définition de la dimension de Dvoretzky. Le fait que la jauge soit une fonction convexe joue un rôle mineur, comme l'atteste le théorème suivant : toute fonction lipschitzienne sur la sphère est presque constante sur une sous-sphère typique. On désigne par $S_{\mathbb{C}^d}$ la sphère-unité de $\mathbb{C}^d$. On dit qu'une fonction $f : S_{\mathbb{C}^d} \to \mathbb{R}$ est *cerclée* si elle vérifie $f(e^{i\theta}x) = f(x)$ pour $x \in S_{\mathbb{C}^d}$ et $\theta \in \mathbb{R}$, et on note $\mathbf{E}\, f$ la valeur moyenne de f par rapport à la mesure uniforme sur $S_{\mathbb{C}^d}$.

Théorème 1.2.3 (Dvoretzky–Milman pour les fonctions lipschitziennes). *Pour toute fonction $f : S_{\mathbb{C}^d} \to \mathbb{R}$ 1-lipschitzienne cerclée, tout $0 < \varepsilon < 1$, et tout $k \leqslant c\varepsilon^2 d$, si E est un sous-espace de dimension k choisi aléatoirement selon la mesure de Haar sur la grassmannienne $\mathsf{Gr}(k, \mathbb{C}^d)$, alors, avec grande probabilité,*

$$\sup_{x \in S_{\mathbb{C}^d} \cap E} |f(x) - \mathbf{E}\, f| \leqslant \varepsilon.$$

Nous énonçons le Théorème 1.2.3 dans le cadre complexe car c'est celui dans lequel nous l'appliquerons. Notons que ce contexte nous interdit d'invoquer les inégalités de Slepian–Gordon, qui permettent d'obtenir dans le cas réel une preuve élégante du Théorème 1.2.3 avec la dépendance optimale en ε, cruciale pour nos applications. Comme nous l'avons remarqué dans [A13], un palliatif consiste à utiliser un argument de chaînage dû à Schechtman [33] qui se transpose sans difficulté au cadre complexe.

1.3 Inégalité MM^*

L'inégalité ponctuelle $j_K(\cdot)j_{K^\circ}(\cdot) \geqslant 1$, ou encore $w(K,\cdot)w(K^\circ,\cdot) \geqslant 1$, implique après intégration la borne inférieure $w(K)w(K^\circ) \geqslant 1$ sur les largeurs moyennes. Il est facile de voir, par exemple en considérant des ellipses de grande excentricité, que le produit $w(K)w(K^\circ)$ peut prendre des valeurs arbitrairement grandes même en dimension 2 : il n'y a pas d'analogue de l'inégalité de Santaló pour la largeur moyenne. Néanmoins une inégalité remarquable, combinant des résultats de Pisier [30] et de Figiel–Tomczak-Jaegermann [10], affirme que tout corps convexe *symétrique* a une image linéaire pour laquelle ce produit admet une borne supérieure en $\log n$.

Théorème 1.3.1 (Inégalité MM^*)**.** *Soit $K \subset \mathbb{R}^n$ un corps convexe symétrique. Il existe une application linéaire $T \in \mathsf{GL}(n,\mathbb{R})$, telle que, si on note $L = TK$, on ait*

$$w(L)w(L^\circ) \leqslant C \log n. \tag{1.2}$$

L'application linéaire T est obtenue comme l'unique solution d'un problème de minimisation, ce qui permet d'obtenir des informations supplémentaires : toute transformation orthogonale préservant K doit aussi préserver L. Lorsque le groupe des isométries de K agit irréductiblement, on peut donc choisir $L = K$.

On ne sait pas si la borne supérieure de (1.2) peut être améliorée en $C\sqrt{\log n}$, qui est la valeur obtenue lorsque K est un cube (voir la Table 1.1). Une autre question intéressante est de savoir si le théorème reste vrai sans l'hypothèse de symétrie centrale sur K, en choisissant alors T parmi le groupe affine.

On peut donner une interprétation géométrique du Théorème 1.3.1 en le combinant avec le théorème de Dvoretzky–Milman. Supposons pour cela que le corps convexe $L = TK$ vérifie de plus $\delta(L) \gg 1$ et $\delta(L^\circ) \gg 1$, ce qui est le cas pour les exemples usuels. On peut alors appliquer le théorème de Dvoretzky–Milman simultanément à L et L° et conclure que pour un sous-espace générique de dimension $k \ll \min(\delta(L), \delta(L^\circ))$, la section $L \cap E$ est

presque une boule euclidienne de rayon $w(L^\circ)^{-1}$ tandis que la projection orthogonale $P_E L$ est presque une boule euclidienne de rayon $w(L)$. Le produit $w(L)w(L^\circ)$ apparaît donc comme le rapport entre les rayons des projections et sections typiques.

1.4 Inégalité de Figiel–Lindenstrauss–Milman

Une conséquence du théorème de Dvoretzky–Milman est une inégalité due à Figiel–Lindenstrauss–Milman qui exprime une borne inférieure sur la complexité d'un corps convexe. Nous exprimons cette inégalité à l'aide des concepts de dimension en sommets et dimension en facettes introduits dans [A2]. Ces notions ne sont pas présentes explicitement dans l'article d'origine [9] mais seront particulièrement utiles pour nos applications.

Si $K \subset V$ est un corps convexe, notons $\mathscr{P}_K$ l'ensemble des polytopes P vérifiant $P \subset K \subset 4P$ (le choix de la constante 4 est arbitraire). Définissons la *dimension en sommets* de K comme

$$\dim_V(K) = \log \inf\{N \ : \ \text{il existe } P \in \mathscr{P}_K \text{ ayant } N \text{ sommets}\},$$

ainsi que la *dimension en facettes* de K comme

$$\dim_F(K) = \log \inf\{N \ : \ \text{il existe } Q \in \mathscr{P}_K \text{ ayant } N \text{ facettes}\},$$

où par *facette* on entend face de codimension 1. Pour justifier la terminologie de dimension, on peut signaler que pour tout corps convexe $K \subset \mathbb{R}^n$ ayant son centre de gravité à l'origine, on a

$$\dim_V(K) \leqslant Cn, \quad \dim_F(K) \leqslant Cn.$$

Ces inégalités sont très classiques dans le cas de corps convexes symétriques. Enfin, on note $a(K)$ l'*asphéricité* de K, qui est la distance de Banach–Mazur de K à la boule euclidienne et s'écrit comme

$$a(K) = \inf\left\{ \frac{r_{\text{ext}}(TK)}{r_{\text{int}}(TK)} \ : \ T \in \mathsf{GL}(V) \right\}.$$

On peut argumenter que chacun des paramètres $\dim_V(K)$, $\dim_F(K)$ et $a(K)$ quantifie différents aspects de la complexité du corps convexe K. Le paramètre $a(K)$ mesure combien K diffère d'une boule euclidienne, idéal platonicien de simplicité. L'inégalité de Figiel–Lindenstrauss–Milman implique qu'au moins une de ces trois quantités doit être grande. Cette inégalité est illustrée dans la Table 1.2 sur quelques corps convexes de référence.

Théorème 1.4.1 (Inégalité de Figiel–Lindenstrauss–Milman, [9]). *Pour tout corps convexe $K \subset \mathbb{R}^n$, on a*

$$\dim_F(K) \dim_V(K) a(K)^2 \geqslant cn^2.$$

TABLE 1.2 – Dimension en sommets, dimension en facettes et asphéricité de quelques corps convexes de référence.

	dimension	$\dim_V(K)$	$\dim_F(K)$	$a(K)$
B_n	n	$\Theta(n)$	$\Theta(n)$	1
$[-1,1]^n$	n	$\Theta(n)$	$\Theta(\log n)$	$\sqrt{n}$
$([-1,1]^n)^\circ$	n	$\Theta(\log n)$	$\Theta(n)$	$\sqrt{n}$
Δ_n	n	$\Theta(\log n)$	$\Theta(\log n)$	n

Si $K \subset \mathbb{R}^n$ est un corps convexe symétrique, alors $a(K) \leqslant \sqrt{n}$, comme on peut le voir en considérant l'ellipsoïde de volume maximal contenu dans K (c'est une conséquence du théorème de John). On en déduit alors le résultat remarquable suivant sur la complexité des polytopes, dont aucune autre démonstration n'est connue : si P est un polytope symétrique de dimension n à v sommets et f facettes, alors $\log v \cdot \log f \geqslant cn$.

1.5 Sous-espaces de dimension finie de L_1

Donnons enfin un autre résultat de la théorie locale des espaces de Banach qui aura une application immédiate en théorie quantique de l'information. Ce résultat est dû à Talagrand [39] et raffine des résultats antérieurs de Schechtman [32] et Bourgain–Lindenstrauss–Milman [3]. À nouveau, la preuve repose sur l'utilisation de la méthode probabiliste.

Théorème 1.5.1 ([39]). *Soit X un sous-espace de dimension n de L_1 et $\varepsilon > 0$. Alors X est $(1+\varepsilon)$-isomorphe à un sous-espace de ℓ_1^N, pour $N = C\varepsilon^{-2} n \log n$.*

On ne sait pas si le théorème est valable sans le facteur $\log n$. On peut également reformuler géométriquement le Théorème 1.5.1. On définit pour cela un *zonotope* comme une somme finie de segments centrés en l'origine, et un *zonoïde* comme une limite de zonotopes au sens de la distance de

Hausdorff. Il est facile de voir qu'un corps convexe K est équivalent (via une application linéaire inversible) à la boule-unité d'un sous-espace de ℓ_1^N si et seulement si K° est un zonotope qui est la somme de N segments ; de même K est équivalent à la boule-unité d'un sous-espace de L_1 si et seulement si K° est un zonoïde. On en déduit donc la reformulation suivante : si $Z \subset \mathbb{R}^n$ est un zonoïde et $\varepsilon > 0$, alors il existe un zonotope $Y \subset \mathbb{R}^n$ qui est la somme de $C\varepsilon^{-2} n \log n$ segments et qui vérifie $Y \subset Z \subset (1+\varepsilon)Y$.

Chapitre 2

L'intrication quantique

Ce chapitre introduit avec un point de vue mathématique le concept d'*intrication quantique* ainsi que quelques notions liées. On se place exclusivement dans le cadre des espaces de Hilbert complexes de dimension finie, ce qui permet de se dispenser de toute considération topologique.

2.1 Intrication vs séparabilité

L'intrication est un phénomène physique fondamental de la mécanique quantique, par lequel des particules distantes interagissent de telle sorte que l'état quantique d'une de ces particules ne peut pas être décrit indépendamment des autres. L'intrication a de nombreuses applications dans divers domaines de l'information quantique : téléportation, cryptographie quantique, ordinateur quantique. On s'intéresse uniquement aux aspects mathématiques de l'intrication quantique.

Soit $\mathcal{H}$ un espace de Hilbert complexe de dimension finie. Un *état* sur $\mathcal{H}$ est un opérateur auto-adjoint positif de trace 1. On désignera par $\mathrm{D}(\mathcal{H})$ l'ensemble des états sur $\mathcal{H}$, et on posera $\mathrm{D}_n = \mathrm{D}(\mathbb{C}^n)$. La lettre D est reminiscente de la terminologie équivalente de « matrice-densité » qui permet de décrire le phénomène de superposition.

Pour simplifier l'exposition, on définira l'intrication uniquement dans le contexte biparti, c'est-à-dire pour un système quantique formé de deux sous-systèmes distants, modélisé par un espace de Hilbert complexe de dimension finie de la forme $\mathcal{H}_1 \otimes \mathcal{H}_2$ (ou plus spécifiquement $\mathbb{C}^d \otimes \mathbb{C}^d$ afin de spécifier que chacun des sous-systèmes possède d niveaux possibles d'énergie).

Si ρ_1 et ρ_2 sont des états sur $\mathcal{H}_1$ et $\mathcal{H}_2$ respectivement, alors $\rho_1 \otimes \rho_2$ est un état sur $\mathcal{H}_1 \otimes \mathcal{H}_2$. Un tel état est appelé *état-produit*. Nous pouvons

maintenant donner la définition fondamentale [41] sur laquelle repose l'étude mathématique du phénomène de l'intrication.

Un état sur $\mathcal{H}_1 \otimes \mathcal{H}_2$ est dit *séparable* s'il peut s'écrire comme combinaison convexe d'états-produits. Un état non séparable est dit *intriqué*.

La dichotomie entre intrication et séparabilité est au centre de mes travaux. Cette dichotomie est fondamentalement asymétrique : montrer qu'un état est séparable nécessite souvent d'en expliciter une écriture comme combinaison convexe d'états-produits ; à l'inverse montrer qu'un état est intriqué peut toujours se faire en produisant une forme linéaire qui le sépare de l'ensemble des états-produits. On sait de plus que le problème de décider si un état donné est séparable ou intriqué est algorithmiquement difficile ; on reviendra sur ces considérations au Chapitre 4.2.

2.2 Témoins d'intrication

Notons M_d l'espace des matrices $d \times d$ (identifié à l'espace des applications linéaires de $\mathbb{C}^d$ dans $\mathbb{C}^d$), et $\mathcal{PSD}_d$ le cône des matrices hermitiennes positives. On dit qu'une application linéaire $\Phi : \mathsf{M}_d \to \mathsf{M}_d$ est *positive* si elle vérifie $\Phi(\mathcal{PSD}_d) \subset \mathcal{PSD}_d$, et que $\Phi : \mathsf{M}_d \to \mathsf{M}_d$ est *complètement positive* si, pour tout $n \in \mathbb{N}^*$, l'application $\Phi \otimes \mathrm{Id}_{\mathsf{M}_n}$ est positive.

Soit $\Phi : \mathsf{M}_d \to \mathsf{M}_d$ une application positive et $\rho \in \mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ un état. Il est facile de voir que lorsque ρ est séparable, l'opérateur $(\Phi \otimes \mathrm{Id})(\rho)$ est positif. Par contraposition, dès que $(\Phi \otimes \mathrm{Id})(\rho)$ a une valeur propre strictement négative, on peut en déduire que ρ est intriqué. On dit alors que Φ est un *témoin d'intrication* de ρ. On a le résultat suivant, qui découle d'une application du théorème de Hahn–Banach.

Théorème 2.2.1 (Critère de Horodecki, [21])**.** *Soit ρ un état sur $\mathbb{C}^d \otimes \mathbb{C}^d$. On a l'équivalence :*

(1) ρ est intriqué,

(2) il existe un témoin d'intrication pour ρ.

Un témoin d'intrication est nécessairement une application positive mais non complètement positive. Un exemple de telle application est la transposition $T : \mathsf{M}_d \to \mathsf{M}_d$. Remarquablement, en dimension 2 la transposition est essentiellement le seul témoin d'intrication. C'est le contenu du résultat suivant dû à Størmer.

Théorème 2.2.2 (Størmer, [38]). *Soit $\Phi : \mathsf{M}_2 \to \mathsf{M}_2$ une application positive. Alors il existe deux applications complètement positives Φ_1 et Φ_2 telles que $\Phi = \Phi_1 + \Phi_2 \circ T$.*

La preuve initiale du Théorème 2.2.2, ainsi que les preuves ultérieures, ne sont pas entièrement satisfaisantes car elles reposent sur des calculs ad hoc. Nous en donnerons une preuve plus conceptuelle au Chapitre 3.2.

2.3 Transposition partielle, réalignement

La *transposition partielle* d'un état $\rho \in \mathrm{D}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ est définie par $\rho^\Gamma := (T \otimes \mathrm{Id})(\rho)$, et on dit que ρ est à transposition partielle positive ou *PPT* si l'opérateur ρ^Γ est positif. Tout état qui n'est pas PPT est intriqué [29]. Une conséquence des Théorèmes 2.2.1 et 2.2.2, spécifique à la dimension 2, est une réciproque :

Corollaire 2.3.1. *Un état sur $\mathbb{C}^2 \otimes \mathbb{C}^2$ est séparable si et seulement si il est PPT.*

Identifions un état sur $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ à une matrice par blocs $A \in \mathsf{M}_{d_1 d_2}$ de la forme $A = (A_{ij,kl})$, où $i, k \in \{1, \ldots, d_1\}$ et $j, l \in \{1, \ldots, d_2\}$. Ainsi le coefficient $A_{ij,kl}$ se situe en position (j, l) au sein du bloc d'indices (i, k). La transposition partielle de A est la matrice $A^\Gamma = (A_{kj,il})$ obtenue en échangeant le rôle des coordonnées i et k, c'est-à-dire en « transposant par blocs ».

Une autre opération consiste à permuter les indices j et k : on définit ainsi le *réalignement* $A^R = (A_{ik,jl}) \in \mathsf{M}_{d_1^2, d_2^2}$ [5]. La matrice ainsi obtenue n'est plus hermitienne, et n'est même plus carrée si $d_1 \neq d_2$. Nous dirons qu'un état $\rho \in \mathrm{D}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ est *réalignable* si $\|\rho^R\|_1 \leqslant 1$. Il est facile de vérifier qu'un état séparable est réalignable (il suffit de le faire pour les états produits). On dispose ainsi d'un critère d'intrication qui est très similaire au critère de la transposition partielle. Le parallèle entre les deux critères est encore plus frappant si on réalise que pour un état ρ, on a l'équivalence

$$\rho^\Gamma \geqslant 0 \iff \|\rho^\Gamma\|_1 = 1.$$

On peut vérifier [22] que les 24 permutations possibles des indices $\{i, j, k, l\}$ sont toutes équivalentes à A, A^Γ ou A^R. Nous illustrons l'effet de la transposition partielle et du réalignement sur le cas le plus simple des matrices

de taille $(2 \times 2) \times (2 \times 2)$.

$$A = \left[\begin{array}{cc|cc} a & b & d & e \\ \bar{b} & c & f & g \\ \hline \bar{d} & \bar{f} & h & i \\ \bar{e} & \bar{g} & \bar{i} & j \end{array}\right] \quad A^{\Gamma} = \left[\begin{array}{cc|cc} a & b & \bar{d} & \bar{f} \\ \bar{b} & c & \bar{e} & \bar{g} \\ \hline d & e & h & i \\ f & g & \bar{i} & j \end{array}\right] \quad A^{R} = \left[\begin{array}{cccc} a & b & \bar{b} & c \\ \hline \bar{d} & \bar{f} & \bar{e} & \bar{g} \\ \hline d & e & f & g \\ \hline h & i & \bar{i} & j \end{array}\right]$$

On sait que les deux critères ne sont pas comparables : il existe des états PPT non réalignables, et des états réalignables non-PPT.

2.4 Canaux quantiques

Le concept de *canal quantique* est fondamental en théorie quantique de l'information. Un canal quantique est une application linéaire $\Phi : \mathsf{M}_m \to \mathsf{M}_k$ qui est complètement positive et qui préserve la trace, c'est-à-dire telle que $\operatorname{Tr}\Phi(X) = \operatorname{Tr} X$ pour tout $X \in \mathsf{M}_m$. C'est l'analogue quantique du concept de matrice stochastique. Donnons maintenant un résultat structurel concernant les applications complètement positives.

Théorème 2.4.1. *Soit $\Phi : \mathsf{M}_m \to \mathsf{M}_k$ une application linéaire. Les assertions suivantes sont équivalentes.*

1. *Φ est un canal quantique.*
2. *Il existe $N \in \mathbb{N}^*$ et une isométrie $U : \mathbb{C}^m \to \mathbb{C}^k \otimes \mathbb{C}^N$ tels que, pour tout $X \in \mathsf{M}_m$,*
$$\Phi(X) = (\mathrm{Id} \otimes \mathrm{Tr})(UXU^{\dagger}). \tag{2.1}$$
3. *Il existe une famille finie $A_1, \ldots, A_N \in \mathsf{M}_{k,m}$ vérifiant $\sum A_i^{\dagger} A_i = \mathrm{I}$ et telle que, pour tout $X \in \mathsf{M}_m$,*
$$\Phi(X) = \sum_{i=1}^{N} A_i X A_i^{\dagger}. \tag{2.2}$$

La forme (2.1) est la *représentation de Stinespring* du canal quantique Φ et la forme (2.2) est sa *décomposition de Kraus*. Le N minimal dans ces deux écritures est le même, et s'appelle *rang de Kraus* de Φ. Le rang de Kraus d'un canal quantique $\mathsf{M}_m \to \mathsf{M}_k$ vaut au plus mk.

Chapitre 3

Géométrie de l'intrication

Dans ce chapitre, nous explorons la géométrie de l'ensemble des états et de l'ensemble des états séparables, particulièrement en grande dimension, ce qui sera l'occasion de rajouter deux éléments à la liste des corps convexes de références des Tables 1.1 et 1.2. Les informations que nous aurons recueillies seront exploitées dans les Chapitres 4 et 5.

Le sous-espace affine réel engendré par les états sur $\mathbb{C}^m$ est l'espace des opérateurs auto-adjoints de trace 1. Il sera très fructueux de considérer cet espace comme un espace vectoriel où le rôle de l'origine est joué par l'état maximalement mélangé I/m. Nous illustrons notamment cette idée en donnant une nouvelle preuve du Théorème 2.2.2.

3.1 Géométrie de l'ensemble des états

Considérons l'ensemble D_m des états quantiques sur $\mathbb{C}^m$. On vérifie que D_m est un ensemble convexe compact de dimension réelle $m^2 - 1$ dont les points extrémaux sont les projecteurs orthogonaux de rang 1. L'ensemble des points extrémaux s'identifie naturellement à l'espace projectif $\mathbb{CP}^{m-1}$. Bien que D_m ne soit pas un polytope, on peut décrire précisément sa structure faciale : pour tout sous-espace $E \subset \mathbb{C}^m$, l'ensemble des états dont l'image est incluse dans E forme une face de D_m.

L'espace affine engendré par D_m est l'espace, noté V_m, des opérateurs auto-adjoints de trace 1 sur $\mathbb{C}^m$. Pour tous les raisonnements géométriques que nous allons faire, nous allons considérer V_m comme un espace euclidien. Pour cela, nous choisissons comme origine l'état *maximalement mélangé* $\rho_* := \mathrm{I}/m$, et nous notons $\bullet$ la multiplication scalaire dans cet espace

vectoriel : si $\rho \in V_m$ et $t \in \mathbb{R}$, on définit

$$t \bullet \rho \coloneqq t\rho + (1-t)\rho_*.$$

Le produit scalaire sur V_m est simplement le produit scalaire de Hilbert–Schmidt, qui (étant donné notre choix de l'origine) s'écrit pour $\rho, \sigma \in V_m$

$$\langle \rho, \sigma \rangle = \mathrm{Tr}(\rho\sigma) - \frac{1}{m}.$$

Dans l'espace euclidien V_m, le corps convexe D_m vérifie la relation

$$\mathrm{D}_m^\circ = -m \bullet \mathrm{D}_m. \tag{3.1}$$

Cette égalité est une conséquence du fait que le cône des opérateurs positifs est auto-dual.

Le cas de la dimension 2 mérite d'être signalé : en effet l'ensemble D_2 est une boule euclidienne dans V_2 de rayon $1/\sqrt{2}$, que les physiciens appellent *boule de Bloch*. L'ensemble de ses points extrémaux est la *sphère de Bloch*. Cette situation, qui n'est rien d'autre que l'identification classique $\mathbb{CP}^1 = \mathbb{S}^2$, est très spécifique à la dimension 2. Pour $m > 2$, D_m n'est plus une boule euclidienne, c'est plutôt l'analogue non-commutatif du simplexe.

3.2 Preuve du théorème de Størmer

Nous allons présenter une preuve complète du Théorème 2.2.2 : toute application positive $\Phi : \mathsf{M}_2 \to \mathsf{M}_2$ est de la forme

$$\Phi_1 + \Phi_2 \circ T, \tag{3.2}$$

où T est la transposition et Φ_1, Φ_2 sont complètement positives.

Notons $\mathcal{P}$ le cône des applications positives sur M_2. Il suffit de démontrer le résultat lorsque Φ est dans l'intérieur de $\mathcal{P}$. Admettons provisoirement le lemme suivant, où l'on note $\Phi_A(X) = AXA^\dagger$ (il est très facile de vérifier que l'application Φ_A est complètement positive).

Lemme 3.2.1 ([A1])**.** *Si $\Phi \in \mathrm{int}(\mathcal{P})$, il existe $A, B \in \mathrm{int}(\mathcal{PSD}_2)$ tels que l'application positive $\Phi_A \circ \Phi \circ \Phi_B$ soit unitale et préserve la trace.*

Grâce au lemme, il suffit de montrer le Théorème 2.2.2 lorsque Φ est positive, unitale et préserve la trace. Une application $\Phi : \mathsf{M}_2 \to \mathsf{M}_2$ qui préserve la trace induit une application affine $\tilde{\Phi} : V_2 \to V_2$. On vérifie aisément que Φ est unitale si et seulement si $\tilde{\Phi}$ est linéaire. Rappelons que D_2

s'identifie à une boule euclidienne de dimension 3 (la boule de Bloch). La contrainte de positivité $\Phi(\mathrm{D}_2) \subset \mathrm{D}_2$ se traduit alors en l'hypothèse que $\tilde{\Phi}$ est une contraction pour la norme euclidienne.

Déterminons maintenant quelles sont les isométries linéaires de V_2. On vérifie facilement que les isométries directes sont de la forme Φ_U pour $U \in \mathsf{U}(2)$, tandis que la transposition (qui laisse invariant un sous-espace de dimension 2, celui des matrices à coefficients réels) est une isométrie indirecte de V_2. La forme générale d'une isométrie indirecte est donc $\Phi_U \circ T$. On utilise pour conclure un fait classique : toute contraction d'un espace euclidien s'écrit comme combinaison convexe de transformations orthogonales. Cette décomposition donne exactement l'écriture (3.2).

Démontrons maintenant le Lemme 3.2.1. Les équations que doivent satisfaire A et B sont $A\Phi(B^2)A = \mathrm{I}$ et $B\Phi^*(A^2)B = \mathrm{I}$, où Φ^* est l'adjoint de Φ. Dès que $X \in \mathrm{int}(\mathcal{PSD}_2)$ est un point fixe pour la fonction

$$f : X \mapsto \Phi\left(\Phi^*(X)^{-1}\right)^{-1}, \tag{3.3}$$

une solution valable est $A = X^{1/2}$, $B = \Phi^*(X)^{-1/2}$. (L'hypothèse $\Phi \in \mathrm{int}(\mathcal{P})$ garantit que f est bien définie). Il reste à justifier que f admet toujours un point fixe : cela peut se faire en appliquant le théorème de Brouwer sur la boule de Bloch à la fonction $X \mapsto \frac{f(X)}{\mathrm{Tr}\, f(X)}$.

3.3 Géométrie de l'ensemble des états séparables

On note $\mathrm{Sep}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ l'ensemble des états séparables sur $\mathcal{H}_1 \otimes \mathcal{H}_2$. On note également $\mathrm{Sep}_{d\otimes d} = \mathrm{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$, de même que l'on écrira $\mathrm{D}_{d\otimes d}$ pour $\mathrm{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$. Comme la structure de produit tensoriel n'intervient pas dans la définition d'un état, on peut identifier $\mathrm{D}_{d\otimes d}$ et D_{d^2}. Notons également $V_{d\otimes d}$ l'espace des opérateurs auto-adjoints de trace 1 sur $\mathbb{C}^d \otimes \mathbb{C}^d$, considéré comme espace euclidien avec l'état maximalement mélangé comme origine.

On a évidemment $\mathrm{Sep}_{d\otimes d} \subset \mathrm{D}_{d\otimes d}$ et un raisonnement simple montre que ces deux ensembles ont même dimension : ce sont des corps convexes dans $V_{d\otimes d}$. Les points extrémaux de $\mathrm{Sep}_{d\otimes d}$ sont le sous-ensemble des points extrémaux de $\mathrm{D}_{d\otimes d}$ formé des projecteurs orthogonaux de rang 1 dont l'image est engendrée par un vecteur produit de $\mathbb{C}^d \otimes \mathbb{C}^d$. Géométriquement, cet ensemble s'identifie à la variété projective de Segré, qui est de mesure nulle dans l'espace projectif sur $\mathbb{C}^d \otimes \mathbb{C}^d$.

La géométrie de $\mathrm{Sep}_{d\otimes d}$ est beaucoup plus compliquée que celle de $\mathrm{D}_{d\otimes d}$. Par exemple, on ne connaît pas de description de la structure faciale de $\mathrm{Sep}_{d\otimes d}$. Une intuition approximative de la géométrie de $\mathrm{Sep}_{d\otimes d}$ est donnée

par l'expérience de pensée suivante : à quoi ressemble l'enveloppe convexe de la sous-variété de dimension 1 formée par la ligne de couture d'une balle de tennis ?

Dans la suite de ce chapitre, nous allons donner des ordres de grandeur pour les différents invariants géométriques introduits au Chapitre 1, à la fois pour D_n, ce qui est relativement simple, et pour $\mathrm{Sep}_{d\otimes d}$, ce qui est plus ardu.

3.4 Volumes et largeur moyenne

Intéressons d'abord aux grandeurs extensives : rayons interne et externe, rayon volumique, largeur moyenne. Les estimations que nous avons obtenues pour D_n, pour $\mathrm{Sep}_{d\otimes d}$ et pour leurs polaires sont réunies dans la Table 3.1.

TABLE 3.1 – [A21, A8] Différents rayons pour les ensembles D_n et $\mathrm{Sep}_{d\otimes d}$. Dans la dernière ligne on a noté $n = d^2 = \dim(\mathbb{C}^d \otimes \mathbb{C}^d)$. Au sein de chaque ligne, les quantités sont dans l'ordre croissant de gauche à droite. Rappelons l'interprétation qui découle du Théorème de Dvoretzky–Milman : $w(K)$ est le rayon d'une projection typique de K, et $w(K^\circ)^{-1}$ est le rayon d'une section typique de K.

K	$r_{\mathrm{int}}(K)$	$w(K^\circ)^{-1}$	$\mathrm{vrad}(K)$	$w(K)$	$r_{\mathrm{ext}}(K)$
D_n	$\frac{1}{\sqrt{n(n-1)}}$	$\sim \frac{1}{2\sqrt{n}}$	$\sim \frac{\exp(-1/4)}{\sqrt{n}}$	$\sim \frac{2}{\sqrt{n}}$	$\sqrt{\frac{n-1}{n}}$
$\mathrm{Sep}_{d\otimes d}$	$\frac{1}{\sqrt{n(n-1)}}$	$\begin{matrix} O\left(n^{-3/4}\right) \\ \Omega(n^{-3/4}/\log n) \end{matrix}$	$\Theta\left(n^{-3/4}\right)$	$\Theta\left(n^{-3/4}\right)$	$\sqrt{\frac{n-1}{n}}$

Certaines valeurs sont triviales à obtenir : c'est le cas par exemple pour les rayons interne et externe de D_n, qui ont les mêmes valeurs que pour l'analogue commutatif, le simplexe régulier de dimension $n-1$ plongé dans $\mathbb{R}^n$. Comme le rayon externe est atteint sur les points extrémaux, on en déduit immédiatement que $r_{\mathrm{ext}}(\mathrm{D}_{d\otimes d}) = r_{\mathrm{ext}}(\mathrm{Sep}_{d\otimes d})$. L'égalité $r_{\mathrm{int}}(\mathrm{D}_{d\otimes d}) = r_{\mathrm{int}}(\mathrm{Sep}_{d\otimes d})$ est plus surprenante : il s'agit d'un théorème dû à Gurvits et Barnum [14]. Nous en donnons une preuve différente dans [A1], basée sur le lemme suivant :

Lemme 3.4.1. *Si une application linéaire A sur $\mathbb{C}^d \otimes \mathbb{C}^d$ est auto-adjointe et vérifie $\langle x\otimes y|A|x\otimes y\rangle \geqslant 0$ pour tous $x, y \in \mathbb{C}^d$, alors $\mathrm{Tr}(A^2) \leqslant (\mathrm{Tr}\, A)^2$.*

Si $A \in \mathsf{M}_n$ est une matrice hermitienne de trace nulle, alors $w(\mathrm{D}_n, A)$ coïncide avec la plus grande valeur propre de A. Il n'est alors pas très difficile

de calculer la largeur moyenne de D_n en utilisant le théorème de Wigner : après normalisation, le spectre des matrices aléatoires choisies uniformément sur la sphère-unité de V_n converge fortement pour n tendant vers l'infini vers la loi du demi-cercle, à support dans $[-2, 2]$.

Ces considérations sont également valables pour l'ensemble polaire D_n° grâce à la relation d'autopolarité $\mathrm{D}_n^\circ = -n \bullet \mathrm{D}_n$. En particulier, le produit $w(\mathrm{D}_n)w(\mathrm{D}_n^\circ)$ est de l'ordre de 4. Au vu de la remarque à la fin du Chapitre 1.3, on a donc le phénomène suivant : les projections génériques et les sections génériques de D_n sont presque euclidiennes, et les projections sont 4 fois plus grandes que les sections.

Comme il semble hors de portée d'obtenir des estimations aussi précises pour $\mathrm{Sep}_{d\otimes d}$, nous allons nous contenter d'ordres de grandeurs. Puisque $\mathrm{Sep}_{d\otimes d}$ est défini par ses points extrémaux, la largeur $w(\mathrm{Sep}_{d\otimes d}, \cdot)$ peut s'écrire naturellement comme un supremum. Ainsi, un argument standard de discrétisation, combiné avec le Corollaire 1.1.2, permet de donner la borne supérieure $\mathrm{vrad}(\mathrm{Sep}_{d\otimes d}) \leqslant w(\mathrm{Sep}_{d\otimes d}) \leqslant Cd^{-3/2}$, et cette borne supérieure est en fait précise à la fois pour la largeur moyenne et pour le rayon volumique.

En revanche, on ne dispose pas d'outil permettant d'estimer directement $w(\mathrm{Sep}_{d\otimes d}^\circ)$. Cette difficulté peut être reliée au fait que ce nombre est la moyenne d'une quantité (la jauge de $\mathrm{Sep}_{d\otimes d}$) qui est algorithmiquement difficile à évaluer ; on reviendra sur ce point au Chapitre 4.2.

Nous suivons dans [A8] une route indirecte, par un argument de dualité qui exploite le fait que le produit $w(\mathrm{Sep}_{d\otimes d})w(\mathrm{Sep}_{d\otimes d}^\circ)$ est borné comme conséquence de l'inégalité MM^*. Cette approche mène au but, mais ce n'est pas immédiat car il y a deux obstacles empêchant d'appliquer directement le Théorème 1.3.1. Premièrement, $\mathrm{Sep}_{d\otimes d}$ n'est pas symétrique. On parvient à contourner cette difficulté en considérant une version symétrisée et en contrôlant l'impact de la procédure de symétrisation. Deuxièmement, comme le groupe des isométries de $\mathrm{Sep}_{d\otimes d}$ (ou de son symétrisé) n'agit pas irréductiblement, on n'a pas immédiatement l'inégalité MM^* pour le corps convexe symétrisé, mais seulement pour une de ses images linéaires. Une analyse détaillée des contributions des différents sous-espaces invariants permet néanmoins de conclure.

3.5 Dimension en sommets et dimension en facettes

Intéressons-nous maintenant aux paramètres qui mesurent la complexité et qui interviennent dans l'inégalité de Figiel–Lindenstrauss–Milman. Il n'est

pas très difficile de se convaincre que D_n et $\mathrm{Sep}_{d\otimes d}$ ont suffisamment de symétries pour que $a(\cdot) = r_{\mathrm{ext}}(\cdot)/r_{\mathrm{int}}(\cdot)$, de sorte que la valeur exacte de l'asphéricité se calcule à partir de la Table 3.1.

TABLE 3.2 – [A2] Dimension en sommets, dimension en facettes et asphéricité pour les ensembles D_n et $\mathrm{Sep}_{d\otimes d}$.

K	$\dim(K)$	$\dim_V(K)$	$\dim_F(K)$	$a(K)$
D_n	n^2-1	$\Theta(n)$	$\Theta(n)$	$n-1$
$\mathrm{Sep}_{d\otimes d}$	d^4-1	$\Theta(d\log d)$	$\Omega(d^3/\log d)$	d^2-1

Puisque les ensembles D_n et $\mathrm{Sep}_{d\otimes d}$ sont définis comme étant des enveloppes convexes, une stratégie naturelle pour obtenir une borne supérieure sur leur dimension en sommets est de les approximer par l'enveloppe convexe d'un ε-réseau de l'ensemble de leurs points extrémaux, pour ε bien choisi. Les points extrémaux de D_n sont les projecteurs orthogonaux de rang 1, et ce polytope peut donc être engendré à partir d'un ε-réseau de la sphère.

Mais cette approche rencontre une difficulté insoupçonnée : tous les ε-réseaux de la sphère ne se valent pas ! L'utilisation de « mauvais » réseaux nécessite de prendre ε tendant vers 0 avec la dimension, et donne les bornes supérieures $\dim_V(\mathrm{D}_n) \leqslant Cn\log n$ et $\dim_F(\mathrm{Sep}_{d\otimes d}) \leqslant Cd\log d$ faisant intervenir un facteur logarithmique. Une difficulté est que les points d'un réseau peuvent « conspirer » pour éviter des gros sous-ensembles : par exemple il se peut qu'un ε-réseau n'intersecte pas le ε-voisinage ouvert d'un équateur, bien que ce dernier couvre quasiment toute la sphère en termes de volume.

Si ce facteur logarithmique est inévitable pour $\mathrm{Sep}_{d\otimes d}$, il peut être supprimé pour D_n. Afin de se prémunir contre de telles conspirations, nous utilisons à nouveau la méthode probabiliste en choisissant comme ε-réseau un ensemble *aléatoire*. Si on sait depuis Rogers que les problèmes de recouvrement par des calottes sphériques se prêtent bien à la méthode probabiliste, notre analyse est novatrice et utilise des outils inhabituels dans ce contexte, comme les inégalités de Hoeffding non commutatives [A2].

Il reste enfin à justifier la borne inférieure sur la dimension en facettes de $\mathrm{Sep}_{d\otimes d}$: c'est en fait une conséquence immédiate de l'inégalité de Figiel–Lindenstrauss–Milman ! Notons également que la borne supérieure

$$\dim_F(\mathrm{Sep}_{d\otimes d}) \leqslant Cd^4$$

découle d'arguments généraux. Je conjecture que cette borne supérieure

donne le bon ordre de grandeur.

Chapitre 4

Phénomènes de grande dimension en théorie quantique de l'information

Ce chapitre est le cœur de ce mémoire. Comme annoncé, on démontre des théorèmes en théorie quantique de l'information comme conséquences des résultats des chapitres précédents. On explique en particulier comment l'exemple dû à Hastings de canaux quantiques pour lesquels il y a non-additivité de la capacité classique peut être revisité à l'aide du théorème de Dvoretzky–Milman. On démontre également une borne inférieure sur l'efficacité de la détection d'intrication à l'aide de témoins, grâce au concept de dimension en facettes. Enfin, on obtient deux résultats sur l'approximation parcimonieuse : un pour les canaux mélangeants, à l'aide de méthodes de processus empiriques dans les espaces de Banach, et un pour les mesures quantiques, en établissant un lien entre zonoïdes et POVMs.

4.1 Non-additivité de la capacité

Une branche de la théorie quantique de l'information, que l'on pourrait appeler la théorie de Shannon quantique, cherche à quantifier la quantité d'information (classique ou quantique) qui peut être véhiculée par un canal quantique. Il s'agit d'étendre au cadre quantique des résultats connus depuis les travaux pionniers de Shannon en théorie de l'information [35].

Expliquons brièvement un résultat fondamental connu sous le nom de *deuxième théorème de Shannon*. Soient I et J deux ensemble finis, et $C : I \to J$ un *canal classique*, c'est-à-dire la donnée pour tout $i \in I$ d'une mesure de

probabilité sur J décrivant la loi de $C(i)$. Shannon nous a légué une formule pour le taux d'information (c'est-à-dire, le nombre de bits par utilisation du canal) que l'on peut faire transiter par ce canal, dans l'asymptotique d'un grand nombre d'utilisations du canal et d'un taux d'erreur tendant vers 0. Cette formule simple fait intervenir l'information mutuelle entre l'entrée et la sortie du canal.

Il a été démontré à la fin du XX$^{\text{e}}$ siècle par Holevo [19] et Schumacher–Westmoreland [34] que les arguments de Shannon [1] peuvent s'étendre au contexte quantique et donner une formule similaire, faisant intervenir l'information mutuelle quantique, pour la capacité d'un canal *quantique* à transmettre de l'information classique. Il y a toutefois une restriction : cette formule suppose que les états quantiques utilisés pour encoder l'information *ne sont pas intriqués* entre les différentes utilisations du canal.

Savoir si cette restriction en est réellement une, ou autrement dit si le recours à l'intrication permet d'augmenter la capacité des canaux quantiques, a été l'une des principales questions ouvertes, connue sous le nom de *problème de l'additivité*, en théorie quantique de l'information [2]. On connaît depuis Shor [36] une formulation équivalente plus simple à énoncer. Si $\Phi : \mathsf{M}_m \to \mathsf{M}_k$ est un canal quantique, on définit son *entropie minimale de sortie* comme

$$S^{\min}(\Phi) = \min\{S(\Phi(\rho)) \,:\, \rho \in \mathrm{D}_m\}$$

où $S(\sigma) = -\operatorname{Tr}(\sigma \log \sigma)$ est l'entropie de von Neumann d'un état σ. Le problème de l'additivité est alors équivalent à la validité de la relation

$$S^{\min}(\Phi \otimes \Psi) = S^{\min}(\Phi) + S^{\min}(\Psi) \tag{4.1}$$

pour tous les canaux quantiques Φ et Ψ.

Un contre-exemple à (4.1) a été obtenu par Hastings [15], à nouveau à l'aide de la méthode probabiliste. Ma contribution a été, en collaboration avec Stanisław Szarek et Elisabeth Werner [A13], de montrer que l'argument de Hastings peut être grandement simplifié en appliquant le théorème de Dvoretzky–Milman d'une manière adéquate. D'autres approches ont été développées ultérieurement [2, 6]. Notons aussi, comme nous l'avions remarqué dans [A14], que les contre-exemples obtenus antérieurement [18] à une version de la conjecture d'additivité pour la p-entropie de Rényi ($p > 1$)

1. Notons au passage que la preuve de Shannon [35] est une utilisation élégante de la méthode probabiliste, et est contemporaine des résultats combinatoires de Erdős pour lesquels on lui attribue traditionnellement la paternité de la méthode.

2. L'exposé de Holevo au congrès international des mathématiciens de 2006 [20] est consacré à cette seule question !

peuvent aussi être obtenus comme conséquence très directe du théorème de Dvoretzky–Milman.

Tous les contre-exemples connus à la conjecture d'additivité sont basés sur la remarque suivante : on dispose d'une borne supérieure sur $S^{\min}(\Phi \otimes \overline{\Phi})$ en prenant pour état d'entrée un état maximalement intriqué (on désigne par $\overline{\Phi}$ le canal quantique obtenu à partir de Φ par conjugaison complexe) puisque l'état de sortie possède alors une grande valeur propre (supérieure à $\frac{m}{kd}$, dans la notation de la Proposition 4.1.1). Il reste à obtenir des exemples de canaux quantiques pour lesquels l'entropie minimale de sortie est presque maximale. On peut alors voir par un calcul élémentaire que si Φ vérifie la conclusion de la proposition suivante, alors pour k assez grand le couple $(\Phi, \overline{\Phi})$ est un contre-exemple à (4.1).

Proposition 4.1.1 ([A13])**.** *Soit un entier k, et posons $m = \lfloor ck^2 \rfloor$ et $d = k^2$. Alors il existe une isométrie $U : \mathbb{C}^m \to \mathbb{C}^k \otimes \mathbb{C}^d$ telle que le canal quantique Φ défini par*

$$\Phi(X) = (\mathrm{Id} \otimes \mathrm{Tr})(UXU^\dagger). \tag{4.2}$$

vérifie

$$\log k - \frac{C}{k} \leqslant S_{\min}(\Phi) \leqslant \log k. \tag{4.3}$$

Tout le contenu de la Proposition 4.1.1 réside dans la borne inférieure de (4.3). La borne supérieure, triviale, est indiquée à titre de comparaison.

La représentation de Stinespring (4.2) donne un modèle naturel de canal quantique aléatoire : il suffit de considérer une isométrie aléatoire $U : \mathbb{C}^m \to \mathbb{C}^k \otimes \mathbb{C}^d$ choisie selon la mesure de Haar. Notons E l'image de U, de sorte que E est un sous-espace aléatoire distribué selon la mesure de Haar sur la grassmannienne $\mathsf{Gr}(m, \mathbb{C}^k \otimes \mathbb{C}^d)$. Introduisons la fonction f définie sur $S_{\mathbb{C}^k \otimes \mathbb{C}^d}$ par

$$f(x) = S\left(\mathrm{Id} \otimes \mathrm{Tr}\, |x\rangle\langle x|\right).$$

La conclusion de la Proposition 4.1.1 se reformule comme

$$\inf\left\{ f(x) \,:\, x \in E \cap S_{\mathbb{C}^k \otimes \mathbb{C}^d} \right\} \geqslant \log k - \frac{C}{k}.$$

On souhaiterait montrer qu'une fonction définie sur la sphère oscille peu sur une sous-sphère typique : c'est exactement la conclusion du théorème de Dvoretzky–Milman. Néanmoins, deux ajustements sont nécessaires pour pouvoir déduire la Proposition 4.1.1 du Théorème 1.2.3. D'abord, puisque l'on s'intéresse à des valeurs de l'entropie de von Neumann proches de la

valeur maximale $\log k$ sur D_k, il est naturel de remplacer f par son approximation de Taylor : on a pour $x \in S_{\mathbb{C}^k \otimes \mathbb{C}^d}$,

$$f(x) \geqslant \log k - k \left\| \mathrm{Id} \otimes \mathrm{Tr}\, |x\rangle\langle x| - \frac{\mathrm{I}}{k} \right\|_2^2 .$$

On va appliquer le théorème de Dvoretzky–Milman à la fonction

$$g : x \mapsto \left\| \mathrm{Id} \otimes \mathrm{Tr}\, |x\rangle\langle x| - \frac{\mathrm{I}}{k} \right\|_2 .$$

La constante de Lipschitz locale de cette fonction en un point $x \in S_{\mathbb{C}^k \otimes \mathbb{C}^d}$ est contrôlée par la norme d'opérateur, notée $N(x)$, de l'état $\mathrm{Id} \otimes \mathrm{Tr}\, |x\rangle\langle x|$. Des considérations élémentaires sur les matrices de Wishart permettent d'affirmer que la valeur typique de N est bien plus petite que sa valeur maximale : ceci est relié au principe général selon lequel les matrices aléatoires ont tendance à avoir un spectre homogène, où toutes les valeurs propres ont le même ordre de grandeur. On peut alors conclure en appliquant *deux fois* le théorème de Dvoretzky–Milman : une première fois à la fonction N, et une deuxième fois à une fonction $\tilde{g}$ obtenue en modifiant artificiellement la fonction g là où N est grande, de sorte que la constante de Lipschitz de $\tilde{g}$ soit substantiellement plus petite que celle de g. Nous tirons ici profit de la souplesse de la méthode probabiliste, qui permet d'affirmer sans effort supplémentaire que le phénomène de concentration de la mesure a lieu simultanément pour deux fonctions à la fois.

4.2 Complexité de l'intrication

Au vu de l'importance de l'intrication dans les protocoles de la théorie quantique de l'information, un problème fondamental est de décider si un état donné est intriqué ou séparable. Un résultat souvent cité dû à Gurvits [13] affirme que « c'est NP-difficile ». Néanmoins cette formulation un peu lapidaire mérite d'être précisée. Pour y parvenir, considérons la jauge j de l'ensemble $\mathrm{Sep}_{d \otimes d}$, de sorte qu'un état ρ est séparable si et seulement si $j(\rho) \leqslant 1$. Le résultat de Gurvits, raffiné par Gharibian [11], est le suivant : sous la promesse qu'un état ρ vérifie ou bien $j(\rho) \leqslant 1$ ou bien $j(\rho) \geqslant 1+1/d^C$, il est NP-difficile de décider cette alternative.

Cela montre que l'ensemble $\mathrm{Sep}_{d \otimes d}$ est complexe, mais potentiellement à cause de sa frontière ; il serait intéressant de savoir si la complexité persiste au cœur de l'ensemble, par exemple en montrant qu'un résultat analogue

reste vrai sous la promesse $j(\rho) \leqslant 1$ vs $j(\rho) \geqslant 2$. Remarquons que la condition $j(\rho) \geqslant 2$ a un sens physique : elle décrit les états ρ tels que $\frac{1}{2}(\rho + \rho_*)$ est intriqué, autrement dit les états qui demeurent intriqués même en présence de bruit dépolarisant. Nous obtenons dans [A2] un résultat dans cette direction, pour un modèle de complexité spécifique où l'on est autorisé à détecter l'intrication uniquement à l'aide de témoins.

Théorème 4.2.1 ([A2])**.** *Supposons qu'une famille $(\Phi_i)_{1 \leqslant i \leqslant N}$ d'applications positives sur M_d ait la propriété suivante : pour tout état $\rho \in \mathrm{D}_{d \otimes d}$ vérifiant $j(\rho) \geqslant 2$, il existe i tel que Φ_i est un témoin d'intrication pour ρ. Alors*

$$N + 1 \geqslant \exp(cd^3 / \log d).$$

On peut également obtenir des variantes montrant que même la détection d'états extrêmement intriqués est coûteuse : si l'hypothèse « $j(\rho) \geqslant 2$ » est remplacée par « $j(\rho) \geqslant C\sqrt{d}/\log(d)$ », la conclusion devient « $N + 1 \geqslant \exp(cd^2 \log d)$ ».

Nous allons esquisser les grandes lignes de la preuve du Théorème 4.2.1, qui repose sur le concept de dimension en facettes, et utilise les valeurs de la Table 3.2. Supposons que $(\Phi_i)_{1 \leqslant i \leqslant N}$ est une famille d'applications positives sur M_d vérifiant la condition du Théorème 4.2.1. Cela peut se reformuler comme suit

$$\mathrm{Sep}_{d \otimes d} \subset \bigcap_{i=0}^{N} (\Phi_i \otimes \mathrm{Id})^{-1}(\mathrm{D}_{d \otimes d}) \subset 2 \bullet \mathrm{Sep}_{d \otimes d},$$

où l'on a noté $\Phi_0 = \mathrm{Id}$.

Pour simplifier la présentation, faisons des hypothèses supplémentaires sur les applications Φ_i en supposant qu'elles sont inversibles, unitales et préservent la trace (le cas général introduit des complications techniques qui obscurcissent les idées essentielles). On peut alors voir $\Phi_i \otimes \mathrm{Id}$ comme une application linéaire inversible sur l'espace euclidien $V_{d \otimes d}$. On utilise alors deux propriétés élémentaires de la dimension en facettes. La première est l'invariance linéaire : si K est un corps convexe et T une application linéaire inversible, alors $\dim_F(TK) = \dim_F(K)$. La seconde découle de la sous-additivité du nombre de facettes par intersection : si (K_i) sont des corps convexes, on a

$$\dim_F (K_0 \cap \cdots \cap K_N) \leqslant \log \sum_{i=0}^{N} \exp(\dim_F(K_i)). \tag{4.4}$$

On applique l'inégalité (4.4) à $K_i = (\Phi_i \otimes \mathrm{Id})^{-1}(\mathrm{D}_{d\otimes d})$ pour conclure que

$$\dim_F(\mathrm{Sep}_{d\otimes d}) \leqslant \log(N+1) + \dim'_F(\mathrm{D}_{d\otimes d}),$$

où $\dim'_F$ dénote une variante de la dimension en facettes où le facteur d'homothétie utilisé dans la définition est 2 au lieu de 4. On conclut la preuve en utilisant les estimations de la Table 3.2, qui sont aussi valables pour $\dim'_F$ (le choix du facteur d'homothétie n'influe qu'à travers les valeurs des constantes).

4.3 Canaux mélangeants

Un exemple important de canal quantique est le canal *complètement mélangeant* $R : \mathsf{M}_d \to \mathsf{M}_d$, que l'on peut définir par

$$R(X) = \int_{\mathsf{U}(d)} UXU^\dagger \,\mathrm{d}\mathbf{P}(U) \tag{4.5}$$

où $\mathbf{P}$ désigne la mesure de probabilité de Haar sur le groupe unitaire $\mathsf{U}(d)$. Il découle facilement de l'invariance par translation de la mesure de Haar que l'opérateur $R(X)$ doit commuter avec $\mathsf{U}(d)$, d'où l'on tire la relation $R(X) = \mathrm{Tr}(X)\rho_*$: le canal complètement mélangeant envoie tout état sur l'état maximalement mélangé $\rho_* = \mathrm{I}/d$. On vérifie que le rang de Kraus de R, tel que défini dans au Chapitre 2.4, est égal à la valeur maximale d^2.

La relation (4.5) est loin de caractériser la mesure de Haar puisque cette dernière n'intervient qu'à travers les covariances. On dira qu'une mesure de probabilité μ sur $\mathsf{U}(d)$ est *isotrope* si elle vérifie la condition

$$R(X) = \int_{\mathsf{U}(d)} UXU^\dagger \,\mathrm{d}\mu(U), \tag{4.6}$$

ou de manière équivalente si $\int |\operatorname{Tr} UX|^2 \,\mathrm{d}\mu(U) = \frac{1}{d}\|X\|_2^2$ pour tout $X \in \mathsf{M}_d$.

Soit G un sous-groupe de $\mathsf{U}(d)$ qui engendre M_d en tant qu'espace vectoriel. Le même argument que précédemment montre que la mesure de Haar sur G est isotrope. Toute mesure isotrope à support fini donne une décomposition de Kraus de R, et on peut en obtenir une de longueur minimale d^2 en prenant pour G le groupe engendré par les matrices A et B définies par $Ae_j = e_{j+1}$ (addition modulo d) et $Be_j = \exp(2i\pi j/d)e_j$, où $(e_1, \ldots, e_d)$ est la base canonique de $\mathbb{C}^d$. Un autre exemple très important est donné par les matrices de Pauli : lorsque $d = 2^k$ et que l'on identifie $\mathbb{C}^d$ à $(\mathbb{C}^2)^{\otimes k}$, ce sont

les $d^2 = 4^k$ matrices de la forme $\sigma_{i_1} \otimes \cdots \otimes \sigma_{i_k}$, où $i_1, \ldots, i_k \in \{0, X, Y, Z\}$ et

$$\sigma_0 = \mathrm{I}, \quad \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.7}$$

Il se trouve qu'il est possible d'approximer le canal complètement mélangeant par des canaux de rang de Kraus beaucoup plus petit. Soit $\varepsilon \in [0, 1]$. On dira qu'un canal quantique $\Phi : \mathsf{M}_d \to \mathsf{M}_d$ est *ε-mélangeant* si pour tout état ρ sur $\mathbb{C}^d$, on a $\|\Phi(\rho) - \rho_*\|_\infty \leqslant \varepsilon/d$.

Cette propriété a été exploitée dans [16] pour des applications à la dissimulation de données en théorie quantique d'information. L'idée naturelle pour obtenir un canal ε-mélangeant est d'échantillonner la mesure de Haar. J'ai obtenu le résultat suivant, améliorant les résultat de [16].

Théorème 4.3.1 ([A16])**.** *Soit $\varepsilon \in (0, 1)$. Soient $(U_i)_{1 \leqslant i \leqslant N}$ des éléments de $\mathsf{U}(d)$ choisis indépendamment selon la mesure de Haar, pour $N \geqslant Cd/\varepsilon^2$. Alors le canal quantique*

$$X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^\dagger$$

est ε-mélangeant avec grande probabilité.

La dépendance en la dimension est optimale (il est très facile de voir qu'un canal ε-mélangeant a un rang de Kraus au moins d) et la dépendance en ε est également optimale pour des canaux aléatoires. La preuve du Théorème 4.3.1 est relativement simple : puisque la mesure de Haar est sous-gaussienne, on peut utiliser un argument de discrétisation en utilisant un δ-réseau de la sphère-unité de $\mathbb{C}^d$ (par exemple $\delta = 1/4$ convient).

On ne connaît pas d'exemple explicite de canal ε-mélangeant avec un petit rang de Kraus. Le résultat suivant peut être vu comme une étape dans cette direction : on remplace la mesure de Haar par une mesure moins coûteuse à simuler en nombre de bits aléatoires. Il montre qu'on obtient un canal ε-mélangeant en échantillonnant n'importe quelle mesure isotrope.

Théorème 4.3.2 ([A16])**.** *Soit $\varepsilon \in (0, 1)$. Soit μ une mesure isotrope sur $\mathsf{U}(d)$, et $(U_i)_{1 \leqslant i \leqslant N}$ i.i.d. de loi μ pour $N \geqslant Cd \log^6 d/\varepsilon^2$. Alors le canal quantique*

$$X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^\dagger$$

est ε-mélangeant avec grande probabilité.

En particulier, le Théorème 4.3.2 s'applique aux matrices de Pauli (4.7), ce qui est important pour certaines applications. La preuve du Théorème 4.3.2 est considérablement plus complexe que celle du Théorème 4.3.1 : en effet, on n'est plus dans le cadre sous-gaussien. Elle repose sur des méthodes de processus empiriques dans les espaces de Banach inspirées de celles de [12]. On utilise également des estimations de nombres d'entropie ; notons qu'une solution positive à la conjecture de dualité des nombres d'entropie permettrait d'améliorer l'estimation en $N \geqslant Cd \log^4 d/\varepsilon^2$. Remarquons également que cette approche a été reprise par Liu [26] pour montrer que les matrices de Pauli vérifient la propriété d'isométrie restreinte, fondamentale pour l'acquisition comprimée («compressed sensing»).

4.4 Mesures quantiques parcimonieuses

Un autre résultat concerne l'élagage des mesures quantiques. Une mesure quantique est modélisée par un *POVM* (Positive Operator-Valued Measure), qui est une mesure vectorielle $\mathrm{M} : (\Omega, \mathcal{F}) \to \mathcal{PSD}_d$ vérifiant $\mathrm{M}(\Omega) = \mathrm{I}$, où $(\Omega, \mathcal{F})$ est un espace mesurable. Nous nous intéressons au problème de la discrimination entre états : un système quantique est préparé dans un état quantique qui est ou bien ρ ou bien σ (avec équiprobabilité a priori) et on souhaite déterminer lequel en le mesurant à l'aide de M. La probabilité d'erreur est alors

$$p_{\text{erreur}} = \frac{1}{2} - \frac{1}{4}\|\rho - \sigma\|_{\mathrm{M}},$$

où $\|\cdot\|_{\mathrm{M}}$ est la semi-norme associée à M, définie pour $\Delta \in \mathsf{M}_d^{\mathrm{sa}}$ par

$$\|\Delta\|_{\mathrm{M}} = \sup_{A \in \mathcal{F}} \left[\mathrm{Tr}(\Delta \mathrm{M}(A)) - \mathrm{Tr}(\Delta \mathrm{M}(A^c))\right].$$

Cette définition prend une forme plus simple dans le cas où la mesure vectorielle prend un nombre fini de valeurs : un POVM revient alors à la donnée d'une famille finie d'opérateurs positifs $\mathrm{M} = (M_1, \ldots, M_n)$ vérifiant $M_1 + \cdots + M_n = \mathrm{I}$, et on a

$$\|\Delta\|_{\mathrm{M}} = \sum_{i=1}^{n} |\operatorname{Tr} \Delta M_i|.$$

La proposition suivante, très simple, permet de lier POVMs et sous-espaces de L^1.

Proposition 4.4.1 ([A5])**.** *Soit $\|\cdot\|$ une norme sur $\mathsf{M}_d^{\mathrm{sa}}$. On a équivalence entre les deux énoncés suivants.*

1. *Il existe un POVM* M *tel que* $\|\cdot\| = \|\cdot\|_{\mathrm{M}}$.
2. *On a les trois conditions*
   (a) *l'espace normé* $(\mathsf{M}_d^{\mathrm{sa}}, \|\cdot\|)$ *est isométrique à un sous-espace de* L^1,
   (b) $\|\cdot\| \leqslant \|\cdot\|_1$,
   (c) $\|\mathrm{I}\| = d$.

La condition (a) se reformule en disant que l'ensemble polaire de la boule-unité pour $\|\cdot\|_{\mathrm{M}}$ est un zonoïde. Pour un POVM discret $(M_1, \ldots, M_n)$, c'est simplement le zonotope $[-M_1, M_1] + \cdots + [-M_n, M_n]$. Le lien entre zonoïdes et mesures vectorielles est essentiellement le contenu du théorème de Lyapounov qui affirme que l'ensemble des valeurs prises par une mesure vectorielle sans atome est un zonoïde.

La Proposition 4.4.1 fournit un dictionnaire permettant d'importer les résultats de géométrie des espaces de Banach au cadre des POVMs. On a alors, comme conséquence du Théorème 1.5.1, le théorème suivant sur l'élagage des mesures quantiques.

Théorème 4.4.2 ([A5])**.** *Soit* M *un POVM sur* $\mathbb{C}^d$ *et* $\varepsilon \in (0,1)$*. Alors il existe un POVM discret* $\mathrm{M}' = (M_1, \ldots, M_N)$*, avec* $N \leqslant Cd^2 \log d/\varepsilon^2$*, tel que*

$$\|\cdot\|_{\mathrm{M}'} \geqslant (1-\varepsilon)\|\cdot\|_{\mathrm{M}}. \tag{4.8}$$

On pourrait s'attendre à compléter (4.8) par une inégalité du type

$$\|\cdot\|_{\mathrm{M}'} \leqslant (1+\varepsilon)\|\cdot\|_{\mathrm{M}} \tag{4.9}$$

afin d'obtenir une équivalence entre normes. Il n'est pas évident que cela soit toujours possible, la difficulté étant qu'il faut prendre en considération la contrainte de normalisation imposée par la définition d'un POVM. Notons toutefois que c'est l'inégalité (4.8) qui est pertinente : elle affirme que le POVM élagué est au moins aussi performant que le POVM initial.

La dépendance en la dimension est optimale sauf peut-être pour le facteur logarithmique ; notons que la condition $N \geqslant d^2$ est nécessaire pour que $\|\cdot\|_{\mathrm{M}'}$ soit une norme. Dans certains cas, nous pouvons améliorer le Théorème 4.4.2 en supprimant ce facteur logarithmique et en montrant l'inégalité inverse (4.9) : c'est le cas par exemple pour le POVM construit à partir de la mesure uniforme sur la sphère.

Chapitre 5

États quantiques aléatoires

On a vu au cours des chapitres précédents que les méthodes probabilistes permettent d'éclairer d'un jour nouveau la géométrie des états quantiques de grande dimension. Il est donc naturel de chercher à déterminer les propriétés des *états quantiques aléatoires*. Cette direction de recherche a été initiée par Hayden, Leung et Winter [17]. Ce chapitre résume les travaux que j'ai obtenus dans ce domaine.

5.1 États induits

Il existe une famille extrêmement naturelle de lois de probabilités sur l'ensemble des états quantiques. Une construction est la suivante : fixons $\mathcal{H}$ un espace de Hilbert complexe de dimension finie, et un paramètre $s \in \mathbb{N}^*$. Choisissons un vecteur aléatoire ψ uniformément sur la sphère-unité de l'espace $\mathcal{H} \otimes \mathbb{C}^s$, et considérons l'état sur $\mathcal{H}$ obtenu après trace partielle

$$\rho \coloneqq (\mathrm{Id}_{\mathcal{H}} \otimes \mathrm{Tr}_{\mathbb{C}^s})|\psi\rangle\langle\psi|.$$

On obtient ainsi un état aléatoire sur $\mathcal{H}$, dont la loi est notée $\mathrm{Induit}(\mathcal{H}, s)$. Dans la terminologie des systèmes quantiques ouverts, l'espace $\mathbb{C}^s$ est l'environnement, auquel l'expérimentateur n'a pas accès.

Lorsque $s \geqslant \dim \mathcal{H}$, la loi $\mathrm{Induit}(\mathcal{H}, s)$ a une densité par rapport à la mesure de Lebesgue sur $\mathrm{D}(\mathcal{H})$ qui est proportionnelle à

$$\det(\rho)^{\dim \mathcal{H} - s}.$$

Cette formule, obtenue dans [42], permet alors de définir la loi $\mathrm{Induit}(\mathcal{H}, s)$ si $s > \dim \mathcal{H} - 1$ est un nombre réel non nécessairement entier. Une autre conséquence frappante est la suivante : $\mathrm{Induit}(\mathcal{H}, \dim \mathcal{H})$ est la loi uniforme sur

$\mathrm{D}(\mathcal{H})$. Ce résultat (dont je ne connais pas de preuve conceptuelle) est la version non-commutative du fait classique suivant : si $\psi = (\psi_1, \ldots, \psi_s)$ est choisi uniformément sur la sphère-unité de $\mathbb{C}^s$, alors le vecteur $(|\psi_1|^2, \ldots, |\psi_s|^2)$ est uniformément distribué sur le simplexe.

Les états induits sont fortement liés aux matrices de Wishart : si B est une matrice $n \times s$ à coefficients i.i.d. de loi $N_{\mathbb{C}}(0,1)$, alors l'état quantique

$$\rho = \frac{BB^\dagger}{\operatorname{Tr} BB^\dagger}$$

suit la loi $\mathrm{Induit}(\mathbb{C}^n, s)$. On dit que $BB^\dagger$ est une matrice de Wishart de paramètres (n, s). On ne considérera que des matrices de Wishart à coefficients complexes.

Lorsque s tend vers l'infini, la loi $\mathrm{Induit}(\mathcal{H}, s)$ converge vers l'état maximalement mélangé ρ_*. Dans la suite de ce chapitre, on s'intéressera au cas où $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$. Puisque ρ_* est dans l'intérieur de l'ensemble $\mathrm{Sep}_{d\otimes d}$, on en déduit qu'à d fixé, un état aléatoire de loi $\mathrm{Induit}(\mathbb{C}^d \otimes \mathbb{C}^d, s)$ est séparable avec une probabilité tendant vers 1 lorsque s tend vers l'infini. À l'inverse, un état de loi $\mathrm{Induit}(\mathbb{C}^d \otimes \mathbb{C}^d, 1)$ est presque sûrement intriqué puisque les vecteurs produits forment un ensemble de mesure nulle dans $\mathbb{C}^d \otimes \mathbb{C}^d$.

On s'attend donc à l'existence, pour les états induits, d'une transition de phase entre séparabilité et intrication en fonction de la dimension de l'environnement. Ce phénomène sera décrit par le Théorème 5.4.1. Nous allons auparavant énoncer des résultats analogues pour deux relaxations de la séparabilité vues au Chapitre 2.3 : la transposition partielle et le réalignement. Dans ces deux derniers cas, la transition de phase est connue très exactement. Cela est dû à une reformulation en termes de modèles de matrices aléatoires, pour lesquels on peut démontrer la convergence du spectre. Cette direction de recherche, que j'ai initiée dans [A11], a suscité de nombreux travaux (voir [24] pour un article de synthèse).

5.2 Transition de phase pour la transposition partielle

Commençons par rappeler le résultat classique de Marčenko–Pastur sur le spectre des grandes matrices de Wishart. Il est commode d'utiliser la distance ∞-*Wasserstein* entre deux mesures de probabilités μ et ν sur $\mathbb{R}$, définie par

$$d_\infty(\mu, \nu) = \inf \|X - Y\|_{L^\infty},$$

où l'infimum est pris sur tous les couples (X, Y) de variables aléatoires de lois marginales μ et ν. Si $A \in \mathsf{M}_n^{\mathrm{sa}}$ a pour valeurs propres $\lambda_1, \ldots, \lambda_n$, on définit sa *mesure spectrale empirique* par

$$\mu_{\mathrm{sp}}(A) = \frac{1}{n} \sum_{i=1}^{n} \delta_{\lambda_i}.$$

On a alors

Théorème 5.2.1 (Marčenko–Pastur)**.** *Soit $\alpha \geqslant 1$, et soit (W_k) une suite de matrices aléatoires, W_k suivant une loi de Wishart de paramètres (n_k, s_k). On suppose que les suites (n_k) et (s_k) tendent vers l'infini et que $\lim s_k/n_k = \alpha$. On a alors la convergence en probabilité*

$$\lim_{k\to\infty} d_\infty \left(\mu_{\mathrm{sp}}\left(s_k^{-1} W_k\right), \mu_{\mathrm{MP}(\alpha)}\right) = 0,$$

où $\mu_{\mathrm{MP}(\alpha)}$ est la loi de Marčenko–Pastur de paramètre α, de support

$$\left[\left(1 - \tfrac{1}{\sqrt{\alpha}}\right)^2, \left(1 + \tfrac{1}{\sqrt{\alpha}}\right)^2\right].$$

Faisons deux remarques sur la formulation du Théorème 5.2.1. La première est que la convergence au sens de la distance ∞-Wasserstein équivaut à la conjonction de deux énoncés : la convergence en loi et la convergence des valeurs propres extrêmes vers le bord du support de $\mu_{\mathrm{MP}(\alpha)}$. La seconde est que, dans cette généralité, on ne peut pas avoir de convergence presque sûre : elle est en défaut si les matrices aléatoires (W_k) sont indépendantes et si les suites (n_k) et (s_k) croissent suffisamment lentement. La convergence presque sûre n'est pas une notion naturelle pour nos applications à la théorie quantique de l'information, puisque les différentes matrices ne vivent pas naturellement sur le même espace de probabilité.

Notons au passage l'inégalité suivante qui donne une preuve élégante de la convergence de la plus grande valeur propre des matrices de Wishart.

Proposition 5.2.2. *Si A est une matrice $n \times s$ à coefficients i.i.d. de loi $N_{\mathbb{C}}(0, 1)$, alors $\mathbf{E}\,\|A\|_\infty \leqslant \sqrt{n} + \sqrt{s}$.*

Ce résultat est bien connu pour les matrices de Wishart réelles, comme conséquence du lemme de Slepian sur la comparaison de processus gaussiens. La version complexe est moins facile à démontrer car le lemme de Slepian ne peut pas s'appliquer ; on en donne une preuve dans [A1, Section 6.2.4.2] en la déduisant du cas réel par un argument de couplage. L'inégalité jumelle

$\mathbf{E}\, s_{\min}(A) \geqslant \sqrt{n} - \sqrt{s}$, où $s_{\min}$ désigne la plus petite valeur singulière, semble vraie numériquement, mais je ne sais pas la démontrer.

Que se passe-t-il lorsqu'on applique la transposition partielle à une matrice de Wishart ? On suppose pour cela que les matrices sont de taille $d^2 \times d^2$, et on les identifie à des opérateurs sur $\mathbb{C}^d \otimes \mathbb{C}^d$.

Théorème 5.2.3 ([A11]). *Soit $\alpha > 0$, et soit (W_k) une suite de matrices aléatoires, W_k suivant une loi de Wishart de paramètres (d_k^2, s_k). On suppose que les suites (d_k) et (s_k) tendent vers l'infini et que $\lim s_k/d_k^2 = \alpha$. On a alors la convergence en probabilité*

$$\lim_{k\to\infty} d_\infty \left(\mu_{\mathrm{sp}}(s_k^{-1} W_k^\Gamma), \mathrm{SC}(1, 1/\alpha)\right) = 0,$$

où $\mathrm{SC}(1, 1/\alpha)$ est la loi semi-circulaire de moyenne α et de variance α.

La preuve du Théorème 5.2.3 repose sur l'outil le plus commun pour étudier le spectre des matrices aléatoires : la méthode des moments. Il est relativement simple de montrer la convergence des moments : il suffit pour cela de comprendre les termes dominants, qui ont une interprétation combinatoire à l'aide de partitions non-croisées. En revanche, obtenir la convergence des valeurs propres extrêmes nécessite de contrôler la contribution de tous les termes, ce qui est beaucoup plus laborieux. Les efforts sont récompensés par le corollaire suivant sur les états induits, pour lequel il est vital de connaître le comportement de la plus petite valeur propre. On obtient une dichotomie pour la propriété PPT, selon si la loi $\mathrm{SC}(1, 1/\alpha)$ est à support dans $\mathbb{R}^+$ ou non. La valeur critique est $\alpha = 4$.

Théorème 5.2.4 ([A11]). *Soit ρ un état aléatoire de loi* $\mathrm{Induit}(\mathbb{C}^d \otimes \mathbb{C}^d, s)$, *et $\varepsilon > 0$. Alors*

1. *Si $s \geqslant (4+\varepsilon)d^2$, alors ρ est PPT avec grande probabilité.*
2. *Si $s \leqslant (4-\varepsilon)d^2$, alors ρ est non-PPT avec grande probabilité.*

Par « grande probabilité » on entend ici « probabilité supérieure à $1 - C\exp\left(c(\varepsilon)\max(s, d^2)\right)$ », où $c(\varepsilon) > 0$ est une constante dépendant uniquement de ε. La même remarque s'appliquera aux Théorèmes 5.3.2 et 5.4.1.

5.3 Transition de phase pour le réalignement

On peut appliquer à la propriété de réaligement la même démarche que pour la transposition partielle. On commence par démontrer un résultat de convergence sur les matrices de Wishart réalignées. Comme le réalignement

ne préserve pas le caractère hermitien, il faut considérer les valeurs singulières.

Théorème 5.3.1 ([A9]). *Soit $\alpha > 0$, et soit (W_k) une suite de matrices aléatoires, W_k suivant une loi de Wishart de paramètres (d_k^2, s_k). On suppose que les suites (d_k) et (s_k) tendent vers l'infini. On pose aussi $Y_k = (d_k\sqrt{s_k})^{-1}(W_k - s_k\,\mathrm{I})^R$. Alors on a la convergence en moments, en probabilité*

$$\lim_{k\to\infty} \mu_{\mathrm{sp}}(Y_k Y_k^\dagger) = \mathrm{QC},$$

où QC *est la loi du quart-de-cercle, c'est-à-dire la loi de $|X|$ lorsque X suit une loi* $\mathrm{SC}(0,1)$.

La normalisation utilisée dans le Théorème 5.3.1 diffère de celle du Théorème 5.2.3. La raison est que dans le cas du réalignement, l'application aux états induits ne nécessite pas la convergence des valeurs propres extrêmes (que je n'ai jamais pris la peine de vérifier, le modèle matriciel étant d'un intérêt douteux en dehors du corollaire sur les états induits). En contrepartie, on ne fait aucune hypothèse sur la vitesse relative à laquelle les paramètres de Wishart tendent vers l'infini.

On peut déterminer exactement la valeur critique pour le critère de réalignement.

Théorème 5.3.2 ([A9]). *Posons $\gamma = (8/3\pi)^2$. Soit ρ un état aléatoire de loi* $\mathrm{Induit}(\mathbb{C}^d \otimes \mathbb{C}^d, s)$ *et $\varepsilon > 0$. Alors*

1. *Si $s \geqslant (\gamma + \varepsilon)d^2$, alors ρ est réalignable avec grande probabilité.*
2. *Si $s \leqslant (\gamma - \varepsilon)d^2$, alors ρ est non-réalignable avec grande probabilité.*

Puisque $(8/3\pi)^2 < 4$, une conséquence des Théorèmes 5.2.4 et 5.3.2 est que, pour des états génériques, le critère de réalignement est moins performant que le critère de la transposition partielle. Si par exemple ρ est choisi selon la mesure uniforme sur $\mathrm{D}_{d\otimes d}$, la situation qui prédomine est la suivante : ρ est non-PPT (donc intriqué) mais réalignable.

5.4 Transition de phase pour l'intrication

Au vu des Théorèmes 5.2.4 et 5.3.1, il est naturel de se demander si on peut montrer un résultat analogue pour la dichotomie intrication vs séparabilité, qui est beaucoup plus fondamentale. Notons j la jauge de l'ensemble $\mathrm{Sep}_{d\otimes d}$. Comme j ne peut pas se calculer facilement à partir d'informations spectrales, on de dispose pas d'un angle d'attaque par les matrices aléatoires.

Nous avons néanmoins obtenu le théorème suivant, qui montre qu'il existe une transition de phase lorsque la taille de l'environnement s est de l'ordre de d^3. Seuls les cas $s = O(d^2)$ et $s = \Omega(d^4)$ étaient auparavant connus [17].

Théorème 5.4.1 ([A8]). *On note $s_0(d) \coloneqq w\big(\mathrm{Sep}^\circ_{d\otimes d}\big)^2$. Cette fonction vérifie les inégalités*

$$cd^3 \leqslant s_0(d) \leqslant Cd^3 \log^2 d$$

et a la propriété suivante : si ρ est un état aléatoire de loi $\mathrm{Induit}(\mathbb{C}^d \otimes \mathbb{C}^d, s)$*, et $\varepsilon > 0$, alors*

1. *Si $s \geqslant (1+\varepsilon)s_0(d)$, alors ρ est séparable avec grande probabilité.*
2. *Si $s \leqslant (1-\varepsilon)s_0(d)$, alors ρ est intriqué avec grande probabilité.*

Les estimations sur la largeur moyenne de l'ensemble $\mathrm{Sep}^\circ_{d\otimes d}$ sont une conséquence de l'inégalité MM^* ; cela a été expliqué au Chapitre 3.4. Remarquons que $w(\mathrm{Sep}^\circ_{d\otimes d})$ est la valeur moyenne de j sur la sphère-unité de l'espace euclidien $V_{d\otimes d}$. Ce qui nous intéresse est la valeur moyenne de j pour une autre mesure de probabilité : la loi $\mathrm{Induit}(\mathbb{C}^d \otimes \mathbb{C}^d, s)$. Le passage d'une estimation en moyenne à une estimation avec grande probabilité découlera ensuite d'arguments classiques de concentration de la mesure.

Il est bien connu qu'on peut approximer la mesure uniforme sur une sphère de grande dimension par un vecteur gaussien à coefficients indépendants. Dans l'espace euclidien $V_{d\otimes d}$, cette approche amène naturellement à considérer l'ensemble gaussien unitaire (GUE) *conditionné à être de trace nulle*, que nous noterons GUE_0. La proposition suivante permet de comparer les valeurs moyennes de jauges pour ces deux modèles matriciels (les états induits vs l'ensemble GUE_0) et de voir qu'elles sont équivalentes dans le régime $s \gg d^2$. On peut alors en déduire aisément le Théorème 5.4.1.

Proposition 5.4.2 ([A8]). *On rappelle que $V_n \subset \mathsf{M}_n$ désigne l'espace des matrices hermitiennes de trace* 1*. Soit $C_{n,s} \in [1, +\infty)$ la plus petite constante ayant la propriété suivante : pour tout corps convexe $K \subset V_n$, on a*

$$C_{n,s}^{-1}\, \mathbf{E}\left[j_K\left(\rho_* + \frac{G}{n\sqrt{s}}\right)\right] \leqslant \mathbf{E}\left[j_K(\rho)\right] \leqslant C_{n,s}\, \mathbf{E}\left[j_K\left(\rho_* + \frac{G}{n\sqrt{s}}\right)\right],$$

où G est une matrice aléatoire $n \times n$ de loi GUE_0*, et ρ un état aléatoire de loi* $\mathrm{Induit}(\mathbb{C}^n, s)$*. Si (n_k) et (s_k) sont des suites qui tendent vers $+\infty$ et telles que $\lim s_k/n_k = +\infty$, on a*

$$\lim_{k\to\infty} C_{n_k,s_k} = 1.$$

On peut voir la Proposition 5.4.2 comme un théorème central limite quantitatif : la convergence (n fixé, $s \to \infty$) des états induits vers l'état maximalement mélangé ρ_* est exactement la loi des grands nombres, que l'on précise ici en faisant une approximation gaussienne. Pour se faire une intuition des phénomènes mis en jeu derrière la Proposition 5.4.2, il faut remarquer que pour $\alpha \gg 1$, la loi de Marčenko–Pastur $\mathrm{MP}(\alpha)$ peut être approchée par la loi semi-circulaire de moyenne 1 et de variance $1/\alpha$. C'est l'analogue en probabilités libres de l'approximation d'une loi de Poisson de grand paramètre par une loi gaussienne. Les deux modèles matriciels que l'on compare ont précisément ces deux lois comme spectre limite. Enfin, on utilise le concept de *domination de Schur* (voir Chapitre 6.1) pour déduire de la similitude des spectres une comparaison entre l'espérance des jauges ; la notion de convergence ∞-Wasserstein est particulièrement bien adaptée à cette tâche.

Les différents résultats présentés dans ce chapitre donnent une description précise du comportement typique des états induits. En particulier, dans le régime $d^2 \ll s \ll d^3$, les états induits aléatoires sont génériquement PPT et intriqués. De tels états ont des propriétés remarquables qui illustrent l'irréversibilité de la manipulation de l'intrication. En effet, il est possible de les créer par des opérations locales à partir d'états maximalement intriqués sur deux qubits, mais la transformation inverse est impossible : on ne peut pas les *distiller*. L'existence d'états intriqués mais non distillables était bien connue, mais nous montrons que cette situation est loin d'être pathologique : elle prédomine en grande dimension.

5.5 Discrimination des états aléatoires

Le problème de la discrimination des états a déjà été mentionné au Chapitre 4.4, où nous avons considéré une mesure quantique formalisée par un POVM. En pratique, il est souvent possible de choisir parmi une famille de POVMs celui qui est le plus adapté. On a par exemple le résultat élémentaire suivant : pour $\rho, \sigma \in \mathrm{D}_n$, on a

$$\|\rho - \sigma\|_1 = \sup_{\mathrm{M}} \|\rho - \sigma\|_{\mathrm{M}} \tag{5.1}$$

où le supremum est pris sur tous les POVMs sur $\mathbb{C}^n$. L'égalité (5.1) est importante car permet de donner une interprétation de la norme $\|\cdot\|_1$ comme mesurant notre capacité à distinguer des états.

Intéressons-nous maintenant à un problème de discrimination générique, lorsque ρ et σ sont des états aléatoires indépendants de loi uniforme sur D_n

(on pourrait plus généralement considérer des états de loi Induit($\mathbb{C}^n, s$), qui donnent la loi uniforme pour $s = n$). On peut, à l'aide des probabilités libres, donner un équivalent précis de $\|\rho - \sigma\|_1$ quand n tend vers l'infini [31]. La situation est beaucoup plus complexe si on introduit des contraintes de localité pour les mesures quantiques que l'on s'autorise. Le langage habituel pour décrire ces contraintes est celui de deux expérimentateurs distants, traditionnellement prénommés Alice et Bob, ayant chacun accès à l'une des copies de $\mathbb{C}^d$. Les restrictions de localité les plus souvent considérées sont présentées ci-après. Ces contraintes définissent chacune une famille de POVMs sur $\mathbb{C}^d \otimes \mathbb{C}^d$.

LOCC$^\rightarrow$ est l'ensemble des opérations locales avec communication unilatérale : Alice effectue une mesure quantique et en transmet le résultat à Bob. Ensuite, Bob effectue une mesure quantique dont le choix peut dépendre du résultat transmis par Alice.

LOCC est l'ensemble des opérations locales avec communication bilatérale : Alice et Bob effectuent alternativement des mesures quantiques dont ils transmettent le résultat à leur partenaire. Le choix des mesures à effectuer et du moment où s'arrêter dépendent de l'historique du protocole.

SEP est l'ensemble des opérations séparables, dont la définition est modelée sur celle des états séparables.

PPT est la classe des opérations à transposition partielle positive, dont la définition est modelée sur celle des états PPT.

ALL est la classe de toutes les opérations possibles.

On peut donner une définition mathématique précise de toutes ces classes (voir par exemple [A6]). La classe la plus naturelle du point de vue de la théorie quantique de l'information est la classe **LOCC**, mais c'est aussi celle dont la définition est la plus compliquée, en particulier car le nombre de mesures effectuées alternativement par Alice et Bob peut être arbitrairement grand. On a les inclusions

$$\mathbf{LOCC}^\rightarrow \subset \mathbf{LOCC} \subset \mathbf{SEP} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Lorsque $\mathbf{X}$ est une de ces familles de POVMs, on pose

$$\|\cdot\|_{\mathbf{X}} = \sup_{\mathrm{M} \in \mathbf{X}} \|\cdot\|_{\mathrm{M}}. \tag{5.2}$$

On peut remarquer que $\|\cdot\|_{\mathbf{ALL}} = \|\cdot\|_1$.

Notre résultat principal, en collaboration avec Cécilia Lancien, est une comparaison de l'impact relatif de ces différentes contraintes de localité pour un problème de discrimination générique.

Théorème 5.5.1 ([A6]). *Soient ρ et σ deux états aléatoires indépendants de loi uniforme sur $\mathrm{D}_{d\otimes d}$. Alors, avec grande probabilité, on a*

1. $\|\rho - \sigma\|_{\mathbf{X}} = O(1)$ *pour* $\mathbf{X} \in \{\mathbf{PPT}, \mathbf{ALL}\}$,
2. $\|\rho - \sigma\|_{\mathbf{X}} = O\left(1/\sqrt{d}\right)$ *pour* $\mathbf{X} \in \{\mathbf{LOCC}^{\rightarrow}, \mathbf{LOCC}, \mathbf{SEP}\}$.

On peut, par des arguments similaires à ceux utilisés dans la preuve de la Proposition 5.4.2, ramener la preuve du Théorème 5.5.1 à l'estimation du volume de différents corps convexes associées à chacune des classes de localité, ce qui peut se traiter par des arguments classiques de géométrie convexe. Notons aussi que le Théorème 5.5.1 justifie, dans les scénarios génériques, une hypothèse simplificatrice commune en information quantique : au lieu de considérer la classe **LOCC** qui est délicate à manipuler, on travaille sur sa relaxation **SEP**. Une autre conséquence plus surprenante du notre résultat est que, toujours pour des scénarios génériques, la communication bilatérale n'est pas sensiblement plus efficace que la communication unilatérale.

Enfin, les algorithmes de dissimulation de données reposent sur l'existence d'états ρ et σ tels que $\|\rho - \sigma\|_1 = 2$ tandis que $\|\rho - \sigma\|_{\mathbf{LOCC}} \ll 1$. De tels états ne peuvent être efficacement distingués que par des mesures quantiques globales. Un exemple bien compris est la paire formée des projections sur les sous-espaces symétrique et antisymétrique de $\mathbb{C}^d \otimes \mathbb{C}^d$, correctement normalisées. Une variante du Théorème 5.5.1 permet de montrer que de tels états sont en fait génériques. Il est possible que cette flexibilité supplémentaire soit utile pour certaines applications.

Chapitre 6

Autres travaux de recherche

Ce dernier chapitre décrit brièvement les travaux que j'ai effectués et qui ne sont pas directement liés à l'intrication quantique. Une fil directeur est néanmoins l'utilisation, dans des contextes qui font intervenir des objets de grande dimension, de techniques qui ne font pas partie de la boîte à outils traditionnelle de la méthode probabiliste (théorème de Cramér et convergence des statistiques de Kolmogorov–Smirnov vers un pont brownien)

6.1 Catalyse quantique et théorème de Cramér

On appelle *vecteur de probabilité* $x \in \mathbb{R}^n$ un vecteur à coordonnées positives et de somme 1. Un ordre partiel sur l'ensemble des vecteurs de probabilité est donné par la *domination de Schur* : on dit que x est dominé par y ($x \prec y$) si x est combinaison convexe de vecteurs obtenus en permutant les coordonnées de y. Cet ordre a une interprétation en théorie quantique de l'information. Pour un vecteur de probabilité $x \in \mathbb{R}^n$, notons $\psi_x \in \mathbb{C}^n \otimes \mathbb{C}^n$ le vecteur

$$\sum_{i=1}^{n} \sqrt{x_i} e_i \otimes e_i,$$

où (e_i) est la base canonique de $\mathbb{C}^n$. Le théorème de Nielsen affirme que $x \prec y$ si et seulement si il est possible de transformer l'état $|\psi_y\rangle\langle\psi_y|$ en l'état $|\psi_x\rangle\langle\psi_x|$ par des opérations de la classe **LOCC**.

On peut donner des exemples de vecteurs de probabilités x, y, z tels que

1. $x \not\prec y$,
2. $x^{\otimes 2} \prec y^{\otimes 2}$,
3. $x \otimes z \prec y \otimes z$.

On est en présence d'un phénomène un peu surprenant : la transformation individuelle de ψ_y vers ψ_x est impossible, mais la transformation par groupes de deux est possible. De même, la transformation individuelle devient possible si l'environnement se trouve dans un état ψ_z : on dit alors que z est un *catalyseur*.

J'ai contribué dans [A18, A17] à la description de conditions nécessaires et suffisantes sur x, y pour que les transformations multiples, ou la transformation en présence de catalyseur, soient possibles. On a par exemple

Théorème 6.1.1 ([A18]). *Soit y un vecteur de probabilité, et notons $T_y \subset \mathbb{R}^{(\mathbb{N})}$ l'ensemble des vecteurs de probabilités x tels que $x^{\otimes n} \prec y^{\otimes n}$ pour un entier n. Alors l'adhérence de T_y pour la norme de ℓ_1 est décrite par les inégalités $\|\cdot\|_p \leqslant \|y\|_p$ pour tout $p \geqslant 1$.*

Des variantes font intervenir les généralisations des normes ℓ_p pour $p \in \mathbb{R}$. Notre contribution est de faire le lien avec la question suivante : si μ et ν sont deux mesures de probabilité sur $\mathbb{R}$, quelles conditions garantissent l'existence d'un entier n tel que la convolution μ^{*n} soit stochastiquement dominée par ν^{*n} ? Le théorème de grandes déviations de Cramér permet d'y répondre. Pour le problème de la catalyse (mais non pas celui des transformations multiples), des résultats plus précis ont été obtenus indépendamment par Turgut à l'aide d'une méthode très différente [40].

On étudie dans [A4] une généralisation en dimension infinie, et on montre dans [A12] un résultat lié : parmi toutes les normes sur $\mathbb{R}^{(\mathbb{N})}$ invariantes par permutation, les normes ℓ_p sont caractérisées par l'équation $\|x \otimes y\| = \|x\| \cdot \|y\|$.

6.2 Fonction maximale pour les cubes de grande dimension

La fonction maximale associée à une mesure de probabilité μ sur $\mathbb{R}^n$ est définie pour $x \in \mathbb{R}^n$ par

$$M\mu(x) = \sup_{r>0} \frac{\mu(Q(x,r))}{\mathrm{vol}(Q(x,r))},$$

où $Q(x,r)$ désigne le cube de centre x et de rayon r. L'inégalité de Hardy–Littlewood pour la fonction maximale, fondamentale en analyse harmonique, peut être vue comme un raffinement de l'inégalité de Markov : pour tout $t > 0$, et pour toute mesure de probabilité μ, on a

$$t\,\mathrm{vol}\{M\mu > t\} \leqslant D_n,$$

où D_n est une constante qui ne dépend que de la dimension. Les preuves classiques passent par des lemmes de recouvrement et donnent une borne $D_n \leqslant C^n$, qui a été raffinée en $D_n \leqslant Cn \log n$ par Stein et Strömberg [37]. Un progrès spectaculaire a été obtenu par Aldaz [1] en montrant que la suite (D_n) n'est pas bornée. A titre d'illustration, on ne sait pas si la cela est vrai quand on remplace les cubes par des boules euclidiennes.

L'argument d'Aldaz repose sur l'idée suivante : on choisit pour μ la mesure uniforme sur $\mathbb{Z}^n \cap Q(0,R)$ avec R assez grand, et on montre que la valeur de la fonction maximale en $x \in \mathbb{R}^n$ dépend de la répartition statistique des coordonnées de x modulo 1. Ma contribution [A15] a été d'y incorporer le théorème central limite fonctionnel de Donsker : pour n grand, cette répartition est décrite par un pont brownien. Cela donne une preuve conceptuelle du fait que (D_n) n'est pas bornée. On peut également, à l'aide de la loi du logarithme itéré, obtenir une borne inférieure $D_n \geqslant (\log n)^{1-o(1)}$. Quelques années plus tard, ce résultat a été grandement amélioré par Iakovlev et Strömberg [23] : à l'aide d'un argument plus sophistiqué, ils ont obtenu la minoration $D_n \geqslant cn^{1/4}$. Une excellente référence sur les fonctions maximales en grande dimension est l'article de survol [7].

Bibliographie

[1] J. M. Aldaz. The weak type $(1,1)$ bounds for the maximal function associated to cubes grow to infinity with the dimension. *Ann. of Math. (2)*, 173(2) :1013–1023, 2011.

[2] S. T. Belinschi, B. Collins, and I. Nechita. Almost one bit violation for the additivity of the minimum output entropy. *Comm. Math. Phys.*, 341(3) :885–909, 2016.

[3] J. Bourgain, J. Lindenstrauss, and V. Milman. Approximation of zonoids by zonotopes. *Acta Math.*, 162(1-2) :73–141, 1989.

[4] J. Bourgain and V. D. Milman. New volume ratio properties for convex symmetric bodies in $\mathbf{R}^n$. *Invent. Math.*, 88(2) :319–340, 1987.

[5] K. Chen and L.-A. Wu. A matrix realignment method for recognizing entanglement. *Quantum Inf. Comput.*, 3(3) :193–202, 2003.

[6] B. Collins. Haagerup's inequality and additivity violation of the Minimum Output Entropy. *Houston J. Math.*, to appear.

[7] L. Deléaval, O. Guédon, and B. Maurey. Dimension free bounds for the Hardy–Littlewood maximal operator associated to convex sets. *arXiv preprint arXiv :1602.02015*, 2016.

[8] A. Dvoretzky. Some results on convex bodies and Banach spaces. In *Proc. Internat. Sympos. Linear Spaces (Jerusalem, 1960)*, pages 123–160. Jerusalem Academic Press, Jerusalem ; Pergamon, Oxford, 1961.

[9] T. Figiel, J. Lindenstrauss, and V. D. Milman. The dimension of almost spherical sections of convex bodies. *Acta Math.*, 139(1-2) :53–94, 1977.

[10] T. Figiel and N. Tomczak-Jaegermann. Projections onto Hilbertian subspaces of Banach spaces. *Israel J. Math.*, 33(2) :155–171, 1979.

[11] S. Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Inf. Comput.*, 10(3-4) :343–360, 2010.

[12] O. Guédon, S. Mendelson, A. Pajor, and N. Tomczak-Jaegermann. Majorizing measures and proportional subsets of bounded orthonormal systems. *Rev. Mat. Iberoam.*, 24(3) :1075–1095, 2008.

[13] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 10–19. ACM, 2003.

[14] L. Gurvits and H. Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Phys. Rev. A*, 66(6) :062311, 2002.

[15] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4) :255–257, 2009.

[16] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing quantum states : Constructions and applications. *Comm. Math. Phys.*, 250(2) :371–391, 2004.

[17] P. Hayden, D. W. Leung, and A. Winter. Aspects of generic entanglement. *Comm. Math. Phys.*, 265(1) :95–117, 2006.

[18] P. Hayden and A. Winter. Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$. *Comm. Math. Phys.*, 284(1) :263–280, 2008.

[19] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1) :269–273, Jan 1998.

[20] A. S. Holevo. The additivity problem in quantum information theory. In *International Congress of Mathematicians. Vol. III*, pages 999–1018. Eur. Math. Soc., Zürich, 2006.

[21] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states : necessary and sufficient conditions. *Physics Letters A*, 223(1–2) :1–8, 1996.

[22] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed quantum states : Linear contractions and permutation criteria. *Open Systems & Information Dynamics*, 13(01) :103–111, 2006.

[23] A. S. Iakovlev and J.-O. Strömberg. Lower bounds for the weak type $(1, 1)$ estimate for the maximal function associated to cubes in high dimensions. *Math. Res. Lett.*, 20(5) :907–918, 2013.

[24] M. A. Jivulescu, N. Lupa, and I. Nechita. Thresholds for entanglement criteria in quantum information theory. *Quantum Inf. Comput.*, 15(13-4) :1165–1184, 2015.

[25] G. Kuperberg. From the Mahler conjecture to Gauss linking integrals. *Geom. Funct. Anal.*, 18(3) :870–892, 2008.

[26] Y.-K. Liu. Universal low-rank matrix recovery from Pauli measurements. In *Advances in Neural Information Processing Systems 24*, pages 1638–1646. Curran Associates, Inc., 2011.

[27] V. D. Milman. A new proof of A. Dvoretzky's theorem on cross-sections of convex bodies. *Funkcional. Anal. i Priložen.*, 5(4) :28–37, 1971.

[28] F. Nazarov. The Hörmander proof of the Bourgain-Milman theorem. In *Geometric aspects of functional analysis*, volume 2050 of *Lecture Notes in Math.*, pages 335–343. Springer, Heidelberg, 2012.

[29] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77 :1413–1415, Aug 1996.

[30] G. Pisier. Un théorème sur les opérateurs linéaires entre espaces de Banach qui se factorisent par un espace de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 13(1) :23–43, 1980.

[31] Z. Puchała, Ł. Pawela, and K. Życzkowski. Distinguishability of generic quantum states. *Phys. Rev. A*, 93 :062112, Jun 2016.

[32] G. Schechtman. More on embedding subspaces of L_p in l_r^n. *Compos. Math.*, 61 :159–169, 1987.

[33] G. Schechtman. A remark concerning the dependence on ϵ in Dvoretzky's theorem. In *Geometric aspects of functional analysis (1987–88)*, volume 1376 of *Lecture Notes in Math.*, pages 274–277. Springer, Berlin, 1989.

[34] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56 :131–138, Jul 1997.

[35] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27 :379–423, 623–656, 1948.

[36] P. W. Shor. Equivalence of additivity questions in quantum information theory. *Comm. Math. Phys.*, 246(3) :453–472, 2004.

[37] E. M. Stein and J.-O. Strömberg. Behavior of maximal functions in $\mathbf{R}^n$ for large n. *Ark. Mat.*, 21(2) :259–269, 1983.

[38] E. Størmer. Positive linear maps of operator algebras. *Acta Math.*, 110 :233–278, 1963.

[39] M. Talagrand. Embedding subspaces of L_1 into ℓ_1^N. *Proc. Am. Math. Soc.*, 108(2) :363–369, 1990.

[40] S Turgut. Catalytic transformations for bipartite pure states. *Journal of Physics A : Mathematical and Theoretical*, 40(40) :12185, 2007.

[41] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40 :4277–4281, Oct 1989.

[42] K. Życzkowski and H.-J. Sommers. Induced measures in the space of mixed quantum states. *J. Phys. A*, 34(35) :7111–7125, 2001.

Géométrie de l'intrication quantique

Résumé :

Ce mémoire étudie le phénomène de l'intrication quantique avec le point de vue de la géométrie des convexes de grande dimension. On estime divers invariants géométriques (volume, largeur moyenne, approximabilité par des polytopes) associés à l'ensemble convexe formé par les états quantiques non intriqués, ainsi qu'à l'ensemble dual. Les informations ainsi obtenues sont utilisées pour démontrer des théorèmes de théorie quantique de l'information : non-additivité de la capacité, bornes inférieures sur la complexité de l'intrication, approximation parcimonieuse de canaux ou de mesures quantiques. On obtient également une description précise des propriétés typiques des états quantiques aléatoires de grande dimension.

Geometry of quantum entanglement

Abstract :

This dissertation studies the phenomenon of quantum entanglement with an approach from high-dimensional convex geometry. We estimate several geometric invariants (volume, mean width, approximability by polytopes) associated with the convex set consisting of all non-entangled quantum states, and with the dual set. Using this information we derive several results in quantum information theory : non-additivity of capacity, lower bounds on the complexity of entanglement, sparse approximation of quantum channels and quantum measurements. We also obtain a precise description of typical properties of high-dimensional random quantum states.

Image en couverture : Une section tridimensionelle aléatoire d'un hypercube de dimension 1000. Crédit image : Jos Leys.

UNIVERSITÉ DE LYON